CONFERENCE PROCEEDINGS

Proceedings of the 3rd International Conference on Cryptology and Computer Security

4th June - 6th June 2012
Langkawi, Kedah, Malaysia

Editors :
Hailiza Kamarulhaili
Yahya Abu Hasan
Azman Samsudin
Muhammad Rezal Kamel Ariffin
Mohamad Afendee Mohamed
Mohd Rushdan Md Said
Goi Bok Min
Heng Swee Huay
Rabiah Ahmad
Nor Azman Abu
Moesfa Soeheila Mohamad

Jointly Organized By:

UNIVERSITI SAINS MALAYSIA

MSCR

UNIVERSITI PUTRA MALAYSIA

CyberSecurity MALAYSIA

CRYPTOLOGY 2012

Proceedings of the 3rd International Conference on Cryptology and Computer Security

4th June – 6th June 2012
Langkawi, Kedah, Malaysia

Jointly Organized By:

Perpustakaan Negara Malaysia Cataloguing-In-Publication Data

International Conference on Cryptology and Computer Security
(3rd : 2012 : Langkawi, Kedah)
Proceedings of the 3rd International Conference on Cryptology and Computer Security, 4th June – 6th June 2012, Langkawi, Kedah, Malaysia / editors Hailiza Kamarulhaili ... [et al.].
ISBN 978-967-394-084-4
1. Cryptography—Kedah--Congresses. 2. Computer security--Kedah--Congresses. I. Hailiza Kamarulhaili, 1969-, II. Title.
005.8072

FIRST PUBLISHER 2012
School of Mathematical Sciences, Universiti Sains Malaysia, Pulau Pinang

ISBN 978-967-394-084-4

Published and Printed in Malaysia by:

School of Mathematical Sciences,
Universiti Sains Malaysia,
11800 USM, Pulau Pinang

Edited By:
Hailiza Kamarulhaili
Yahya Abu Hasan
Azman Samsudin
Muhammad Rezal Kamel Ariffin
Mohamad Afendee Mohamed
Mohd Rushdan Md Said
Goi Bok Min
Heng Swee Huay
Rabiah Ahmad
Nor Azman Abu
Moesfa Soeheila Mohamad

EDITORIAL PREFACE

Since the time of Julius Caesar and possibly up until the Greek era, cryptography (a word that is derived from the Greek term "cryptos") has been an integral tool for organizations (and indeed for individuals too) to ensure information that is intended only for authorized recipients remain confidential only to this set of people. Cryptography had far reaching implications for organizations in the event information leakage occurred. Often referred to as the "last bastion of defence" – after all other mechanisms had been overcome by an adversary, encrypted information would still remain useless to the attacker (i.e. that is, under the usual security assumptions). Nevertheless, this simple fact has remained oblivious to the practitioners of information security – omitting cryptographic mechanism for data being transferred and also during storage.

Fast forward to World War 2, – the war between cryptographic and cryptanalytic techniques. While the Germans were efficiently transferring information via the Enigma encryption machine, the Allies in Bletchley Park, England were busy intercepting these ciphered information being transmitted via telegraph by the Germans. Leading mathematicians, linguists, engineers etc. were all working to cryptanalyze these ciphers in the most information way. It is here that the first electrical machine (i.e. the "bomba") was born – and revolutionized computing. Post World War 2 saw the emergence of the "computer". Every organization that had to process data had to acquire a computer so as not to be left behind by their competitor. The banking sector advanced on a global scale due to the invention of the computer. Techniques to secure information among the headquarters of these banks had to be developed. Encryption procedures using the same key (i.e. symmetric encryption) played this role in the early days. Then came the unthinkable problem – computers were being deployed almost everywhere. How is it possible to deploy cryptographic keys in secure manner so that symmetric encryption could take place? Thus, leading to the so-called "key distribution" problem. It was not until 1975, when Diffie and Hellman provided us with a secure key exchange method – and in 1976 when Rivest, Shamir and Adleman with the "asymmetric encryption" scheme (i.e. to encrypt using key e and decrypt uing key d, where $e \neq d$). Since then, cryptographic procedures evolved, not only playing the role of ensuring confidentiality of data, but also to ensure integrity and authenticity of data. It is also able to ensure that non-repudiating of data does not occur.

Mechanisms to transfer and store data has changed of the centuries and more so every 5 years (in this modern age). Cryptography that has long existed before mechanisms changed from manual – telegraphic – electrical – electronic (WAN/LAN/internet) – wired until wireless procedures, has to be properly deployed in order to maintain a high level of security confidence among the stakeholders of a certain organization. The concept of securing information via encryption procedures has to be properly understood in order to avoid a null intersection to occur between cryptography and computer security practitioners. This scenario would not be to the best interest for stakeholders. As a "friendly" reminder, this scenario could already been seen in other discipline of knowledge where the "minuting" ("minute-ting") of knowledge has forced the original body of knowledge to look as though it is independent and disassociated.

Ever since mass usage of computers became a reality, computer security issues have never been this complicated. However, as the human race advances so will ingenious ideas emerge to overcome challenges.

It is hoped that Cryptology2012 will not only provide a platform for every participant to exchange ideas in their respective fields, but also to exchange new ideas on a broader scale for the advancement of the field of cryptology and computer security. The organizing committee hopes every participant will have an enjoyable and beneficial conference.

Thank you.

Editors :

Hailiza Kamarulhaili
Yahya Abu Hasan
Azman Samsudin
Muhammad Rezal Kamel Ariffin
Mohamad Afendee Mohamed
Mohd Rushdan Md Said
Goi Bok Min
Heng Swee Huay
Rabiah Ahmad
Nor Azman Abu
Moesfa Soeheila Mohamad

Penang, June 2012

EDITORS

Hailiza Kamarulhaili
School of Mathematical Sciences, Universiti Sains Malaysia (USM)

Yahya Abu Hasan
School of Mathematical Sciences, Universiti Sains Malaysia (USM)

Azman Samsudin
School of Computer Sciences, Universiti Sains Malaysia (USM)

Muhammad Rezal Kamel Ariffin
Institute for Mathematical Research (INSPEM) Universiti Putra Malaysia (UPM)

Mohamad Afendee Mohamed
Faculty of Computer Science & Information Technology, Universiti Putra Malaysia (UPM)

Mohd Rushdan Md Said
Faculty of Science, Universiti Putra Malaysia (UPM)

Goi Bok Min
University Tunku Abdul Rahman (UTAR)

Heng Swee Huay
Multimedia University (MMU)

Rabiah Ahmad
Universiti Teknikal Malaysia, Melaka (UTEM)

Nor Azman Abu
Universiti Teknikal Malaysia, Melaka (UTEM)

Moesfa Soeheila Mohamad
Malaysian Institute of Microelectronic Systems (MIMOS Bhd.)

ADVISORY COMMITTEE

1. Prof. Dato Dr. Hj. Kamel Ariffin Mohd Atan (Universiti Putra Malaysia)
2. Prof. Ahmad Izani Md. Ismail (Universiti Sains Malaysia)
3. Assoc. Prof. Dr. K.W.Wong (City University of Hong Kong)
4. Dato Prof. Dr. Norbik Bashah Idris (Universiti Teknologi Malaysia)
5. Prof. Mohamed Ridza Wahiddin (MIMOS)
6. Prof. Dr. Shahrin Sahib (Universiti Teknikal Malaysia, Melaka)
7. Prof. Fred Piper (Royal Holloway, University of London, U.K)
8. Prof. Dr. Mohd Salmi Md Noorani (Universiti Kebangsaan Malaysia)
9. Prof. Dr. Keith Martin (Royal Holloway, University of London, U.K)
10. Lt. Col. Dato' Prof. Husin Jazri (CyberSecurity Malaysia)

GENERAL CHAIR

1. Assoc. Prof. Dr. Rabiah Ahmad (Universiti Teknikal Malaysia, Melaka)
2. Dr. Muhammad Rezal Kamel Ariffin (Universiti Putra Malaysia)

PROGRAMME CHAIR

Assoc. Prof. Dr. Hailiza Kamarulhaili (Universiti Sains Malaysia)

PROGRAMME COMMITTEE

1. Lt. Kol.(B) Asmuni Yusof (CyberSecurity Malaysia)
2. Dr. Raphael C. W. Phan (Loughborough University)
3. Assoc. Prof. Dr. Goi Bok Min (Universiti Tunku Abdul Rahman)
4. Assoc. Prof. Dr. Heng Swee Huay (Multimedia University, Malaysia)
5. Rasidah Abdul Mutalib (Universiti Teknologi MARA)
6. Nor Azman Abu (Universiti Teknikal Malaysia, Melaka)
7. Hazlin Abdul Rani (CyberSecurity Malaysia)
8. Wan Zariman Omar @ Othman (CyberSecurity Malaysia)
9. Assoc. Prof. Dr. Mohd Rushdan Md Said (Universiti Putra Malaysia)

LOCAL COMMITTEE

1. Assoc. Prof. Dr. Azman Samsudin
2. Dr. Ang Miin Huey
3. Dr. Azhana Ahmad
4. Dr. Joshua Ignatius
5. Dr. Nuzlinda Abdul Rahman
6. Dr. Syakila Ahmad
7. Dr. Teh Su Yean
8. Dr. Yahya Abu Hasan
9. Dr. Yazariah Yatim
10. Muhamad Rashidi A.Rahman

TABLE OF CONTENTS

MOUFANG LOOPS AS POTENTIAL PLATFORMS FOR CRYPTOSYSTEMS

Wing Loon Chee
School of Mathematical Sciences, Universiti Sains Malaysia,
11800 USM, Penang, Malaysia.
wlchee@usm.my

Abstract:

One of the earliest examples of public key cryptography is the Diffie-Hellman key exchange protocol. The protocol is based on number theory, in particular, the discrete logarithm problem (DLP): given integers g, h and n, find an integer a such that ga ≡ h (mod n). In 2000, Ko, Lee et al. modified the Diffie-Hellman protocol by using a class of algebraic structures called groups, as platform. The security of this protocol lies on the conjugacy search problem (CSP): given elements g and h in a group, find an element a in the group such that a−1ga = h. In this paper, we propose another type of algebraic structures—Moufang loops, which can potentially serve as platforms for cryptosystems. Moufang loops differ from groups mainly due to their lack of associativity. We shall present a new protocol which uses nonassociative Moufang loops of order pq3 as platform.

Introduction

Public-key cryptosystems are widely used in electronic communications, banking and commerce, the internet and e-mail systems to encrypt confidential information and to verify the identities of communicating parties. The current cryptosystems like the Diffie-Hellman, the ElGamal and RSA cryptosystems remain very secure. Number theory is the basis of these cryptosystems. But in the future with the possible development of quantum computers, these cryptosystems can possibly be broken by computationally unbounded adversary.

For a brief history of the development of cryptography, we begin with the Diffie-Hellman key exchange protocol which was invented by Whitfield Diffie and Martin Hellman in 1976. It was the first practical method for establishing a shared secret over an unprotected communications channel. The security of this protocol lies on the discrete logarithm problem, that is, given integers g, h and n, can we find an integer a such that $g^a \equiv h \pmod{n}$? The method was followed shortly afterwards by RSA, another implementation of public key cryptography. The RSA algorithm was first described publicly in 1978 by Ron Rivest, Adi Shamir and Leonard Adleman. Its security is based on the problem of integer factorisation.

Besides number theory, other mathematical areas such as geometry, chaos theory and abstract algebra have been applied in the study of cryptosystems. In the field of abstract algebra, for instance, K. H. Ko, S. J. Lee et al. (2000) proposed a new protocol that makes use of the conjugacy search problem, a generalisation of the discrete logarithm problem to algebraic structures called groups. The conjugacy search problem states that given elements g and h in a group G, can we find an element a in G such that $a^{-1}ga = h$? In the Ko-Lee et al. protocol, the braid groups were used as platform. Following that, semigroups and rings have also been used in cryptosystems (see Maze et al., 2007; Kropholler et al., 2010; and Baumslag et al., preprint). Since the structures mentioned above are all associative, we propose the use of nonassociative structures as potential platforms of cryptosystems.

A possible candidate is Moufang loop—a nonassociative structure which behaves very similarly to groups. In the absence of the associative property, we conjecture that the use of Moufang loops in cryptosystems would increase the computational difficulty of an adversary and strengthen the security of the systems. In this paper, we shall present a new protocol which uses nonassociative Moufang loops of order pq^3 as platform.

Two Known Protocols

In this section, we recall two key exchange protocols, namely the Diffie-Hellman, and the Ko-Lee et al., key exchange protocols.

We begin with the Diffie-Hellman key exchange protocol where the security is based on the discrete logarithm problem (DLP). Most of the current public key cryptosystems and public key exchange protocols use the DLP as the basis of their security, for example, the Diffie-Hellman key exchange protocol (1976), the ElGamal public key cryptosystem (1985), the Digital Signature Algorithm (Menezes et al., 1996, §11.5.1) and the ElGamal's signature scheme (1985).

First, we give some mathematical definitions before introducing the protocols.

Definition 2.1. A ***group*** is a set G together with a binary operation that satisfies the following three conditions:
(a) *Existence of identity element:* G has an identity element (denoted by 1_G or 1) such that $1x = x1 = x$ for every element $x \in G$;
(b) *Existence of inverse elements:* Every element $x \in G$ has an inverse element in G (denoted by x^{-1}) such that $x^{-1}x = xx^{-1} = 1$;
(c) *Associativity:* All elements $x, y, z \in G$ satisfy the associative law $(xy)z = x(yz)$.
Furthermore, a group is ***commutative*** (or *abelian*) if any elements x and y satisfy $xy = yx$.

Now the DLP can be restated in algebraic terminologies.

Problem 2.2 (Discrete Logarithm Problem). Let G be a group and $g, h \in G$. Find an integer a such that $g^a = h$.

Problem 2.2 has a solution if and only if $h \in \langle g \rangle$, the cyclic group generated by g. If $h \in \langle g \rangle$, then there is a unique integer a satisfying $1 \leq a \leq |g|$ such that $g^a = h$. This unique integer is called the discrete logarithm of h with base g. The Diffie-Hellman key exchange protocol uses the multiplicative group of integers modulo n (where n is a large prime) as the platform group.

Protocol 2.3 (Diffie-Hellman Key Exchange Protocol). Let G be a group.
(1) Alice and Bob agree on a public element $g \in G$.
(2) Alice chooses a secret integer n and sends g^n to Bob.
(3) Bob chooses a secret integer m and sends g^m to Alice.
(4) Their secret shared key is

$$(g^n)^m = (g^m)^n.$$

Since g^n and g^m are sent through an unprotected channel, the eavesdropper, Eve is able to capture g^n and g^m. Suppose Eve can solve Problem 2.2, that is, Eve can find an integer a such that $g^a = g^n$, then she can compute $(g^m)^a = (g^a)^m = g^{mn}$ which is the common secret key. The brute force attack on Problem 2.2 is to compute $g^1, g^2, g^3, \ldots$ until we obtain an integer a such that $g^a = g^n$. But this process takes exponential time.

Next, we introduce another search problem—the conjugacy search problem (CSP) which was used in Ko-Lee et al. key exchange protocol.

Problem 2.4 (Conjugacy Search Problem). Let G be a group and g, h conjugate elements in G. Find an element $a \in G$ such that $a^{-1}ga = h$.

Protocol 2.5 (Ko-Lee et al. Key Exchange Protocol). Let G be a group and A, B commuting subgroups of G, that is, $xy = yx$ for any $x \in A$ and $y \in B$.
(1) Alice and Bob agree on a public element $g \in G$.
(2) Alice chooses a secret element $a \in A$ and sends $a^{-1}ga$ to Bob.
(3) Bob chooses a secret element $b \in B$ and sends $b^{-1}gb$ to Alice.
(4) Their secret shared key is

$$b^{-1}(a^{-1}ga)b = a^{-1}(b^{-1}gb)a$$

by associativity and commutativity.

In this protocol, the CSP has been implemented using the braid groups as the platform. According to Shpilrain (2004), there are several deterministic algorithms to solve the CSP over the braid groups that are believed to be in polynomial time. Once they are proved to be solvable in polynomial time, the CSP cannot be used over the braid groups. We therefore have to use other groups as platform or find another search problem.

A New Key Exchange Protocol Based on Moufang Loops

In this section, we begin with the discussion of Moufang loops, followed by our proposed protocol. The definition of Moufang loops is very similar to that of groups as they both have a unique identity element, and the inverse property. However, the associative law is replaced by the Moufang identity.

Definition 3.1. A ***Moufang loop*** is a set L equipped with a binary operation, which fulfills the following conditions:
(a) *Existence of identity element:* There exists an element $1 \in L$ such that $1x = x1 = x$ for all $x \in L$.
(b) *Existence of inverse elements:* For every element $x \in L$, there exists $x^{-1} \in L$ such that $x^{-1}x = xx^{-1} = 1$.
(c) *Moufang identity:* Every element in L satisfies $(xy)(zx) = [x(yz)]x$.

Since Moufang loops are generally not associative, the concept of associator is introduced to estimate the degree of nonassociativity of a Moufang loop.

Definition 3.2. The ***associator*** of three elements x, y and z in a loop L is the unique element $(x, y, z) \in L$ such that $(xy)z = [x(yz)](x, y, z)$.

In 2001, A. Rajah constructed a class of nonassociative Moufang loops of order pq^3 where p and q are distinct odd primes satisfying $q \equiv 1 \pmod{p}$. These Moufang loops serve as the platform for our new protocol.

Theorem 3.3. *Let p and q be distinct odd primes such that $q \equiv 1 \pmod{p}$. Define $L = \{(\alpha, \beta, \gamma, \delta) \mid \alpha \in \mathbb{Z}_p, \beta, \gamma, \delta \in \mathbb{Z}_q\}$ and the product of two elements in L is given by*

$$(\alpha_1, \beta_1, \gamma_1, \delta_1)\cdot(\alpha_2, \beta_2, \gamma_2, \delta_2) = (\alpha_{(1,2)}, \beta_{(1,2)}, \gamma_{(1,2)}, \delta_{(1,2)})$$

where

$$\alpha_{(1,2)} \equiv (\alpha_1 + \alpha_2) \pmod{p};$$

$$\beta_{(1,2)} \equiv (\beta_1 \mu^{(p-1)\alpha_2} + \beta_2) \pmod{q};$$

$$\gamma_{(1,2)} \equiv (\gamma_1 \mu^{(p-1)\alpha_2} + \gamma_2) \pmod{q};$$

$$\delta_{(1,2)} \equiv \left[\delta_1 \mu^{\alpha_2} + \delta_2 + \phi\beta_2\gamma_1\mu^{(p-1)\alpha_2} + \frac{\beta_1\gamma_1(\mu^{\alpha_2} - \mu^{(p-2)\alpha_2}) + (\beta_1\gamma_2 - \beta_2\gamma_1)(\mu^{(\alpha_1+\alpha_2)} - \mu^{(p-1)\alpha_2})}{\mu - 1}\right] \pmod{q};$$

μ and ϕ are integers satisfying

$$\mu^p \equiv 1 \pmod{q} \text{ but } \mu \not\equiv 1 \pmod{q},$$

$$\phi \text{ is any integer when } p = 3,$$

$$\phi(\mu - 1) \equiv -2 \pmod{q} \text{ when } p \neq 3.$$

Then L is a nonassociative Moufang loop of odd order pq^3.

Protocol 3.4. Let L be a nonassociative Moufang loop of odd order pq^3.
(1) Alice and Bob publicly agree on the values of p, q, μ, ϕ and an element $g = (\alpha_g, \beta_g, \gamma_g, \delta_g) \in L$.
(2) Alice chooses a secret element $a = (\alpha_a, \beta_a, \gamma_a, \delta_a) \in L$ and sends $a^{-1}ga$ to Bob.
(3) Bob chooses a secret element $b = (\alpha_b, \beta_b, \gamma_b, \delta_b) \in L$ and sends $b^{-1}gb$ to Alice.
(4) Alice receives $b^{-1}gb$ and computes $(a, g, b^{-1}gb)$.
(5) Bob receives $a^{-1}ga$ and computes $(a^{-1}ga, g, b)$.
(6) Their secret shared key is

$$(a, g, b^{-1}gb)^{\mu^{-\alpha_a}} = (a^{-1}ga, g, b)^{\mu^{-\alpha_b}}.$$

Computational Details of Protocol 3.4

By Definition 3.2, we can rewrite the associator of any element x, y and z in a loop as $(x, y, z) = [x(yz)]^{-1}[(xy)z]$. Now let L be a nonassociative Moufang loop of odd order pq^3 and $x = (\alpha_x, \beta_x, \gamma_x, \delta_x)$, $y = (\alpha_y, \beta_y, \gamma_y, \delta_y)$, $z = (\alpha_z, \beta_z, \gamma_z, \delta_z) \in L$. Then (x, y, z) can be computed by using the product rule in Theorem 3.3 as follows:

$$(x, y, z) = \left(0, 0, 0, \frac{\mu^{\alpha_x+\alpha_y}(\mu^{\alpha_z}-1)(\beta_x\gamma_y - \beta_y\gamma_x)}{\mu-1} + \frac{\mu^{\alpha_y+\alpha_z}(\mu^{\alpha_x}-1)(\beta_y\gamma_z - \beta_z\gamma_y)}{\mu-1} + \frac{\mu^{\alpha_z+\alpha_x}(\mu^{\alpha_y}-1)(\beta_z\gamma_x - \beta_x\gamma_z)}{\mu-1}\right).$$

In Protocol 3.4, given the public element $g = (\alpha_g, \beta_g, \gamma_g, \delta_g)$, Alice has to choose a secret element $a = (\alpha_a, \beta_a, \gamma_a, \delta_a)$ and compute $a^{-1}ga$. By Theorem 3.3,

$$\begin{aligned} a^{-1}ga = \Big(&\alpha_g, \beta_a(1-\mu^{-\alpha_g}) + \beta_g\mu^{-\alpha_a}, \gamma_a(1-\mu^{-\alpha_g}) + \gamma_g\mu^{-\alpha_a}, \\ &\delta_a(1-\mu^{\alpha_g}) + \delta_g\mu^{\alpha_a} + \phi\mu^{-\alpha_g}(\mu^{3\alpha_a+2\alpha_g}-1)\beta_a\gamma_a + \phi\mu^{-\alpha_a}\left[\beta_a\gamma_g - \mu^{3\alpha_a-\alpha_g}\beta_g\gamma_a\right] \\ &+\frac{\mu^{-2\alpha_g}\left[\mu^{3\alpha_g}(\mu^{3\alpha_a}-1) + \mu^{3(\alpha_a+\alpha_g)}-1\right]\beta_a\gamma_a}{\mu-1} \\ &+\frac{\left[\mu^{-\alpha_a}(\mu^{2\alpha_a+\alpha_g}-1) - \mu^{\alpha_g}(\mu^{2(\alpha_a-\alpha_g)}-1\right](\beta_g\gamma_a - \beta_a\gamma_g)}{\mu-1} \\ &+\frac{\mu^{-2\alpha_a}(\mu^{3\alpha_a}-1)\left[\beta_g\gamma_g - \mu^{\alpha_a-\alpha_g}(\beta_g\gamma_a + \beta_a\gamma_g)\right]}{\mu-1}. \end{aligned}$$

Bob also chooses a secret element $b = (\alpha_b, \beta_b, \gamma_b, \delta_b)$ and computes $b^{-1}gb$ in a similar manner.

After Alice receives $b^{-1}gb$ from Bob, she needs to compute the associator of a, g and $b^{-1}gb$. Hence, by Theorem 3.3, she gets

$$(a, g, b^{-1}gb) = \left(0, 0, 0, \frac{\mu^{\alpha_g+\alpha_a-\alpha_b}(\mu^{\alpha_b}-1)(\mu^{\alpha_g}-1)(\beta_a\gamma_g - \beta_g\gamma_a)}{\mu-1} + \frac{\mu^{\alpha_a}(\mu^{\alpha_g}-1)^2(\beta_b\gamma_a - \beta_a\gamma_b)}{\mu-1} + \frac{\mu^{\alpha_g}(\mu^{\alpha_a}-1)(\mu^{\alpha_g}-1)(\beta_g\gamma_b - \beta_b\gamma_g)}{\mu-1}\right).$$

On the other hand, Bob receives $a^{-1}ga$ and computes $(a^{-1}ga, g, b)$. Thus

$$(a^{-1}ga, g, b) = \left(0, 0, 0, \frac{\mu^{\alpha_g}(\mu^{\alpha_b}-1)(\mu^{\alpha_g}-1)(\beta_a\gamma_g - \beta_g\gamma_a)}{\mu-1} + \frac{\mu^{\alpha_b}(\mu^{\alpha_g}-1)^2(\beta_b\gamma_a - \beta_a\gamma_b)}{\mu-1} + \frac{\mu^{\alpha_g-\alpha_a+\alpha_b}(\mu^{\alpha_a}-1)(\mu^{\alpha_g}-1)(\beta_g\gamma_b - \beta_b\gamma_g)}{\mu-1}\right).$$

Now by multiplying the fourth term of $(a, g, b^{-1}gb)$ with $\mu^{-\alpha_a}$ and the fourth term of $(a^{-1}ga, g, b)$ with $\mu^{-\alpha_b}$, we get the same element in L. Since $(0, 0, 0, \delta n) = (0, 0, 0, \delta)^n$, we have $(a, g, b^{-1}gb)^{\mu^{-\alpha_a}} = (a^{-1}ga, g, b)^{\mu^{-\alpha_b}}$ which serves as the secret shared key between Alice and Bob.

Future Research Directions

Now that the protocol has been established, the next course of action is to examine its efficiency and security. For the efficiency of the protocol, all the computations in this protocol are believed to take polynomial time as they only involve basic modular arithmetic operations. For its security, we note that the product rule of the nonassociative Moufang loops of odd order pq^3 and the values of p, q, μ, ϕ must be published as Alice and Bob need this information in the process of encryption and decryption. Hence, future research may focus on the difficulty to recover a (and b) from $a^{-1}ga$ (and $b^{-1}gb$).

Acknowledgments

The author wishes to acknowledge Peng Choon Wong and Kok Bin Wong for introducing algebraic cryptography to the author, and Andrew Rajah for his advice on the theoretical aspects of Moufang loops.

References:

Baumslag, G., Brukhov, Y., Fine, B., Rosenberger, G. Encryption methods using formal power series rings. Preprint.

Diffie, W., Hellman, M. E. (1976). New directions in cryptography. *IEEE Trans. Inf. Theory* IT-22(6), 644–654.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory* 31(4), 469–472.

Ko, K. H., Lee, S. J., Cheon, J. H., Han, J. W., Kang, J. S., Park, C. (2000). New public-key cryptosystem using braid groups. *Advances in Cryptology—CRYPTO 2000, Lecture Notes in Computer Science* 1880, 166–183.

Kropholler, P. H., Pride, S. J., Othman, W. A. M., Wong, K. B., Wong, P. C. (2010). Properties of certain semigroups and their potential as platforms for cryptosystems. *Semigroup Forum* 81, 172–186.

Maze, G., Monica, C., Rosenthal, J. (2007). Public key cryptography based on semigroup actions. *Adv. Math. Commun.* 1(4), 489–507.

Menezes, A. J., van Oorschot, P. C., Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press, New York.

Rajah, A. (2001). Moufang loops of odd order pq^3. *J. Algebra* 235, 66–93.

Rivest, R., Shamir, A., Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* 21(2), 120–126.

Shpilrain, V. (2004). Assessing security of some group based cryptosystem. *Contemp. Math. Amer. Math. Soc.* 360, 167–177.

CRYPTANALYSIS OF 3D BYTE PERMUTATION BLOCK CIPHER

Suriyani Ariffin[1,2], Ramlan Mahmod[1], Azmi Jaafar[1]and
Muhammad Rezal Kamel Ariffin[1]
[1]*Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia*
[2]*Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia*
suriyani@tmsk.uitm.edu.my, ramlan@fsktm.upm.edu.my, azmi@fsktm.upm.edu.my,
rezal@math.upm.edu.my

Abstract:

The antigen-antibody interaction, somatic hyper mutation and protein structural features in immune systems have been selected as inspired approach in designing the new block cipher algorithm called 3D-AES. However, these computation elements from immune systems have not proved yet whether it can be successfully applied and satisfies with Shannon's diffusion property in designing a new block cipher algorithm. This paper introduces two different types of attacks on the proposed block cipher. This paper measures and analyzes the diffusion property of the block cipher by a branch number. It also discussed the best possible diffusion and described how it is relevant for differential and linear cryptanalysis in the contact of the wide trail strategy family. This research defined that there are no three- round linear trails with predictable input output correlation above 2^{-102} and no three- round differential trails with a predictable propagation ratio above 2^{-204}, hence, making 3D-AES secure against differential and linear attacks.

Introduction

There is a number of block ciphers based on the wide trail strategy family such as Shark (Rijmen et. al., 1996), Square (Daemen et. al., 1997), Crypton (Lim, 1998), Khazad (Barreto and Rijmen, 2000a), Anubis (Barreto and Rijmen, 2000b), AES (Daemen and Rijmen, 2002b), Pyramid or High Diffusion (Mathur et. al., 2006), Curupira (Barreto and Simplicio, 2007) and 3D block cipher (Nakahara, 2008). Reducing the total number of iteration round of byte permutation realizations is the principal problem considered especially based on the design of this family. Immune systems were found as a basic design in many algorithms from different domains, but still there was no research that uses the immune system as a basis for designing block cipher especially in terms of round reduction. Ariffin et. al. (2011a) and Ariffin et. al. (2011b) identified the correspondences and highlight essential computation elements which are antigen-antibody interaction, somatic hyper mutation model and protein structure that can be applied in symmetric block cipher that satisfies with Shannon's confusion and diffusion property (Shannon, 1949). However, these computation elements from immune systems have not been proved yet whether it can be successfully applied and satisfies with Shannon's diffusion property. To ensure adequate high security of the systems in the world of information technology, this paper measures and analyzes the diffusion property of 3D-AES cipher (Ariffin et. al., 2011a; Ariffin et. al., 2011b). A metric to measure diffusion called branch number is described in the next section. It discussed the best possible diffusion in the contact of the wide trail strategy. It also described how it is relevant for differential and linear cryptanalysis. This paper is organized as follows: Second section reviews the design of 3D-AES block cipher, third section describes the wide trail strategy design, fourth section measures of diffusion based on branch number, fifth section identifies the resistance to differential and linear cryptanalysis and last section conclusions and future works of the paper.

3D-AES Block Cipher Review

The 3D-AES block cipher is based on the AES which is a key-alternating block cipher, composed of rotation key function, n iterations of round function and key mixing operations. The round function consists of non linear substitution function, permutation function and transposition function. A block diagram of the 3D-AES is given in Figure 1 in the form of 4 x 16 bytes. The original message is called the plaintext, denoted P^i, where $i = \{0, 1, 2, 3\}$. The unreadable form is called the ciphertext, denoted by C^i, where $i = \{0, 1, 2, 3\}$. The secret master key is denoted by K. The transformation of P into C is called encryption and the reverse process is called decryption. The P, as it goes through each round of the cipher, is referred to as the cipher state, denoted as F. Note that, the output cipher state, F of the key mixing layer of round r_1 forms the input cipher state to the next round r.

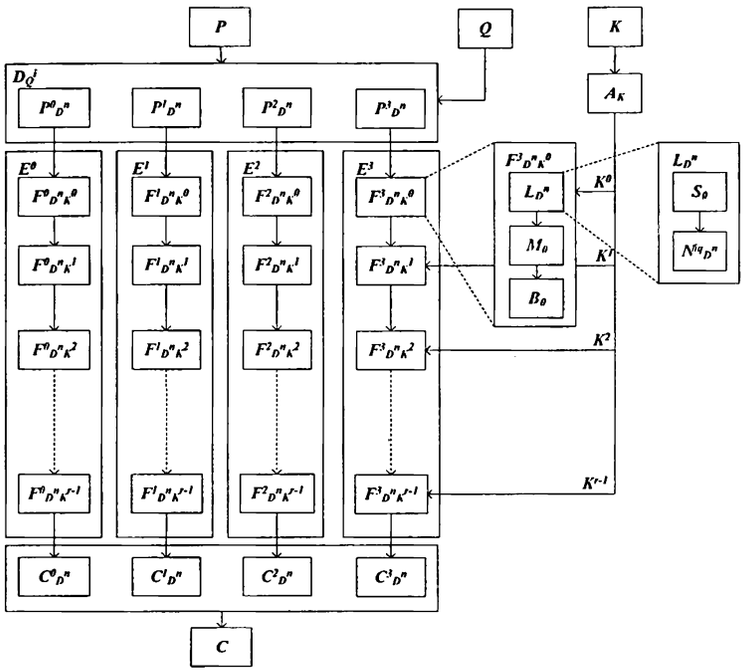


Figure 1: The structure of 3D-AES block cipher

A detailed description of all the layers of 3D-AES block cipher follows:

- $P^i_{D^n}$ is a plaintext for i^{th} slice at n^{th} cube.
- $C^i_{D^n}$ is a ciphertext for i^{th} slice at n^{th} cube.
- Q is a rotation key .
- D^n_Q is the output of n^{th} cube from arranging function at rotation key Q.
- E^i is a encryption function for i^{th} slice.
- $F^i_{D^n K^r}$ is a output block of encryption function for i^{th} slice at cipher state for n^{th} cube in round r.
- K^r is the sub key used in round r.
- A_K is key scheduling function.
- $L^i_{D^n}$ is a output block of linear transformation function for i^{th} slice at Q rotation key at n^{th} cube.
- S_i is a nonlinear transformation of the i^{th} slice at round function .
- $N^{iq}_{D^n}$ is a rotation function at arranging function of i^{th} slice and q degree at n^{th} cube.
- M_i is a linear transformation of the i^{th} slice at round function.
- B_i is a XOR operation.

The 3D-AES identified the encryption and decryption functions. When r = 3, the output cipher state is the ciphertext. The third round of 3D-AES cipher operates on plaintext size of 16 x 4 bytes to produce an output ciphertext 64 bytes. The secret key size required by the 3D-AES cipher is 16 bytes. All the operations in 3D-AES cipher are performed in the finite field of order 2^8, denoted by $GF(2^8)$.

Permutation function

This immune-inspired block cipher adopted amino acid sequences model that can be rotate with a different angle. However for the purpose of evaluation and testing the implementation of 3D-AES block cipher, every *Slice* of the *Cube* module will be rotate at *3D-SliceRotate* module implementation in four types of angel and clockwise rotation only, which is denoted as $N^{iq}_{D^n}$. The q degree is based on the rotation angel for every i^{th} *Slice* where i = {1, 2, 3, 4} and q = {0, 1, 2, 3}. There is no rotation slice for the first slice, second will be rotate in 90^0, third slice will be rotate in 180^0 and fourth slice will be rotate in 270^0.

Wide Trail Strategy Design

In order to measure diffusion property specifically for substitution-permutation network block ciphers is the branch number (Daemen and Rijmen, 2002b) where is often used in wide trial strategy. Branch number is the sum of the input and output active bytes (nonzero difference in input/output blocks). The branch number denotes the minimum number of active S-boxes for any two consecutive rounds. Therefore, to provide resistance against differential and linear cryptanalysis, the 3D-AES designed according to the wide trail strategy. This paper use branch number of a function as a primary measure of its diffusion. From the analysis, the output differences that occur for more than one pair or, equivalently, many difference propagations with propagation probabilities should larger than 2^{1-nb}. The number can be used to estimate the success of differential and linear attacks on a particular block cipher. There are two ways of measuring the branch number, one is the differential measure and the other is the linear measure. For this purpose, a short introduction of the theory of linear codes by MacWilliams and Sloane (1978) will be described in this section.

The *Hamming weight* is defined as follows:

Definition 1 *The Hamming weight, $w_H(x)$ of the vector x is the number of non-zero components of the vector x.*

The *Hamming distance* is defined based on the definition of *Hamming weight.*

Definition 2 *The Hamming distance, $d_H(x_1, x_2)$ between two vectors x_1 and x_2 is equal to the Hamming weight of the difference of the two vectors.*

The *linear code* is defined as follows:

Definition 3 *A linear [n, k, d] code over $GF(2^p)$ is a k-dimensional subspace of the vector space $GF(2^p)^n$, where any two different vectors of the subspace have a Hamming distance of at least d and d is the largest number with this property.*

The distance *d* of a linear code equals the minimum weight of a nonzero code word in the code.

Definition 4 *The differential branch number of a transformation, T is defined as:*

$$B_d^{diff}(T) = \min_{d_H(x_1, x_2) \neq 0} \{d_H(x_1, x_2) + d_H(T(x_1), T(x_2))\} \quad (1)$$

where, x_1 and x_2 are two input and d_H is the byte Hamming distance, as defined in Definition 2.

Definition 5 *The linear branch number of a transformation, T is defined as:*

$$B_d^{lin}(T) = \min_{x \neq 0} \{w_H(x) + w_H(T(x))\} \quad (2)$$

where, $w_H(x)$ is the Hamming weight as defined in Definition 1 in the number of non-zero codes. If the function T is linear, both linear and differential branch numbers for that function are the same.

Let consider [*n*, *k*, *q*] block code, defined the Galois field of order *q*, *GF(q)* where *n* refers to the number of output codes and *k* refers to the number of input codes. The diffusion is defined as follows:

Definition 6 *A [n, k, q] code C, is said to be a diffusion with the encoding operation, c, if $B_d^{lin,diff}(c) = n + 1$.*

From the definition, the branch number of diffusion should be exactly equal to *n + 1*. The function that measures branch number is denoted as *B( )*.

By definition, 3D-AES has a branch number of *n+1*.

Lemma 1 *The upper bound of branch number is n + 1.*

Proof. For a one byte difference in the messages, the corresponding code words have to differ by all n bytes to maintain the branch number of $n + 1$. Since there are only n bytes in every code word, it is not possible to get a branch number greater than $n + 1$.

By Lemma 1, this is the upper bound and the diffusion is optimal.

Measure of Diffusion Based on Branch Number

From the discussions on the definition of branch number, 3D-AES functions, defined in previous section and by Lemma 1, is the branch number of the output block of encryption function for i^{th} slice at cipher state for n^{th} cube in round r, $F^{i}_{D^n K^r}$, for n^{th} cube from arranging function at rotation key Q, D^{n}_{Q} , denoted as $B(V)$.

In generating the diffusion operation, V, by the transformation, D^{n}_{Q} at *Cube* and $L^{i}_{D^n}$ at *Slice*, V is actually a generator for 16 x 16 diffusion matrix operating in $GF(2^8)$ with branch number,

$$B(V) = 16 + 1 = 17 \qquad (3)$$

The inverse V^{-1} is obtained by inverting V in $GF(2^8)$.

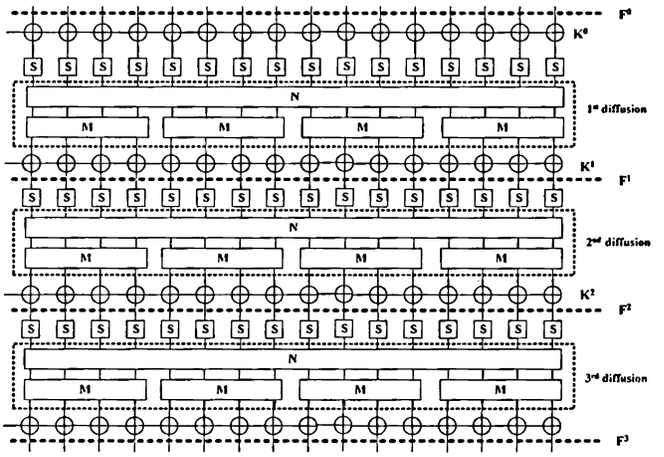


Figure 2: Three round trail of 3D-AES cipher.

Lemma 2 *The minimum number of active bytes in any one round trail of the 3D-AES cipher is 17.*

Proof. The key XOR and substitution do not turn an active byte into an inactive byte, and they also do not turn an inactive byte into an active byte. The sum of active bytes in the input and the output cipher state of a one round trail depends entirely on the branch number of the *mixColumns* function, M. From the Equation 3, it can be concluded that $B(V) = 17$.

Lemma 3 *The minimum number of active bytes in any three round trail of the 3D-AES cipher is 34.*

Proof. From a three round trail illustrated in Figure 2, the minimum number of active bytes in any three round trail of the 3D-AES cipher is $\min(\sum_0^3(F^r))$. This is equal to $\min(\sum_0^1(F^r) + \sum_2^3(F^r))$. From Lemma 2, it has a $\min(\sum_0^1(F^r)) = \min(\sum_2^3(F^r)) = 17$. Therefore, the minimum number of active bytes in any three round trail of the 3D-AES cipher is 34.

Resistance to Differential and Linear Cryptanalysis

It follows that a lower bound on the number of active bytes in any linear or differential trail will give a lower bound on the resistance of the cipher to linear and differential cryptanalysis. From the S-box implemented on AES as mentioned in (Ariffin et. al., 2011a) and for any three-round trail of the 3D-AES cipher as shown in Figure 2, the minimum number of active bytes is shown to be greater than or equal to 34 in Lemma 3. This shows that there are no three-round linear trails with predictable input output correlation above $2^{-3x34} = 2^{-102}$ and no three-round differential trails with predictable propagation ratio of above $2^{-6x34} = 2^{-204}$. From the wide trail strategy (Daemen and Rijmen, 2002a) which is also applicable to AES, it is considered sufficient to resist differential and linear attacks.

Conclusions and Future Works

The antigen-antibody interaction, somatic hyper mutation and protein structural features in immune systems have been selected as an inspired approach in designing the new block cipher algorithm. The branch number of 3D-AES block cipher provides adequate diffusion to the cipher, especially in terms of round reduction. These computation elements from immune systems that can be successfully applied in a symmetric encryption algorithm that satisfies with Shannon's diffusion property in designing a new block cipher algorithm. The construction of 3D-AES block cipher from 3D permutation proves the potential as transformation blocks for ciphers. From the resistance cryptanalysis, this making 3D-AES block cipher secure against cryptanalytic differential and linear attacks. Future work should include possibility deeper analysis of the block cipher algorithm, particularly against other attacks.

References:

Ariffin, S., Mahmod, R., Jaafar, A., and Ariffin, M. R. K.. (2011a). Byte permutations in block cipher based on immune systems. In *International Conference on Software Technology and Engineering, 3rd (ICSTE 2011)*, New York, NY. ASME Press.

Ariffin, S., Mahmod, R., Jaafar, A., and Ariffin, M. R. K. (2011b). Immune systems approaches for cryptographic algorithm. In *Bio-Inspired Computing: Theories and Applications (BIC-TA), 2011 Sixth International Conference on,* pages 231-235.

Barreto, P. S. and Rijmen, V. (2000a). The khazad legacy-level block cipher. Available from http://www.cryptonessie.org/workshop/submissions.html.

Barreto, P. S. and Rijmen, V. (2000b). the anubis block cipher. Available from http://www.cryptonessie.org/workshop/submissions.html.

Barreto, P. S. L. M. and Simplicio, M. (2007). Curupira, a block cipher for con- strained platforms.
Daemen, J. and Rijmen, V. (2002a). AES and the wide trail design strategy. In Knudsen, L., editor, *Advances in Cryptology EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 108-109. Springer Berlin Heidelberg.

Daemen, J. and Rijmen, V. (2002b). *The Design of Rijndael, AES - The Advanced Encryption Standard.* Springer-Verlag.

Lim, C. H. (1998). Crypton: A new 128-bit block cipher specification and analysis.

MacWilliams, F. J. and Sloane, N. (1978). *The Theory of Error-Correting Codes.* North-Holland Publishing Company.

Mathur, C., Narayan, K., and Subbalakshmi, K. (2006). High diffusion cipher:Encryption and error correction in a single cryptographic primitive. In Zhou, J., Yung, M., and Bao, F., editors, *Applied Cryptography and Network Security*, volume 3989 of *Lecture Notes in Computer Science*, pages 309-324. Springer Berlin / Heidelberg.

Nakahara, J. (2008). 3d: A three-dimensional block cipher. In Franklin, M., Hui, L., and Wong, D., editors, *Cryptology and Network Security*, volume 5339 *of Lecture Notes in Computer Science*, pages 252{267. Springer Berlin / Heidelberg.

Rijmen, V., Daemen, J., Preneel, B., Bosselaers, A., and De Win, E. (1996). The cipher shark. In Gollmann, D., editor, *Fast Software Encryption*, volume 1039 of *Lecture Notes in Computer Science*, pages 99-111. Springer Berlin / Heidelberg.

Shannon, C. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656 - 715.

CORRELATED NODE BEHAVIOR MODELING APPROACH FOR EVALUATING SURVIVABILITY IN WIRELESS AD HOC NETWORKS

A.H Azni, Rabiah Ahmad and Zul Azri Muhamad Noh
Center for Advanced Computing Technology
Faculty of Information Technology and Communication
University Technical Malaysia Melaka
P031010002@student.utem.edu.my, rabiah@utem.edu.my, zulazri@utem.edu.my

Abstract:

In this paper we present a k-correlated survivability model for correlated node behavior of wireless ad hoc networks. The model is an extended version of k-connectivity of individual node model. The k-correlated survivability model takes connectivity edge ω to measure node correlation as a new function of survivability. The study evaluates the impact of correlated node behavior particularly selfish, malicious and fails nodes toward network resilience and survivability. The results show that correlated node behaviors have more adverse effects on the survivability. In order to shed light on the effect of correlated node misbehavior correlation on the networks' survivability, common performance metrics are evaluated.

Introduction

Network survivability in ad hoc networks is an essential aspect of reliable communication. It has been defined from different perspective (Lima, et al) to fit different survival system. The most influencing definition is presented by a research group of CMU/SEI, who define survivability as the capability of a system to fulfill its mission on time while attacks, failures or accidents are present (Bakkaloglu). However, in the context of ad hoc networks, survivability depends on how well the ad hoc network demands the survivability requirement. The fundamental requirement for survivability is the ability of the network to provide communication between two nodes in an ad hoc network at any instant. Communication between nodes in ad hoc network is pivotal due to their self organizing topology where each node in the network acts as routers and terminals to forward packets to other nodes. Due to lack of routing infrastructure, the nodes have to cooperate to communicate. Thus, nodes must be in cooperative state for the network to be able to communicate and survive.

Whenever node aberration from normal routing and forwarding behavior, it will drop the data packets from the network and network topology will change drastically. This change of state means nodes are performing misbehavior activity. An example misbehavior activity is power saved when a selfish node does not forward packets for other nodes. An advantage for a malicious node arises when misbehavior enables it to mount an attack. Eventually, node misbehavior leads to node failures. When failures occur, the network suffers from degraded performance because of the unavailability of the failed nodes. The subsequent impact could range from insignificant topological survivability to devastating network shutdown. In literature (Xing), survivability computations assume that:

1. All node failures are equally likely.

2. The node behaviors are mutually independent.

However, these assumptions do not adequately reflect the nature of real world network environments. Typically, different nodes or links can have different failure probabilities depending how the nodes enter failed state. More importantly, real systems show correlated behavior in the event of node failure. For example, node has a correlation with other nodes in such a way that if a node has more and more neighbors failed, it may need to load more traffic originally forwarded by those failed neighbors, and thus might become failed faster due to excessive energy consumption. Similarly, it is also possible that the more malicious neighbors a node has, the more likely the node will be compromised by its malicious neighbors. These circumstances can result in reduced system reliability and availability (Die & Xie). Thus, in comparison to the random and independent node misbehavior, correlated behavior poses an even greater challenge for network connectivity. This new insight has yields new challenges to the survivability of wireless ad hoc networks and motivates us to reveal their fundamental impacts on network survivability. In this paper, we analyzed probabilistically the survivability of wireless ad hoc networks and we quantify the impacts of their correlated node behavior.

Network Survivability Analysis

Survivability in ad hoc networks is defined as its capability to keep contact with neighboring nodes to perform forwarding activity. In this section we evaluate network survivability based on probability of k-correlated in the present of correlated node behavior. K-correlated is a study of network connectivity of the weighted edge graph. Previous study (Xing) has shown survivability on k-connectivity on individual nodes, however, due to correlated node behavior, k-connectivity it is not accurate to analyze the survivability on correlated node behavior. In this paper, we study general cases of correlated node behavior by considering the following three scenarios: (i) the effect of correlated selfish nodes with reluctance in forwarding (control) packets, (ii) the effect of correlated malicious nodes with intent of disrupting routing operations and (iii) the effect of correlated failure node. The objective studied in this work is to model survivability of correlated node behavior. Given a mobile ad hoc network G with four states node behavior (Azni Et al), we find out the probability of network survivability $S_{uv}(G)$ in the present of correlated node behavior.

Network Model

In this work, N mobile nodes in a mobile ad hoc network are randomly and uniformly distributed over a 2-D square with area A. The node transmission radius, denoted by r, is assumed to be identical for all nodes. Thus, the underlying communication graph of a wireless ad hoc network is modeled by undirected weighted graph $G = G(V, E)$ [103] where V denotes the vertex set with $|N| = N$ and an edge E exists between two vertices only if their distance is no greater than r with the weight function $P : E(G) \rightarrow \omega$, interpreted as the probability of the edge being connected. The weighted assign to the edge $e \in E(G)$ denoted with $\omega(e)$. We assume that $\omega(e) \geq 0$ for all edges e. These denotations will be used in the succeeding definitions and analysis.

Network Survivability Definition

We define survivability as connectivity of nodes with correlated cooperative degree to perform forwarding activity. A node is not connected if node u has either selfish or malicious node. Both selfish and malicious nodes can caused multiple failures, we refer them together as misbehaving nodes, denoted as n_{sm} and n_f as failed nodes. The reason these misbehavior nodes are not part of connected network because they cause network to partition, which further affects network survivability. This affect also known as node isolation problem. The node isolation problem has been discuss in various research papers (Nath et al, Thanakornworakij et al, Xing). On the contrary, cooperative nodes, denoted by n_c, comply with the standard in the route discovery and packet forwarding. For nodes to get connected, let $G = (V, E, \omega)$ be undirected graph which has assigned edge connectivity $\omega(u, v)$ for each pair of ϑ_u, ϑ_v of vertices. The edge connectivity of ω also known as *correlated degree* which indicated correlated behavior of neighboring nodes. The edge connectivity must satisfy the following requirements:

$$\omega(u, v) = \omega(d_{uv}, \delta_u, \delta_v) > 0, d_{uv} \leq d_{max}) \tag{1}$$

where d_{uv} is the Euclidean distance between u and v, and δ_u, δ_v are the forwarding capacity of u and v respectively. We define $\omega(u, v) = d_{uv}^b(1/\delta_u + 1/\delta_v)$ where d_{uv}^b represent the forwarding capacity for transmitting data packets between u and v with a distance d_{uv}.

$$\omega(u, v) \geq \delta, \text{ if and only if } \vartheta_u, \vartheta_v \text{ are adjacent in } (G, \omega). \tag{2}$$

Let ω_u denote the degree of $\vartheta_u \in V(G, \omega)$, that is,

$$\omega_u = \sum_v \omega(u, v) = \sum d_{uv}^b(1/\delta_u + 1/\delta_v). \tag{3}$$

δ denotes the forwarding capacity of ω_u which indicate cooperative behavior of neighboring nodes. If $\omega(u, v) \leq \delta$, node is dropping its packets and connection could not be establish, thus node will be isolated from the networks.

To explain node isolation problem in this work, let N_u^i denote node disjoint outgoing path of node u. N_u^i also refer to the number of neighbors of node u at state $i \in \{C, S, M, F\}$.

Proposition 1: *Given the correlated degree of node $\omega(u) \geq \delta$ then node u is connected to the network, and if otherwise node u is isolated from the network. Probability of node being isolated denoted by*

$$\begin{aligned} P_{sm} &= \omega_{(u)} < \delta | \omega_{(u)} = \delta \\ &= P(n_{sm} + n_f) = \delta | \omega = \delta) \\ &= 1 - (1-b)^{\delta} \end{aligned} \tag{4}$$

where b is the probability of node in cooperative state (Azni et al).

Proposition 2: *Given a network G with Nnodes $(N \gg 1)$ and a connectivity requirement w, let P_{sm} denote the probability of node being misbehave and isolated, and μ denote the average number of nodes within one nodes transmission range, then the k-correlated survivability of G is approximated by*

$$S_{uv}(w, G) \approx \left(1 - \frac{\Gamma(w, \mu(1 - P_{sm}))}{\Gamma(w)}\right)^N \tag{5}$$

Given proposition 2, the node is said to be k-correlated if it is (ω, δ)-edge-connected. The physical meaning of this definition is that if a node's cooperative degree is ω then it may communicate with the nodes other than its neighborhood via ω disjoint outgoing paths. Thus, the network survivability of G, denoted by $S_{uv}(G)$, is defined as the probability that nodes in G are connected with cooperative edge δ.

Survivability Computing

As describe above, network survivability measures the connectivity of a correlated node in the network. The connectivity is to calculate the probability that every vertices or nodes in G are connected by a link of correlated edges ω. A network G is connected if and only if any cooperative node u of G has at least ω node-disjoint outgoing paths or has at least k cooperative neighbors. The correlated node survivability will be denoted by $S_{uv}(\omega, G)$.To obtain $S_{uv}(\omega, G)$, $Pr(\omega_{uv} \geq \delta)$ need to be determines. We first derived $Pr(\omega_{uv} \geq \delta)$ by calculating the probability $Pr(d_{uv}^b = \omega | \omega = \delta)$ and $Pr(\omega = \delta)$, where ω denote correlated degree. Then applying the total probability law to get $Pr(d_{uv}^b = \omega)$. We derive $Pr(d_{uv}^b = \omega | \omega = \delta)$ since nodes is either misbehave or cooperative and P_{sm} is the probability of node being misbehave. Thus, the probability of node being cooperative is $1 - P_{sm}$. By a binomial distribution

$$Pr(d_{uv}^b = \omega | \omega = \delta) = \binom{\delta}{\omega} \cdot (1 - P_{sm})^{\omega} \cdot P_{sm}^{\delta - \omega} \tag{6}$$

Now, we investigate the probability of node degree $Pr(\omega = \delta)$. The nodes can be modeled by a Poison point process (Komathy & Narayanasamy). In this process, the Poisson parameter μ presents the average number of nodes within transmission range r. Then $Pr(\omega = \delta)$ is given by

$$Pr(\omega = \delta) = \frac{\mu^d}{\delta!} e^{-\mu} \tag{7}$$

Next, by using the total probability law with (6) and (7), $Pr(\omega = \delta)$ is

$$Pr(\omega = \delta) = \sum_{(\delta = \omega)}^{N-1} \binom{\delta}{\omega} (1 - P_{sm})^{\omega} \cdot p_{sm}^{\delta - \omega} \frac{\mu^{\delta}}{\delta!} e^{-\mu} \tag{8}$$

In (8), δ is bounded by $[\omega, N-1]$. Since N is sufficiently large $(N \gg 1)$, we can rewrite (8) as:

$$Pr(\omega = \delta) \approx \sum_{(\delta=\omega)}^{\infty} \binom{\delta}{\omega} (1 - P_{sm})^{\omega} \cdot p_{sm}^{\delta-\omega} \frac{\mu^{\delta}}{\delta!} e^{-\mu} \tag{9}$$

The using (9), $Pr(\omega_{uv} \geq \delta)$ can be approximated by

$$Pr(\omega \geq \delta) \approx \sum_{a=0}^{\omega-1} \sum_{(\delta=\omega)}^{\infty} \binom{\delta}{a} (1 - P_{sm}^{a}) \cdot p_{sm}^{\delta-a} \frac{\mu^{\delta}}{\delta!} e^{-\mu}$$

$$\approx \frac{\Gamma(\omega, \mu(1 - P_{sm}))}{\Gamma(\omega)} \tag{10}$$

By substituting (10) into (1), (2), and (3) and (4), the *k*-correlated survivability can be given by (5).

Network Survivability Evaluation

In this section, we verify the correctness of our correlated node behavior theory on the network survivability. In simulation, all network parameters are set to the default value given in Table 1 below. Next, we explain our simulation results.

Table 1 : The Network Simulation Set Up

Parameter	Setting
Simulation area	1000 *m* x 1000 *m*
Transmission range	100 *m*
Mobility model	SMS model (uniform placement)
Movement features	Avg. speed 4 *m/s/* pause time 1 *s*
Link capacity	CBR (64 bytes)
Traffic load	100 connections, 8 packet per sec
Simulation time	2000 *s*

The effect of Cooperativeness of Correlated Node

As explain above, correlated node degree is represented by edge connectivity δ. The higher the δ, it implies that the node is strongly connected. To observe the effect of probability of cooperation b, we set $\delta = 0.7$ for cooperative threshold. Figure 1 shows the analytic results of survivability under different nodes range 5, 15, 25, 50 nodes respectively. It is observed that survivability incline steady line with fewer nodes. This is due to the misbehavior node effect are less. Thus, the effect of node behavior is tractable with fewer nodes. This result proofs the concept from (10). Cooperative nodes are affected by correlated survivability ω to obtain a higher survivability. Thus it is necessary to have a higher packet forwarding rate b in order for network to survive. When drop packets are higher, the nodes become less cooperative and network survivability is impossible to achieve.

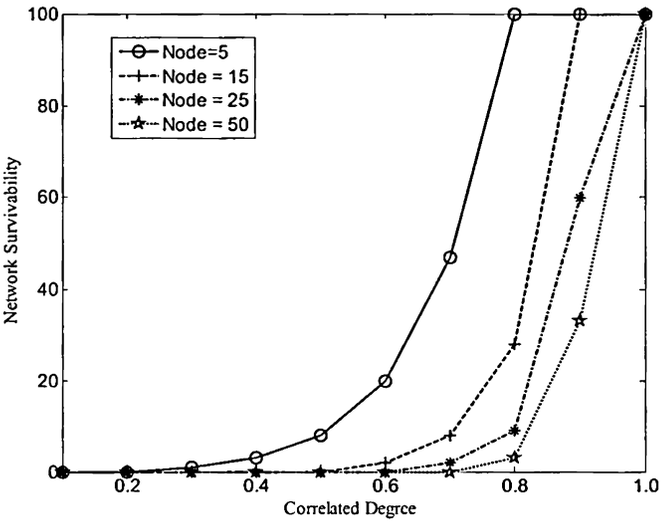


Figure 1 : Effect on survivability of correlated degree ω

The effect of Correlated Misbehave Node (selfish and malicious)

Similar to that in Figure 1, the plot in Figure 2 shows that the survivability decreases as b decrease. The survivability does not change significantly at the beginning especially if network scalability is less. In contrast, survivability for fewer nodes starts to decline faster compared to networks with large nodes. Network also becomes unstable when the δ less than 0.7. From Figure 2 the network survivability decreases very fast due to the packet loads increase. This is due to nodes behave maliciously and disconnected from the network. Thus the load originally routed to the node will be redistributed to neighboring nodes which cause chain reaction. This cause the node cluster will be isolated from the giant network as explain in equation (4) above. It also can be seen that network with more nodes could not sustain it survivability when network under attacks.

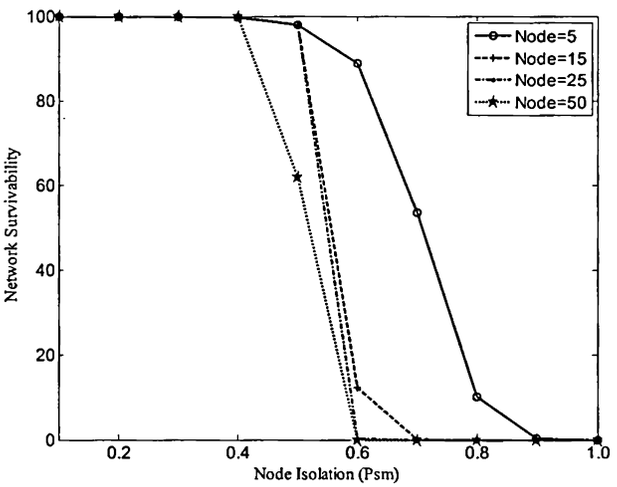


Figure 2 : Effect on survivability of node isolation P_{sm}

The Effect of Correlated Node Failure

For highly survival network, the effect of node failure is more significant, e.g., the survivability drop to almost 0 when $\delta < 0.7$. Compare to malicious and selfish nodes, failed nodes shown severe effect on network survivability. The severer impact of node failures is due to the fact that node failures are also isolated from the network, which reduces the density of active nodes [ ]. Therefore, the probability of network failure cannot be ignored especially for a large scale network.

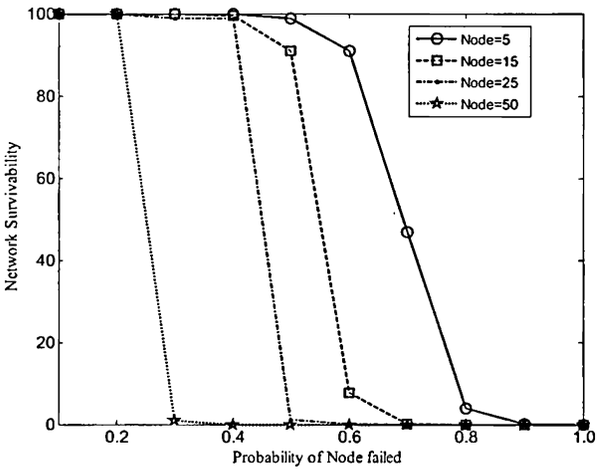


Figure 3 : Effect on survivability of probability of failed node (P_{N_f})

Conclusion

In this paper, we developed an analytical model to study the impact of correlated node behavior on network survivability, which is defined as the probabilistic k-correlated of the network. We derived the approximation of the network survivability by using an edge connectivity function ω. As a conclusion, the impact of node behaviors on network survivability can be evaluated probabilistically from equation (10) which can be further used as a guideline to design or deploy a survivable of wireless ad hoc network given a predefined survivability preference.

Acknowledgments

A.H.Azni would like to thank Universiti Sains Islam Malaysia (USIM) and Ministry of Higher Education (MOHE) for financial support throughout her studies in Universiti Teknikal Melaka Malaysia (UTEM), Melaka, Malaysia.

References:

Azni, A. H., Ahmad, R., Azri, Z., Noh, M., Samad, A., Basari, H., & Hussin, B. (2012). Correlated Node Behavior Model based on Semi Markov Process for MANETS. *International Journal of Computer Science Issues (IJCSI), 9*(1).

Bakkaloglu, M. (2002). *On correlated failures in survivable storage systems. Information Systems.* Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA461303

Dai, Y., & Xie, M. (2005). Modeling and analysis of correlated software failures of multiple types. *Reliability, IEEE Transactions on, 54*(1), 100-106. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1402688

Komathy, K., & Narayanasamy, P. (2007). A Probabilistic Behavioral Model for Selfish Neighbors in a Wireless Ad Hoc Network. *IJCSNS, 7*(7), 77. Retrieved from http://paper.ijcsns.org/07_book/200707/20070710.pdf

Lima, M. N., da Silva, H. W., dos Santos, A. L., & Pujolle, G. (2008). An architecture for survivable mesh networking. *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE* (Vol. 6, pp. 1–5). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4697913

Lima, M., dos Santos, A., & Pujolle, G. (2009). A survey of survivability in mobile ad hoc networks. *IEEE Communications Surveys & Tutorials*, *11*(1), 66-77. doi:10.1109/SURV.2009.090106

Nath, S., Yu, H., Gibbons, P. B., & Seshan, S. (2004). Tolerating correlated failures in wide-area monitoring services. *Submitted for publication.* Retrieved from http://www.intel-research.net/Publications/Pittsburgh/101220041252_263.pdf

Neumayer, S., & Modiano, E. (2010). Network Reliability With Geographically Correlated Failures. *2010 Proceedings IEEE INFOCOM*, 1-9. Ieee. doi:10.1109/INFCOM.2010.5461984

Ning, N., & Yang, B. (n.d.). Software Reliability Models Based on Markov Renewal Process 2 Software Reliability Modeling Framework Considering Failure Correlation. *Science And Technology*, 1-9.

Thanakornworakij, T., Nassar, R., Leangsuksun, C. B., & Paun, M. (2011). The Effect of Correlated Failure on the Reliability of HPC Systems. *2011 IEEE Ninth International Symposium on Parallel and Distributed Processing with Applications Workshops*, 284-288. Ieee. doi:10.1109/ISPAW.2011.55

Xing, F. (2009). *Modeling, Design, and Analysis on the Resilience of Large-scale Wireless Multi-hop Networks. Communication.* University of North Carolina. Retrieved from http://repository.lib.ncsu.edu/ir/handle/1840.16/4329

Xing, F. (2010). On the survivability of wireless ad hoc networks with node misbehaviors and failures. *Secure Computing, IEEE Transactions on*, *7*(3), 284-299. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4674373

Xing, F., & Wang, W. (2006). Modeling and analysis of connectivity in mobile ad hoc networks with misbehaving nodes. *IEEE International Conference on Communications, 2006* (Vol. 4, pp. 1879–1884). IEEE. doi:10.1109/ICC.2006.254994

A KNOWLEDGE ENCRYPTION SCHEME WITH EXACT LABEL SEARCH

MoesfaSoeheila Mohamad and Geong Sen Poh
MIMOS Berhad
soeheila.mohamad@mimos.my, gspoh@mimos.my

Abstract:

This work presents two searchable encryption schemes for knowledge which utilize symmetric encryption. The knowledge is representedbyconceptualgraphs. With this scheme a user can store his/her knowledge in encrypted form on a remote storage. Parts of the knowledge can be extracted when queried by the user in such a way that the storage cannot obtain any information about the knowledge. We show that both schemes achieve (L_1,L_2)-security under CQA2.

Introduction

The main concern in utilizing a storage facility owned and handled by a third party is the confidentiality of the data. In order to ensure confidentiality is to have an encryption method which does not require decryption of the whole data during search for parts of the stored encrypted data [Song, Wagner, Perrig]. These methods are called searchable encryption schemes. Many searchable encryption schemes have been proposed for textual data with keyword search. An improvement in security is made when Goh introduced secure indexes [Goh]. Goh also defines non-adaptive and adaptive semantic security for SSE.Then, Curtmola et al.generalize the definition of symmetric searchable encryption (SSE) for any data structure in [Curtmola,Garay,Kamara,Ostrovsky]. In addition, the authors defined a better security model for SSE.

In [Chase, Kamara] the SSE was extended to schemes for matrices, labeled data and graphs. These schemes are categorized as private-key structured encryption $\Sigma = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Token}, \mathbf{Query_e}, \mathbf{Dec})$ [Chase, Kamara; Definition 4.1]. In the same paper a new security model is proposed, namely $(\mathcal{L}_1, \mathcal{L}_2)$-security under adaptive chosen query attack (CQA2).

Security of SSE

When discussing the security of SSE, the adversary is an entity in or has access to the storage including the storage provider. The adversary can view what is in the storage and may deduce some information about the unencrypted data $(\delta, \mathbf{m})$.In [Chase,Kamara] the authors label the information leaked by the ciphertexts $(\gamma, \mathbf{c})$as $\mathcal{L}_1$, and the information leaked by the tokens$(\tau_i)_i$in a sequence of queries$(q_i)_i$as $\mathcal{L}_2$.An SSE scheme achieves$(\mathcal{L}_1, \mathcal{L}_2)$-security[Chase,Kamara] when both of the following hold.

- Given an encrypted data structure γ and a sequence of ciphertexts $\mathbf{c}$, an adversary cannot learn any partial information about $\mathbf{m}$besides $\mathcal{L}_1(\delta, \mathbf{m})$.
- Given a sequence of tokens for a sequence of queries, an adversary cannot learn any partial information about either $\mathbf{m}$ or q besides $\mathcal{L}_2(\delta, q)$ and what is revealed by the semi-private data $\mathbf{v}_l$.

Security of an SSE scheme is proven by defining the simulator $\mathcal{S}$ for the game$\boldsymbol{Sim}_{\Sigma,\mathcal{A},\mathcal{S}}(k)$ so that output of the game is indistinguishable from output of $\boldsymbol{Real}_{\Sigma,\mathcal{A}}(k)$.

The game$\boldsymbol{Real}_{\Sigma,\mathcal{A}}(k)$ proceeds as follows.

1. The adversary $\mathcal{A}$ generate data $(\delta, \mathbf{M})$ where $\mathbf{M} = (\mathbf{m}, \mathbf{v})$with$\mathbf{m} = (m_1, m_2, \ldots, m_t)$and $\mathbf{v} = (v_1, v_2, \ldots, v_t)$. The data $(\delta, \mathbf{M})$ is given to the user.
2. The userruns $\mathbf{Gen}(1^k)$ to generate a key K, and then encrypts the data $\mathbf{Enc}(K, \delta, \mathbf{M})$ to output $(\gamma, \mathbf{c})$ which is given to $\mathcal{A}$.
3. $\mathcal{A}$chooses a query q_0 and submit to the user.
4. The userreturns thetoken $\tau_0 = \mathbf{Token}(K, q_0)$.
5. For t=1,…,$p(k)$ where $p(.)$ is a polynomial
    a. Based on previous queries,$\mathcal{A}$ chooses query q_t.
    b. The user returns the corresponding token $\tau_t = \mathbf{Token}(K, q_t)$.
6. $\mathcal{A}$gives$\gamma, \mathbf{c}, \langle(q_t)_{t=1,\ldots,p(k)}\rangle, \langle(\tau_t)_{t=1,\ldots,p(k)}\rangle$to the distinguisher $\mathcal{D}$.
7. $\mathcal{D}\big(\gamma, \mathbf{c}, \langle(q_t)_{t=1,\ldots,p(k)}\rangle, \langle(\tau_t)_{t=1,\ldots,p(k)}\rangle\big)$returns a bit b.
8. $\mathcal{A}$outputs b.

In thegame $\boldsymbol{Sim}_{\Sigma,\mathcal{A},\mathcal{S}}(k)$, the adversary interacts with the simulator $\mathcal{S}$ as follows.

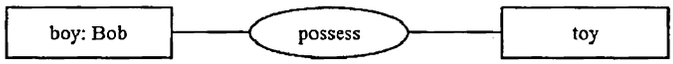
1. The adversary $\mathcal{A}$ generates data $(\delta, \mathbf{M})$ where $\mathbf{M} = (\mathbf{m}, \mathbf{v})$ with $\mathbf{m} = (m_1, m_2, \ldots, m_t)$and $\mathbf{v} = (v_1, v_2, \ldots, v_t)$.
2. The simulator $\mathcal{S}$ is given $\mathcal{L}_1(\delta, \mathbf{M})$.
3. $\mathcal{S}$generates$(\tilde{\gamma}, \tilde{\mathbf{c}})$ and gives it to $\mathcal{A}$.
4. $\mathcal{A}$chooses a query q_0.
5. $\mathcal{S}$is given $\left(\mathcal{L}_2(\delta, q_0), \mathbf{v}_{I_0}\right)$ for the query.
6. $\mathcal{S}$returns a token $\tilde{\tau}_0$.
7. For t=1,…,$p(k)$ where $p(.)$ is a polynomial.
   a. Based on previous queries$\mathcal{A}$ chooses query q_t.
   b. $\mathcal{S}$is given $\left(\mathcal{L}_2(\delta, q_i), \mathbf{v}_{I_t}\right)$.
   c. $\mathcal{S}$returns the corresponding token $\tilde{\tau}_t$.
8. $\mathcal{A}$gives$\tilde{\gamma}, \tilde{\mathbf{c}}, \langle(q_t)_{t=1,\ldots,p(k)}\rangle, \langle(\tilde{\tau}_t)_{t=1,\ldots,p(k)}\rangle$ to the distinguisher $\mathcal{D}$.
9. $\mathcal{D}\left(\tilde{\gamma}, \tilde{\mathbf{c}}, \langle(q_t)_{t=1,\ldots,p(k)}\rangle, \langle(\tilde{\tau}_t)_{t=1,\ldots,p(k)}\rangle\right)$returns a bit b.
10. $\mathcal{A}$outputs b.

We say that the SSE is $(\mathcal{L}_1, \mathcal{L}_2)$-secure under CQA2 if for all polynomial-time adversary $\mathcal{A}$, there exists a simulator $\mathcal{S}$ such that the distributions of the distinguisher's output given the two games results are computationally the same. In symbols, $\left|Pr\left[\boldsymbol{Real}_{\Sigma,\mathcal{A}}(k) = 1\right] - Pr\left[\boldsymbol{Sim}_{\Sigma,\mathcal{A},\mathcal{S}}(k) = 1\right]\right| \leq negl(k)$.

Under the CQA2 attack model the adversary is allowed to make a sequence of search queries to the challenger. In return the adversary will be given the corresponding token. The adversary makes the queries based on the tokens it obtains from the previous query in such a way that it will be able to derive more information regarding the stored data.

Conceptual Graph

In this work, knowledge is represented by conceptual graph.Conceptual graphs (CG) are undirectedgraphs in which each node may have more than one edges attached to it.There are two types of nodes in CGs, namely concept nodes and relation nodes. In addition, every edge always connects nodes of different types. The CGs may be partially compared, and the relation is called homomorphism. The formal definition of CGs and homomorphism of CGs is presented in [Chien,Mugnier].



'boy'
rker.

Our Contributions

In this work, we define SSE schemeswhich are secure against CQA2 for knowledge represented by conceptual graphs. The scheme adopts the Label scheme from [Chase,Kamara] and for both schemes we adopt the same security model.

Scheme 1

This scheme deploys Labelfrom [Chase,Kamara] with a different data structure. Here a labeling L in $\mathcal{U}$ contains all binary relations between integers in $[n] = \{1,2,\cdots,n\}$ and CGs in the data. In particular, each CG is associated to indexes of CGs which are homomorphic to it. The labeling data structure L supports the operation **Search**: $\mathcal{U} \times \Gamma \rightarrow \wp[n], (L, g) \mapsto L(g) = \{i \in [n]: (i, g) \in L\}$. Note that our data structure does not have semi-private data.

Table 1 shows an example ofdata$\mathbf{m} = (g_1, g_2, \ldots, g_8)$. Here the labeling data structure L_g contains pairs like$(1, \{1,4,5\})$ which means g_1 is homomorphic to g_1, g_4andg_5.Check that$\mathbf{Search}(L_g, g_1) = \{1,4,5\}$.

Table 1: Example of a datamfor $n = 8$.

Index	**m**	g_{index} *homomorphic to*
1	g_1	$\{g_1, g_4, g_5\}$
2	g_2	$\{g_4, g_7\}$
3	g_3	$\{g_1\}$
4	g_4	$\{g_2, g_8\}$
5	g_5	$\{g_7\}$
6	g_6	$\{g_2, g_3, g_7\}$
7	g_7	$\{g_1, g_2, g_4, g_8\}$
8	g_8	$\{g_3\}$

Scheme1 consists of five algorithms, Scheme1 = **(Gen, Enc, Token, Query$_e$, Dec)** and they all are the same as defined for Label in [Chase,Kamara] except that semi-private data v is omitted.

Security of Scheme1

In Scheme1 the information leaked by the ciphertext is $\mathcal{L}_1(L, \mathbf{m}) = (|L|, n, l)$ where n is the number of CGs in the data and l is the maximum size of the CGs. From the construction, the number of entries in $\gamma = T$ is the number of CGs with at least one CG homomorphic to it, denoted by $|L|$. The information leaked by the token τ for a query, g_q, is $\mathcal{L}_2(L, g_q) = (|I|, \text{QP}(g_q), \text{IP}(g_q))$ where $|I|$ denotes the size of the index list in the query result.

Theorem 1: If $F_K(\cdot)$and$H_K(\cdot)$ are pseudo-random and the symmetric encryption Π is CPA secure, then the Scheme1 is $(\mathcal{L}_1, \mathcal{L}_2)$-secure under CQA2 where $\mathcal{L}_1(L, \mathbf{M}) = (|L|, n, l)$ and is $\mathcal{L}_2(L, g_q) = (|I|, \text{QP}(g_q), \text{IP}(g_q))$.

Proof Sketch
Consider a simulator $\mathcal{S}$ defined here. When given $\mathcal{L}_1(L, \Gamma)$, $\mathcal{S}$ does the following steps.

1. Generate a key $K_{S3} = \Pi.\mathbf{Gen}(1^k)$.
2. Generate n random pairs (κ, s) to construct $\tilde{\gamma}$.
3. Compute n ciphertexts $c_i := \Pi.\mathbf{Enc}(K_3, 0^l)$and construct $\tilde{\mathbf{c}} = (c_1, c_2, \cdots, c_n)$.

Then, for each queryg_q made by the adversary A,$\mathcal{S}$ receives$\mathcal{L}_2(L, g_q)$ and performs the following.

1. Check $\text{QP}(g_q)$ whether the query has been submitted before.
2. If the query has been submitted previously, output the same token as before.
   If the query is new, there are two cases, either $|I| = 0$or $|I| \neq 0$.
3. If $|I| = 0$, choose a random search key κ which is not in $\tilde{\gamma}$, one random value r. Output token$\tau = (r, \kappa)$.
4. If $|I| \neq 0$, check $\text{IP}(g_q)$ to determine list of items$(j_x)_x$ accessed by current query which has been accessed by previous queries. Include all of the $j_x$in J.
5. If there is no item in $\text{IP}(g_q)$or $|J| < |I|$, choose random indexes$j$and include in J until $|J| = |I|$.
6. Choose randomly an unused search key κin $\tilde{\gamma}$.
7. Extract$s = \tilde{\gamma}(\kappa)$ and compute $r = J \oplus s$.
8. Output token $\tau = (\kappa, r)$.

We argue that despite generating a dictionary without seeing the data, this simulator outputs tokens which produces the given$\mathcal{L}_2(L, g_q)$. Formally, with this simulator we achieve $\left|Pr[\boldsymbol{Real}_{\Sigma,\mathcal{A}}(k) = 1] - Pr[\boldsymbol{Ideal}_{\Sigma,\mathcal{A},\mathcal{S}}(k) = 1]\right| \leq negl(k)$ and hence Scheme 1 is $(\mathcal{L}_1, \mathcal{L}_2)$-secure under CQA2.

Scheme 2

Using Scheme2, a user can search the encrypted knowledge by words that are labels in the CGs nodes. Scheme2 combines Scheme1 and Label.

The knowledge is a set of CGs and is denoted as Γ. Scheme1 is used on Γ and denote the universeas$\mathcal{U}_G$. At another level in this scheme, define W to be the set of all concept and relation labels of CGs and use the Label scheme withM = Γ.Denote the universe defined under Label as$\mathcal{U}_W$ and the labelingasL_W. The operation supported is **Search:** $\mathcal{U}_W \times \mathrm{W} \rightarrow \wp[\Gamma]$ which takes as input a word w and a labelingin $\mathcal{U}_W$, and returns a set of CGs containing w and all CGs homomorphic to them.

Let Label be the scheme defined in Figure2 in [Chase,Kamara] and Scheme1 as defined above. We define Scheme2 = **(Gen, Enc, Token, Query$_e$, Dec)** by the following five algorithms.

$K \leftarrow \mathbf{Gen}(1^k)$:

1. Generate K_{S1} = Scheme1.**Gen**(1^k).
2. Generate K_L = Label.**Gen**(1^k).
3. Set $K := (K_{S1}, K_L)$.

$(\gamma, \mathbf{c}) \leftarrow \mathbf{Enc}(K, L_G, \Gamma)$:

1. Set $(T^G, \mathbf{c}^G) = Scheme1.\mathbf{Enc}(K_{S1}, L_G, \Gamma)$.
2. For each $g_i \in \Gamma$ such that $L_G(g_i) \neq \emptyset$, compute τ_i = Scheme1.**Token**(L, g_i).
3. From Γ generate labeling $L_W \in \mathcal{U}_W$.
4. For each $w \in$ W such that $L_W(w) \neq \emptyset$, set $m_i = L_W(w)$ and $v_i = (\tau_j)_{j \in L_W(w_i)}$.
5. Compute $(T^W, \mathbf{c}^W)$ = Label.**Enc**$(K_L, L_W, (\mathbf{m}, \mathbf{v}))$.
6. Output $\gamma = (T^G, T^W), \mathbf{c} = (\mathbf{c}^G, \mathbf{c}^W)$.

$\tau \leftarrow \mathbf{Token}(K, w)$:

1. Compute and output τ = Label.**Token**(w).

$(\mathrm{J}, \mathbf{v}_I) \leftarrow \mathbf{Search}(\gamma, \tau)$:

1. Parse γ as $(\mathrm{T^W}, \mathrm{T^G})$.
2. Get $(J, \mathbf{v}_I)$ = Label.**Search**(T^W, τ).
3. If $J \neq \emptyset$,for $j_i \in J$, computeJ_i = Scheme1.***Search***(T^G, v_i).
   Otherwise, set $\tilde{J} = \emptyset$.
4. Output $\tilde{J} = \langle (j_i, J_i)_{i \in I} \rangle$.

$m_j \leftarrow \mathbf{Dec}(K, c_j^G)$:

1. Output $g_j := \Pi.\mathbf{Dec}(K_{S1}, c_j^G)$.

Security of Scheme 2

Since Scheme2 effectively is a combination of two SSEs, its security is discussed by considering the leaks by the two SSE within the encryption and search algorithms. The following games are defined to consider the leak in two stages.

Game 0:

1. The challenger generates key $K = (K_{S1}, K_L)$.
2. The adversary generates data L_G, Γ.
3. The challenger computes $Scheme2.\mathbf{Enc}(K, L_G, \Gamma)$ and gives the adversary the ciphertext, $\gamma = (T^G, T^W), \mathbf{c} = (\mathbf{c}^G, \mathbf{c}^W)$.
4. Adversary make adaptive queries and for each query the challenger returns a token $\tau = Label.\mathbf{Token}(w)$.
5. The adversary outputs the experiment result.

Game1:

Let $\mathcal{S}^{Label}$ be the simulator as described in the proof of Theorem 5.2 in [Chase,Kamara].

1. The challenger generates key $K = (K_{S1}, K_L)$.
2. The adversary generates data L_G, Γ.
3. The challenger prepares $(\mathbf{m}, \mathbf{v})$.

4. The simulator $\mathcal{S}^{Label}$ is given $\mathcal{L}_1^{label}(L_W, (\mathbf{m}, \mathbf{v}))$.
5. $\mathcal{S}^{Label}$generates ciphertext $(\tilde{T}^W, \tilde{\mathbf{c}}^W)$.
6. The challenger computes $(T^G, \mathbf{c}^G) = Scheme1.\mathbf{Enc}(K_{S1}, L_G, \Gamma)$.
7. The adversary is given the ciphertext $(\tilde{T}^W, T^G, \tilde{\mathbf{c}}^W, \mathbf{c}^G)$.
8. The adversary makes polynomially many queries.
9. For each query w, the simulator $\mathcal{S}^{Label}$ is given $(\mathcal{L}_2^{Label}(L_G, \Gamma), \mathbf{v}_I)$ where $(I, \mathbf{v}_I) = \text{Label.}\mathbf{Search}(\text{T}^W, \tau)$ and $\tau = \text{Label.}\mathbf{Token}(w)$.
10. $\mathcal{S}^{Label}$generates a token $\tilde{\tau}$ and return to the adversary.
11. The adversary outputs the experiment result.

Theorem 2: If there exists an adversary $\mathcal{A}$ which makes Game1 and Game0 distinguishable, then there exists an adversary $\mathcal{B}$ which breaks the $(\mathcal{L}_1, \mathcal{L}_2)$-security of Label under CQA2.

Proof
Assume that there exists an adversary A which makes Game0 and Game1 distinguishable. Here we define the adversary B who plays game $\boldsymbol{Real}_{\text{Label},\mathcal{B}}(k)$ and $\boldsymbol{Ideal}_{\text{Label},\mathcal{B},\mathcal{S}^{Label}}(k)$ while interacting with A to use A's adaptive queries. In A's perspective it is playing Game0 and Game1 respectively with B being the challenger.

When B receives data from A, B does the following.
1. B gives $(L_W, (\mathbf{m}, \mathbf{v}))$ to the challenger.
2. B receives ciphertext $(T^W, \mathbf{c}^W) = Label.\mathbf{Enc}(K_L, L_W, (\mathbf{m}, \mathbf{v}))$ in $\boldsymbol{Real}_{\text{Label},\mathcal{B}}(k)$ or $(T^W, \mathbf{c}^W) = \mathcal{S}^{Label}\left(\mathcal{L}_1^{Label}(L_W, (\mathbf{m}, \mathbf{v}))\right)$in $\boldsymbol{Ideal}_{\text{Label},\mathcal{B},\mathcal{S}^{Label}}(k)$.
3. B gives A the complete ciphertext $(T^W, T^G, \mathbf{c}^W, \mathbf{c}^G)$.

For each query w received from A, B does the following.
4. B submits$w$ to the challenger and obtains $\tau = \text{Label.}\mathbf{Token}(w)$ in $\boldsymbol{Real}_{\text{Label},\mathcal{B}}(k)$or $\tau = \mathcal{S}^{Label}(\mathcal{L}_2^{Label}(L_G, \Gamma), \mathbf{v}_I)$in $\boldsymbol{Ideal}_{\text{Label},\mathcal{B},\mathcal{S}^{Label}}(k)$.
5. B forwards the token to A.
6. B outputs the output of A.

Since B uses the adaptive queries from A which makes Game0 and Game1 distinguishable, the games $\boldsymbol{Real}_{\text{Label},\mathcal{B}}(k)$ and $\boldsymbol{Ideal}_{\text{Label},\mathcal{B},\mathcal{S}^{Label}}(k)$ is also distinguishable. This means that Scheme1 does not have $(\mathcal{L}_1, \mathcal{L}_2)$-security under CQA2.■

Game2:
Let $\mathcal{S}^{Label}$ be as in Game1.
1. The challenger generates key $K = (K_{S1}, K_L)$.
2. The adversary generates data L_G, Γ.
3. The challenger computes $Scheme2.\mathbf{Enc}(K, L_G, \Gamma)$ with the following change:
   a. Steps 2 and 3 are omitted.
   b. Step 4 is replaced by: The simulator$\mathcal{S}^{Label}$ is given $\mathcal{L}_1^{label}(L_W, (\mathbf{m}, \mathbf{v}))$ and returns $(\tilde{T}^W, \tilde{\mathbf{c}}^W)$.
4. The adversary is given $(\tilde{T}^W, T^G, \tilde{\mathbf{c}}^W, \mathbf{c}^G)$.
5. For every query $w$submitted by the adversary, the challenger computes $\tau_i = \text{Scheme1.}\mathbf{Token}(K_{S1}, g_i)$for each $i \in L_W(w)$. Set $\mathbf{v} = (\tau_i)_{i \in L_W(w)}$.
6. $\mathcal{S}^{Label}$is given$(\mathcal{L}_2^{Label}(L_G, \Gamma), \mathbf{v})$ and returns $\tilde{\tau}$ to the adversary.
7. The adversary outputs the distinguisher experiment result.

Game3 :
Let $\mathcal{S}^{Label}$ be as in Game1 and $\mathcal{S}^{Scheme1}$ be the simulator defined in the proof of Theorem 1.
1. The challenger generates key $K = (K_{S1}, K_L)$.
2. The adversary generates data L_G, Γ.
3. The challenger computes $Scheme2.\mathbf{Enc}(K, L_G, \Gamma)$ with the following change:
   a. Step 1 is replaced by: The simulator $\mathcal{S}^{Scheme1}$ is given $\mathcal{L}_1^{scheme1}(L_G, \Gamma)$ and returns $(\tilde{T}^G, \tilde{\mathbf{c}}^G)$.
   b. Steps 2 and 3 are omitted.

c. Step 4 is replaced by: The simulator $\mathcal{S}^{Label}$ is given $\mathcal{L}_1^{label}(L_W, (\mathbf{m}, \mathbf{v}))$ and returns $(\tilde{T}^W, \tilde{\mathbf{c}}^W)$.

4. The adversary is given the ciphertext $(\tilde{T}^W, \tilde{T}^G, \tilde{\mathbf{c}}^W, \tilde{\mathbf{c}}^G)$.
5. For every query w the adversary makes to challenger, $\mathcal{S}^{Scheme1}$ is given $\mathcal{L}_2^{Scheme1}(L_G, g_i)$ for each $i \in L^W(w)$ and returns $\tilde{\mathbf{v}} = (\tilde{\tau}_i)_{i \in L^W(w)}$ to the challenger where $\tau_i = \mathcal{S}^{Scheme1}\left(\mathcal{L}_2^{Scheme1}(L_G, g_i)\right)$.
6. $\mathcal{S}^{Label}$ is given $(\mathcal{L}_2^{label}(L_W, w), \tilde{\mathbf{v}})$ and returns $\tilde{\tau} = \mathcal{S}^{Label}(\mathcal{L}_2^{label}(L_W, w), \tilde{\mathbf{v}})$ to the adversary.
7. The adversary outputs the distinguisher experiment result.

Theorem 3: If there exists an adversary A which makes Game2 and Game3 distinguishable, then there exists an adversary B which breaks the $(\mathcal{L}_1, \mathcal{L}_2)$-security of Scheme1 under CQA2.

The proof for Theorem 3 uses the same strategy as the proof for Theorem 2. The proof is omitted here because of space constraint.

Since it has been proven that Label and Scheme1 are $(\mathcal{L}_1, \mathcal{L}_2)$-secure under CQA2, we conclude from Theorem 2 and Theorem 3 that Scheme2 is also $(\mathcal{L}_1, \mathcal{L}_2)$-secure under CQA2.

Conclusion

We have presented SSEs for knowledge represented by CGs and showed that the scheme achieves $(\mathcal{L}_1, \mathcal{L}_2)$-security under CQA2.The first SSE, Scheme1, allows search by a CG which returns a set of CGs homomorphic to the query CG. The second SSE, Scheme2, allows search by a concept or relation label. The search result includes CGs containing the query label and CGs homomorphic to those CGs. This work should be extended to enable search on encrypted knowledge by any CG.

References:

Chase, M, Kamara, S (2010). Structured encryption and controlled disclosure. *Advances in Cryptology – ASIACRYPT 2010*, LNCS 6477, 577-594.

Chien, M, Mugnier M-L, (2009). Graph-based knowledge representation: Computational Foundations of conceptual graphs. *Advanced Information and Knowledge Processing Series, Springer-Verlag London Limited.*

Curtmola, R, Garay, J.A, Kamara, S, Ostrovsky, R, (2006). Searchable symmetric encryption: Improved definitions and efficient constructions. *ACM Conference on Computer and Communications Security*, 79-88.

Goh, E (2003). Secure indexes. *Cryptology ePrint Archive*, 2003/216, http://eprint.iacr.org/2003/216/.

Song, D.X, Wagner, D, Perrig, A, (2000).Practical techniques for searches on encrypted data.*Proceedings of the 2000 IEEE Symposium on Security and Privacy (SP'00)*, 44-55.

ANALYSIS OF THE LBLOCK LIGHTWEIGHT BLOCK CIPHER

Iskandar Bahari[1] and Muhammad Reza Z'aba[2]
Cryptography Lab, Advanced Analysis and Modeling (ADAM) Cluster,
MIMOS Berhad, Kuala Lumpur, Malaysia
[1]iskandar.bahari@mimos.my, [2]reza.zaba@mimos.my

Abstract:

This paper presents algebraic analysis on the LBlock lightweight block cipher proposed in ACNS 2011.The cipher is intended for use in resource-constrained devices such as RFID tags. The structure of the cipher is based on the Feistel scheme, which is used by the Data Encryption Standard (DES). In the specification of LBlock, no analysis on its resistance to algebraic attacks is given. This paper is a first attempt at evaluating the strength of LBlock against algebraic attacks. We use Gröebner Basis computations to attempt to solve the system of equations that describe LBlock.

Introduction

Lightweight block cipher has gained a lot of attention by the cryptographic community. These ciphers need to be able to provide confidentiality with adequate security in resource-constrained devices. Such devices may have limited memory, storage, implementation area and power. Numerous lightweight block ciphers have been proposed since 2006 such as HIGHT (Hong et al, 2006), PRESENT (Bogdanov et al, 2007), KATAN, KTANTAN (De Cannière, Dunkelman and Knezevic, 2009), PRINTcipher (Knudsen et al, 2010), LED (Guo et al, 2011), EPCBC (Yap et al, 2011) and recently, LBlock (Wu and Zhang, 2011).

Cryptanalysis is the most important step in the design and analysis of block ciphers. Every new block cipher nowadays has to show resistance to at least differential and linear cryptanalysis. There are also variants of these two cryptanalysis such as impossible differential, boomerang, rectangle and differential-linear cryptanalysis. Other advanced cryptanalysis includes algebraic and side-channel cryptanalysis. Basically, algebraic cryptanalysis is a known plaintext attack that investigates the mathematical relationship between bits of the plaintext, ciphertext, secret key and intermediate states of the block cipher.

As far as we know, the only cryptanalysis on LBlock so far is done by the designers. They have shown the resistance of LBlock against differential, linear, impossible differential, integral and related-key cryptanalysis. No analysis however, was done on its resistance to algebraic attacks. This paper is a first attempt at evaluating the strength of LBlock against algebraic attacks.

This paper is organized as follows. The first section describes the specification of LBlock. The analysis of LBlock with respect to algebraic analysis is given in the second section. The last section summarizes and concludes the paper.

Specification of LBlock

The block cipher LBlock accepts a 64-bit plaintext block and an 80-bit secret master key. The cipher uses the Feistel structure and has 32 rounds. Let $X = X_1 || X_0$ denote the plaintext block which consists of the concatenation of two 32-bit words X_i. For encryption, the plaintext block is processed as follows for $i = 2, 3, \ldots, 33$:

$$X_i = F(X_{i-1}, K_{i-1}) \oplus (X_{i-2} \lll 8)$$

where$F$ is the round function and$\lll$ denotesrotation to the left. The 64-bit ciphertext block is denoted by $X_{32} || X_{33}$. For decryption, the right rotation is replaced by rotation to the right.

The round function F is defined as follows where the functions S and P will be described later.

$$F(X_i, K_i) = P(S(X_i \oplus K_i)$$

The function S is a nonlinear transformation that consists of 8 different 4 × 4(i.e. 4-bit input and 4-bit output) S-boxess_j applied in parallel to its input where $j = \{0, 1, \ldots, 7\}$.The function P is a linear transformation that permutes its input to produce the output. Figure 1 shows a pictorial view of the encryption structure and the round function F.

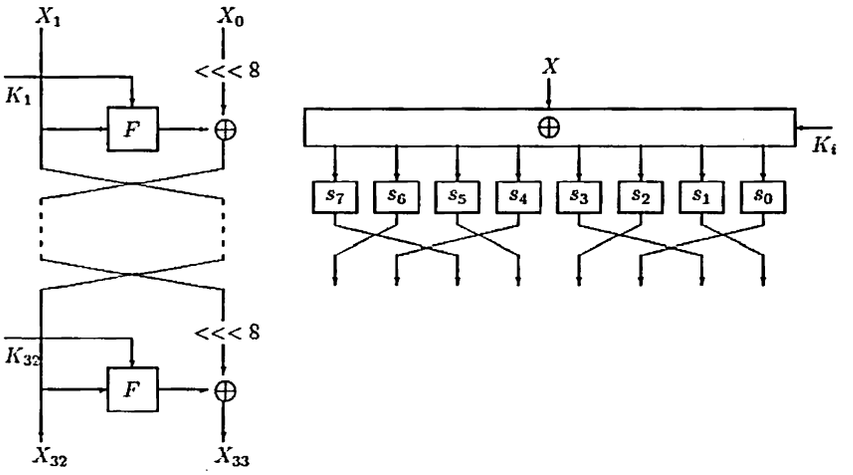


Figure 1: Encryption structure (left) and details of the round function F (right) of LBlock (Wu and Zhang, 2011)

The 80-bit secret master key is processed as follows. Let $K = k_{79}||\, k_{78}\, ||\, \ldots\, ||\, k_0$ denote the 80-bit master key and let K_i denote the round subkey in round i. Then, for $i = 1, 2, \ldots, 31$, repeat the following steps:
Step 1: Rotate the current state of K 29 bits to the left: $K \lll 29$
Step 2: Apply the S-box s_9 and s_8 to bits 79 to 76 and 75 to 72, respectively:

$$k_{79}||\, k_{78}\, ||k_{77}||\, k_{76} = s_9(k_{79}||\, k_{78}\, ||k_{77}||\, k_{76});$$
$$k_{75}||\, k_{74}\, ||k_{73}||\, k_{72} = s_8(k_{75}||\, k_{74}\, ||k_{73}||\, k_{72})$$

Step 3: XOR bits 50 to 46 with the binary representation of the counter i.
Step 4: Output the leftmost 32-bit of the current state of K as the round subkey $K_i = k_{79}||\, k_{78}\, ||\, \ldots\, ||\, k_{48}$

Analysis

Equation system for LBlock

Every function can be represented as a system of equations. The most straightforward way of constructing a system of equations for a block cipher is to derive equations for each individual component and to insert them in a single system (Biryukov and De Canniere, 2003). From the structure of the LBlock, a system of equations can be formed based on the components of the function F.

Linear layers: Similar to any other block cipher, the linear layers of LBlock consist of linear diffusion layers, P and key additions. Writing a system of equations for these layers is very straightforward. Such a linear system will never change the number of equations and the number of terms in the system. In cases

where a linear layer only consists of bit permutations, no separate equations were introduced but we renamed the variables accordingly.

Nonlinear Layers: The main structure of the equation system describing the LBlock was coming from nonlinear transformation function, S which will be the main obstacle that prevents the system from being easily solved. It is actually an S-Box that can be described by a set of polynomials by expressing each output bits in terms of the inputs. Similar to many S-boxes, LBlock is also derived from simple algebraic functions, and this directly leads to simple polynomial systems. Thus, we can easily translate the S-Box into a system of equation by deriving its Algebraic Normal Form (ANF). ANF provides a useful representation of the Boolean function in term of a unique XOR sum of AND products of the input variables (Fuller, 2003). For an $n \times n$ S-box, the highest degree of the ANF is $n - 1$.

In the case of LBlock, the highest degree of the ANF is 3. However, we cannot guarantee that these systems are optimal.

The number of equations and variables for every iteration of LBlock are summarized and shown in Table 1. It is shown that the number of equations and variables in the system rise by 32 and 64 respectively in every new iteration.

Table 1: Number of equations and variables for each iteration of LBlock

Iteration	Equations	Variables
1	32	96
2	64	160
3	96	224
4	128	288
5	160	352
6	192	416
7	224	480
8	256	544
9	288	608
10	320	672
11	352	736
12	384	800
13	416	864
14	448	928
15	480	992
16	512	1056

Iteration	Equations	Variables
17	576	1120
18	608	1184
19	640	1248
20	672	1312
21	704	1376
22	736	1440
23	768	1504
24	800	1568
25	832	1632
26	864	1696
27	896	1760
28	928	1824
29	960	1888
30	992	1952
31	1024	2016
32	1056	2080

Experiment

This section presents the experimental steps and results from the analysis on equation system describing the LBlock. Given the system of equations generated from the ANF, the Gröebner Basis computations method was used to transform the system into a new, simpler and solvable system of equations which once solved, recovers the secret key. The computations were performed using SAGE computational algebra package (William et. al., 2012) and also MAPLE 14 Mathematical package. It was implemented on a 64-bit 2.93 GHz Intel(R) Xeon(R) processor computer with 48 GB of RAM, running on WINDOWS 7 operating system.

The experiments were conducted in four steps. Firstly, we programmed the system of polynomial equations consisting of the LBlock keystream generation both in SAGE and MAPLE packages. Secondly, we provided the plaintext as well as the ciphertext values so that the only variables remained in the system were the keys we trying to solve for. We used single and two known plaintext methods in this experiment.

We then let the SAGE and MAPLE programs compute the corresponding polynomials ideal generated from the polynomials in the system.

Lastly, the Gröebner basis of the related polynomial ideal was computed. If a unique solution was found, Gröebner basis immediately give the solution to the original system.

Result and Discussions

Table 2 : Results using a single known plaintext

Number of rounds	SAGE			MAPLE 14		
	Number of Equations	Number of Variables	Time (in seconds)	Number of Equations	Number of Variables	Time (in seconds)
1	96	96	0.0160	96	96	0.0324
2	192	192	0.7600	192	192	0.2181
3	288	320	2.2761	288	320	3.5260
4	384	448	9.0006	384	448	12.5231
5	480	576	994.7022 (16.58 minutes)	480	576	n/a
6	576	704	3032.4135 (50.54 minutes)	576	704	n/a

Table 3 : Results using two known plaintexts

Number of rounds	SAGE			MAPLE 14		
	Number of Equations	Number of Variables	Time (in seconds)	Number of Equations	Number of Variables	Time (in seconds)
1	192	160	0.0180	192	160	0.0780
2	384	320	0.2440	384	320	3.5410
3	576	544	5.2883	576	544	n/a
4	768	768	18.9851	768	768	n/a
5	960	992	1508.7222	960	992	n/a
6	1152	1216	n/a	1152	1216	n/a

Table 2 and Table 3 conclude the results of the experiment showing the time required to finding the solutions (keys) for the equation system arising from the LBlock using Gröebner basis computations. The time needed to compute the solutions in a single iteration was recorded to be very small in both programs. By constructing the equations over four iterations, MAPLE has exceeded the allocated data limit (4GB) and failed to compute the solutions for the system. The same case goes for the experiment with two known plaintexts, after the second iteration the datalimit was exceeded. However, SAGE has successfully break the system up to 6 iterations in single known plaintext and 5 iterations when two known plaintexts were used. After that, the times required to algebraically break the system using Gröebner basis for LBlock are non-feasible.

In another experiment using SAGE, in a single known plaintext scenario, we included the key scheduling in the existing system of equations. The experiments were performed for three or more rounds of LBlock. We did not include the key scheduling equations in the one- and two- rounds experiment because the number of equations is already the same as the number of variables. If we include the key equations, we would add degree 3 equations which may complicate the system. The degree 3 equations come from the S-box in the key scheduling algorithm. Furthermore, by not including the key scheduling algorithm, SAGE is able to compute the Gröebner basis for the system (refer to Table 2).

As mentioned earlier, we do not know for sure if the system of equations were optimal. So, we believe that the results can be improved if we managed to get a better system that is optimal for solving. We can also see that MAPLE 14 fails after very a few iterations. MAPLE program is very expensive in term of memory, so with the limited resources, MAPLE is not a good option for this experiment.

Conclusion and Future Work

This work intended to break the LBlock lightweight block cipher by using algebraic cryptanalysis. It was shown that LBlock can be algebraically represented by its ANF. Utilizing SAGE and MAPLE 14 computational package we tried to use Gröebner basis method to solve the system of equations describing the cipher. We managed to break the cipher up to 6 round at best with SAGE package while MAPLE performed less than expected.

Motivated by the results derived, we will continue this experiment to improve the output. There are a few strategies planned such as combining this algebraic method with other cryptanalysis methods, which we hope will improve the results.

References:

Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. *Advances in Cryptology – EUROCRYPT '99*, volume 1592 of Lecture Notes in Computer Science, pages 12–23. Springer-Verlag, 1999.

Eli Biham, Orr Dunkelman, and Nathan Keller. The Rectangle Attack – Rectangling the Serpent. *Advances in Cryptology – Eurocrypt 2001*, volume 2045 of Lecture Notes in Computer Science, pages 340–357. Springer-Verlag, 2001.

Eli Biham and Adi Shamir. Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag, 1993.

Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. *Cryptographic Hardware and Embedded Systems – CHES 2007*, volume 4727 of Lecture Notes in Computer Science, pages 450–466. Springer-Verlag, 2007.

Nicolas T. Courtois and Josef Pieprzyk. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. *Advances in Cryptology – ASIACRYPT 2002*, volume 2501 of Lecture Notes in Computer Science, pages 267–287. Springer-Verlag, 2002.

Christophe De Cannière, Orr Dunkelman, Miroslav Knezevic: KATAN and KTANTAN - A Family of Small and Efficient Hardware-Oriented Block Ciphers. *Cryptographic Hardware and Embedded System - CHES 2009*, volume 5747 of Lecture Notes in Computer Science, pages 272-288. Springer-Verlag, 2009.

Jian Guo, Thomas Peyrin, Axel Poschmann, Matthew J. B. Robshaw. The LED Block Cipher. *Cryptographic Hardware and Embedded Systems – CHES 2011*, volume 6917 of Lecture Notes in Computer Science, pages 326-341. Springer-Verlag, 2011.

Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bonseok Koo, Changhoon Lee, Donghoon Chang, Jaesang Lee, Kitae Jeong, Hyun Kim, Jongsung Kim, and Seongtaek Chee. HIGHT: A New Block Cipher Suitable for Low-Resource Device. *Cryptographic Hardware and Embedded Systems – CHES 2006*, volume 4249 of Lecture Notes in Computer Science, pages 46–59. Springer-Verlag, 2006.

Lars R. Knudsen, Gregor Leander, Axel Poschmann, Matthew J. B. Robshaw. PRINTcipher: A Block Cipher for IC-Printing. *Cryptographic Hardware and Embedded Systems – CHES 2010*, volume 6225 of Lecture Notes in Computer Science, pages 16-32. Springer-Verlag, 2010.

Langford, S.K., Hellman, M.E.: Differential-Linear Cryptanalysis. In: Desmedt, Y.G. (ed.) *CRYPTO 1994*. LNCS, vol. 839, pp. 17–25. Springer, Heidelberg (1994)

Mitsuru Matsui. Linear Cryptanalysis Method for DES Cipher. *Advances in Cryptology – EUROCRYPT '93*, volume 765 of Lecture Notes in Computer Science, pages 386–397. Springer-Verlag, 1994.

David Wagner. The Boomerang Attack. *Fast Software Encryption: FSE'99*, volume 1636 of Lecture Notes in Computer Science, pages 156–170. Springer-Verlag, 1999.

Wenling Wu, Lei Zhang: LBlock: A Lightweight Block Cipher. *Applied Cryptography and Network Security - ACNS 2011*, volume 6715 of Lecture Notes in Computer Science, pages 327-344. Springer-Verlag, 2011.

Huihui Yap, Khoongming Khoo, Axel Poschmann, Matt Henricksen: EPCBC - A Block Cipher Suitable for Electronic Product Code Encryption. *Cryptology and Network Security - CANS 2011*, volume 7092 of Lecture Notes in Computer Science, pages 76-97. Springer-Verlag, 2011.

Joanne Elizabeth Fuller. (2003). Analysis of Affine Equivalent Boolean Functions for Cryptography. *PhD Thesis, Queensland University of Technology.*

Alex Biryukov., Christophe De Canniere. (2005). Block Cipher and Systems of Quadratic Equations. *Fast Software Encryption, FSE 2003*, Lecture Notes in Computer Sciences 2887, T. Johansin (ed.), Springer-Verlag, pp. 274-289.

William A. Stein et al. (2012). Sage Mathematics Software (Version 4.8), The Sage Development Team, http://www.sagemath.org.

DES USER-FRIENDLY INTERFACE USING MAPLE

Rasidah Abdull Mutalip, Kamilah Abdullah, Nur Lina Abdullah, Norhidayah A. Kadir, Nor Hanimah Kamis and Mohd Nasruddin Mat Yusof
Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia
rasidah@tmsk.uitm.edu.my, kamilah@tmsk.uitm.edu.my, nurlina@tmsk.uitm.edu.my, norhidayah@tmsk.uitm.edu.my, norhanimah@tmsk.uitm.edu.my

Abstract:

This paper describes about the development of Data Encryption Standard (DES) user-friendly interface by using Maple. Maple is a powerful tool in explaining the cryptography concepts such as RSA Cryptosystem, Advanced Encryption Standard (AES) and Key Exchange – to name a few. In addition, DES is one of the cryptographic algorithm contains encryption and decryption process for the purpose of information security. This interface is found to be helpful in reducing the tediousness of calculations and assist students in teaching and learning process with better understanding. The implementation will be applied in the classroom as to create the interesting learning environment.

Introduction

Learning involves more than just receiving transmitted information (Carlson et al., 1996). The need of an interactive courseware as to promote student involvement nowadays is a must. Guzmán (2006), in his research stressed out the importance of interactive learning as the activity to promote learning but teachers must make clear that the tool are only an abstraction of the theoretical concept and full learning must be complemented as a mixture of both. Many articles describe an ongoing effort to develop a module for teaching and learning mathematics in universities by using Maple, Matlab, Mathematica and others. Maple is a mathematical software package that can be used to solve complex mathematical problems (Khouyibaba, 2010; Suanmali, 2008; McAndrew, 2008).

Suanmali (2008) presented the use of Maple as a multimedia tool in classrooms, particularly in mathematics and related science classes for undergraduate students. Interactive Maple sessions were employed in many classrooms such as in calculus, applications of abstract algebra, combinatorial, and linear algebra to determine the solutions in either numeric or symbolic form. In 2010, Kilicman et al. presented an interactive Maple worksheets and animated graphics for Linear Algebra courses. The utilization of Maple as one of the technology tool in classroom can strengthen students learning process by presenting content numerically, graphically and symbolically without extra burden of spending time to solve the complex computational problems by hand. Furthermore, they proved that the integration of technology can contribute significantly to student engagements, motivation, as well as attitude toward mathematical courses.

Many researches has been done to proved that Maple is a reliable and interactive software in understanding calculus, applications of abstract algebra, combinatorial, and linear algebra (Suanmali, 2008). Therefore, it is a motivation to develop a module for an advance mathematical subject such as Cryptography in order for students to see the use of Cryptography from being bogged down by the mathematics (Baliga and Boztas, 2001). McAndrew (2008) claimed that Maple is a powerful and full-featured commercial system in solving mathematical problem, including Cryptography rather than Mathematica.

Data Encryption Standard (DES) is one of the well known symmetric key cryptography (Schafer, 2003; Trappe & Washington, 2002; Forouzan, 2008). DES is a block cipher which was the modification from a project called Lucifer. DES was released on 1975 by the American National Bureau of Standards, today called as the National Institute of Standards and Technology (NIST). It is worth studying on DES because it represents a good example for symmetric key cryptography. DES is difficult to learn because the structure of DES and its algorithm are complicated. DES consists of many steps, procedures and components that have to be understood. The interactive learning module could be useful as an additional tool for usual lesson in the class. The interactive learning module usually applied through computer in providing a visualization of contents for better understanding (Schweitzer & Baird, 2006).

In this paper we intend to develop an interactive learning module for Data Encryption Standard (DES). The interactive learning module consists of notes and Maplet. The remainder of this paper is organized as follows. Phase

2 presents the DES structure and Maplet interface will be provided in Phase 3. Conclusion and recommendations are presented in Phase 4.

DES Structure

DES consists of round key generation process, encryption process, and decryption process.

Round key generation process

DES consists 16 rounds. Components that are required in this process are parity-bit drop (P56), shift bit and P48. In round key generation process, first, the 64-bit cipherkey will be going through P56 to remove the parity-bits. The 56-bit output then will be divided into two 28-bit parts which assigned as L0 and R0. Then, these L0 and R0 will enter round 1. In round 1, first, L0 and R0 will be going through Shift Bit and the outputs will become L1 and R1 respectively. These L1 and R1 then will be combined together before going through P48 to produce 48-bit output which become round key 1, K1. L1 and R1 from round 1 then will be taken to enter round 2. In round 2 until 15, same steps will be applied to produce round key 2 until round key 15 (K2, K3, K4, K5, K6, K7, K8, K9, K10, K11, K12, K13, K14, K15). In round 16, L15 and R15 from round 15 then will be going through Shift Bit to produce L16 and R16 respectively. Then, these L16 and R16 will be combined together before going through P48 to produce 48-bit output which become round key 16, K16. In round key generation process, 64-bit cipherkey will be taken to produce sixteen 48-bit round keys that will be used in both encryption and decryption process.

Encryption process

Components that are required in these encryption and decryption process are initial permutation (IP), expansion permutation (EP), exclusive (XOR) Operation, S-Box, Straight P-box (P32) and final permutation (FP).

In encryption process, 64-bit plaintext will be going through IP. The 64-bit output then will be divided into two 32-bit parts which assigned as L0 and R0. Then, these L0 and R0 will enter round 1. In round 1, R0 will be expanded through EP. The 48-bit output from EP then will be XORed with round key 1, K1 to produce another 48-bit output. The output then will be going through S-Box. The 32-bit output from S-Box then will be going through P32. The 32-bit output from P32 then will be XORed with L0 to produce new L0. These new L0 and R0 will enter through swapper to swap their position which assigned as L1 and R1 respectively (L1 = R0 & R1 = new L0). Then, these L1 and R1 will enter round 2. In round 2 until 15, same steps will be applied to produce L2 & R2, L3 & R3, L4 & R4, L5 & R5, L6 & R6, L7 & R7, L8 & R8, L9 & R9, L10 & R10, L11 & R11, L12 & R12, L13 & R13, L14 & R14, L15 & R15. The order of the round keys used is K2 until K15 respectively.

In round 16, R15 will be expanded through EP. The 48-bit output from EP then will be XORed with round key 16, K16 to produce another 48-bit output. The output then will be going through S-Box. The 32-bit output from S-Box then will be going through P32. The 32-bit output from P32 then will be XORed with L15 to produce new L15. These new L15 and R15 will be assigned as L16 and R16 respectively (L16 = new L15 & R16 = R15) because there is no swapper in round 16.

Then, these L16 and R16 will be combined together before going through final permutation (FP). The 64-bit output from FP then will become the ciphertext.

There will be sixteen rounds in this process. Each round will requires one round key generated from the round key generation process. Round 1 until 15 consists of mixer and swapper while round 16 only consist of mixer.

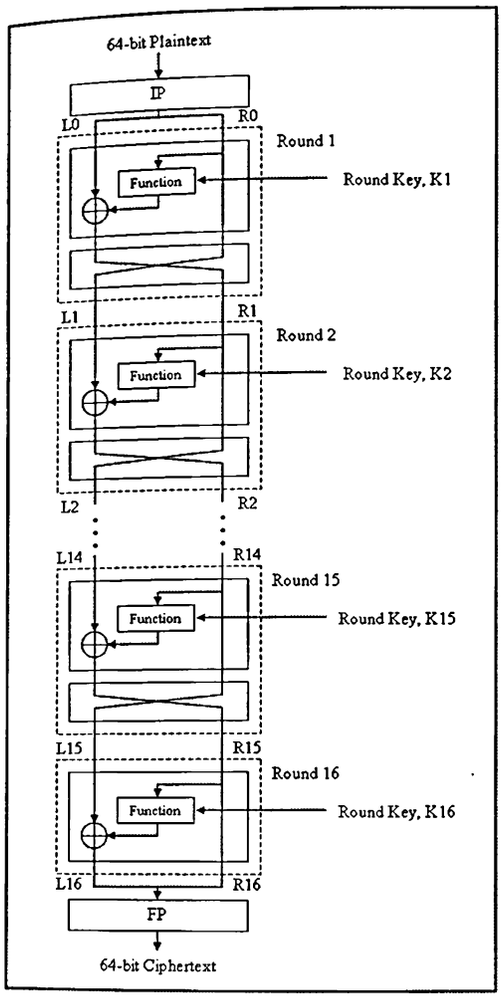


Figure 1: Encryption process of DES

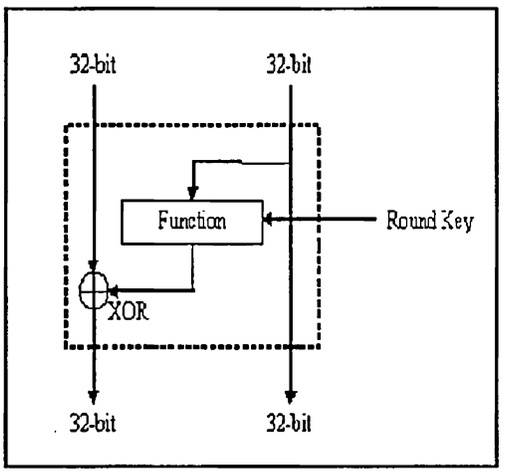


Figure 2: Process flow of mixer

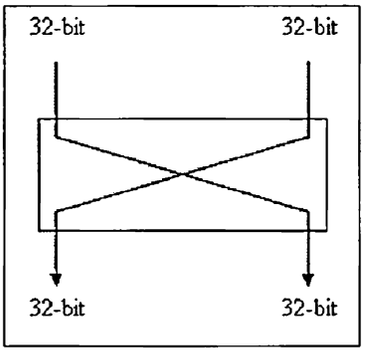


Figure 3: Process flow of swapper

Decryption Process

The flow in decryption process is similar to the flow in encryption process. The only difference between these two processes is the order of the round keys. In encryption process, K1 until K16 will be used in round 1 until round 16 respectively. However, in decryption process, reversed order, K16 until K1 will be used in round 1 until round 16 respectively.

Maplet Interface

Suppose the process in DES is done in binary (base-2 number system), inputs and outputs in the Maplet will be presented in hexadecimal (base-16 number system). Both size of the inserted cipherkey (in hexadecimal) and plaintext (in hexadecimal) must be 16-bit. The actual size of the cipherkey (in binary) and plaintext (in binary) are 64-bit. Figures shown are the Maplet interfaces develop for DES.

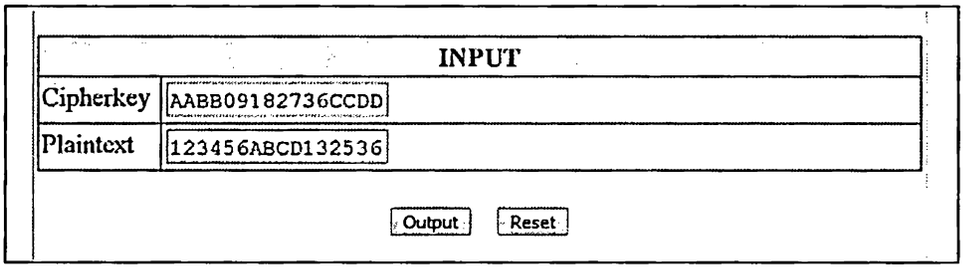


Figure 4 : Input for cipherkey and plaintext from user

The input cipherkey and plaintext will be inserted by user in hexadecimal (16-bit) in which if the cipherkey and plaintext in binary, user must change it into hexadecimal. These input is for generate round key.

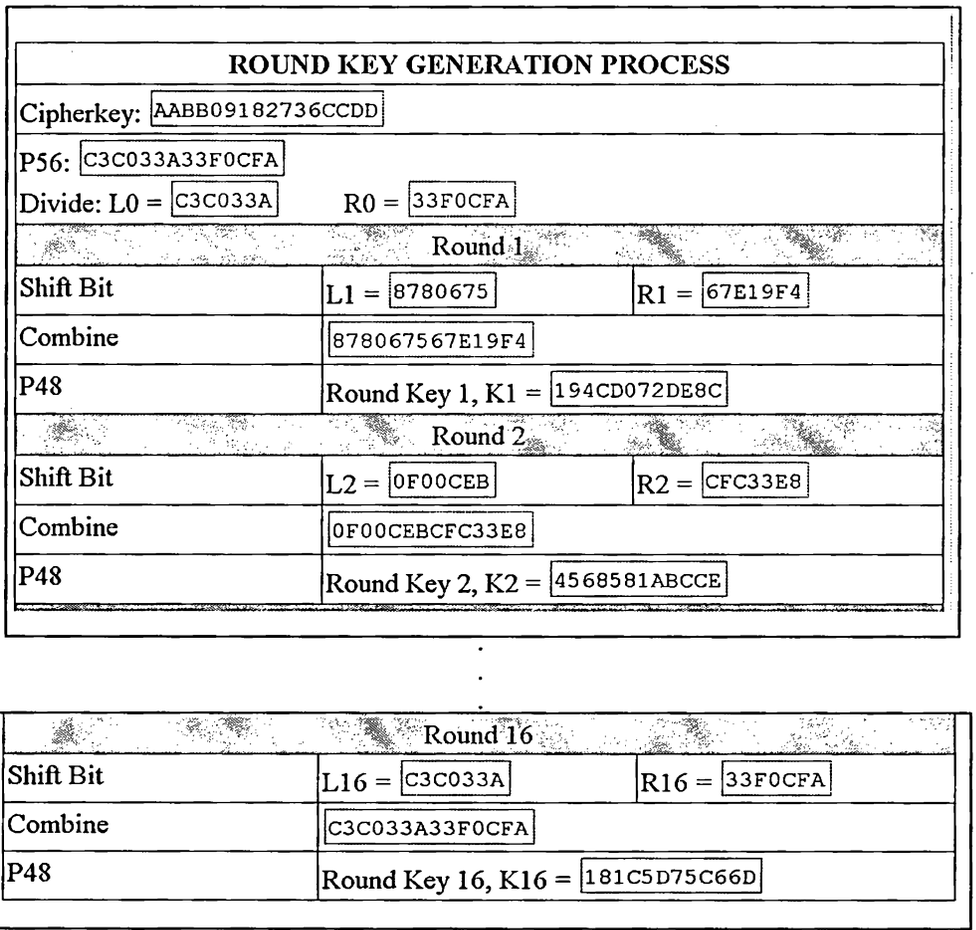


Figure 5: Round-key generation process

Once the input has been inserted by user, the program will generate the round-key 1 until round-key 16.

ENCRYPTION PROCESS			
Plaintext: 123456ABCD132536			
Initial Permutation, IP: 14A7D67818CA18AD Divide: L0 = 14A7D678 R0 = 18CA18AD			
Round	Left	Right	Round Key
Round 1	L1 = 18CA18AD	R1 = 5A78E394	K1 = 194CD072DE8C
Round 2	L2 = 5A78E394	R2 = 4A1210F6	K2 = 4568581ABCCE
.	.	.	.
Round 15	L15 = BD2DD2AB	R15 = CF26B472	K15 = 3330C5D9A36D
Round 16	L16 = 19BA9212	R16 = CF26B472	K16 = 181C5D75C66D
Combine: 19BA9212CF26B472 Final Permutation, FP: C0B7A8D05F3A829C			
Ciphertext: C0B7A8D05F3A829C			

Figure 6: Encryption process of DES

The ciphertext is then sent to the receiver to decrypt it using the cipherkey in the encryption process.

DECRYPTION PROCESS			
Ciphertext: C0B7A8D05F3A829C			
Initial Permutation, IP: 19BA9212CF26B472 Divide: L16 = 19BA9212 R16 = CF26B472			
Round	Left	Right	Round Key
Round 1	L15 = CF26B472	R15 = BD2DD2AB	K16 = 181C5D75C66D
Round 2	L14 = BD2DD2AB	R14 = 387CCDAA	K15 = 3330C5D9A36D
.	.	.	.
Round 15	L1 = 5A78E394	R1 = 18CA18AD	K2 = 4568581ABCCE
Round 16	L0 = 14A7D678	R0 = 18CA18AD	K1 = 194CD072DE8C
Combine: 14A7D67818CA18AD Final Permutation, FP: 123456ABCD132536			
Plaintext: 123456ABCD132536			

Figure 7: Decryption process of DES

Conclusion and Recommendation

The use of DES Maplet Interface is an alternative way in teaching and learning process for any universities. It can be used to aid the understanding of the theoretical and computational aspects of cryptography subject. The user interface will benefit undergraduate and postgraduate in Mathematics by providing perfect illustration of the DES concept. Further investigation is recommended to be done for a better insight on student's perception towards this system.

Acknowledgements

Special thanks and appreciations to Universiti Teknologi MARA (UiTM) and all individuals who have extended a helping hand indirectly or directly in making the study come true.

References:

Baliga, A. and Boztas, S (2001). Cryptography in the classroom using Maple. *Sixth Asian Technology Conference in Mathematics (ATCM)*.

Carlson, D., Guzdial, M., Kehoe, C., Shah, V. and Stasko, J (1996). *SIGCSE '96 Proceedings of the twenty-seventh, SIGCSE Technical Symposium on Computer Science Education*, 290-294.

Forouzan, B. A (2008). *Cryptography and Network Security*. McGraw-Hill, New York.

Khouyibaba, S (2010). Teaching mathematics with technology. *Procedia Social and Behavioral Sciences 9*, 638-643.

Kilicman, A., Hassan M., A., and Hussain S. K. S (2010). Teaching and learning using mathematics software "The New Challenge". *Procedia Social and Behavioral Sciences 8*, 613-619.

McAndrew, A (2008). Teaching cryptography with open-source software. *SIGCE '08 – Proceedings of the 39th ACM Technical Symposium on Computer Science Education*, 325-329.

Suanmali, S (2008). Maple in mathematics. *Proceedings-International Conference on Information Tehnology: New Generations*, 528-533.

EXPERIMENTAL TWO WAY QUANTUM KEY DISTRIBUTION WITH WEAK+VACUUM DECOY STATE

M. F. Abdul Khir[1,3], M. N. Mohd Zain[3], Iskandar Bahari[4], Suryadi[2] and S. Shaari[1]
[1] *Photonic Lab, IMEN, Universiti Kebangsaan Malaysia,UKM Bangi, Malaysia*
[2]*Faculty of Science, International Islamic University of Malaysia (IIUM), Kuantan, Pahang, Malaysia*
[3] *Photonics Technology and Product Development (PTPD), MIMOS Berhad, Kuala Lumpur, Malaysia*
[4] *Cryptography Lab, Advanced Analysis and Modeling (ADAM) Cluster,MIMOS Berhad, Kuala Lumpur, Malaysia*
mfared@mimos.my, zman@mimos.my, iskandar.bahari@mimos.my, suryadi@iiu.edu.my, sahbudin@eng.ukm.my

Abstract:

We report a free space based experimental demonstration of a two way Quantum Key Distribution protocol withweak+vacuum decoy state. By utilizing a different key rate formula a better maximum secure distance closer to the theoretical infinite was achieved.

Introduction

Over the past twenty years, Quantum Cryptography (QC) or better known as Quantum Key Distribution (QKD) has undergone quiet an extensive developments in its realization. Many recent activities have reported efforts on practical aspect of QKD implementation. One such effort is the decoy state protocol (Hwang 2003)which has attracted much attention in within the QKD community. Being a tool to defeat the Photon Number Splitting (PNS) attack, the decoy state QKD has revived the practicality of a weak pulse based QKD implementation.This important discovery by Hwang et al (Hwang 2003) has led to many further important works by such as (Lo et al 2005; Ma et al 2005; Zhao et al 2006)for two decoy states and the weak+vacuum decoy state. However most of these works are confined in within the prepare and measure scheme such as the BB84 protocol and the SARG04 protocol (Zhang et al 2008; Zhang et al 2009). Recently, the extension of decoy state method for two way QKD protocol(Ostermeyer et al 2008; Lucamarini et al 2007; Shaari et al 2006; Lucamarini et al 2005; Cere 2006; Kumar et al 2008) was studied by Shaari et al in (Shaari et al 2011). They have derived relevant bounds for the case of the LM05 protocol with two decoy states at different intensities similar to the one proposed for the BB84 protocol in (Ma et al 2005) and have shown that the maximum secure distance of the LM05 protocol can be increased by nearly double. In their work, two secure key rate formulas denoted as $R_{1+2}$and R_{12} were proposed, representing the case when the single and double photon contributions are separately calculated and the case when the single and double photon contributions are lumped. While the former enjoys better maximum secure distance, the latter enjoys the advantage of not having to concern on how Eve may manipulate thesingle and double photon contributions individually.

The significant work in (Shaari et al 2011) was further extended in (Abdul Khir et al 2011a; Abdul Khir et al 2011b) for the case of weak+vacuum decoy state protocol which has yielded similar result. Having the vacuum state as the second decoy state simplifies the source setup and benefits in terms of cost saving. This is evidenced in our work in (Abdul Khir et al 2012a)when we demonstrated the first implementation of a two way QKD with decoy state. In orderto accommodate the proposed decoy state, we have upgraded the previously developed free space based LM05 system in (Abdul Khir 2012b)which required just a simple modification at the source part and the software part. While the result in (Abdul Khir 2012a)turned out to confirm the theoretical works in (Jesni et al 2011; Abdul Khir 2011b) for the case of R_{12} formula it lacks the same for the R_{1+2}formula. Hence, in this work, we continue the experiment with the R_{1+2}formula and compare the performance with the theoretical values and previous works. The next section reviews the proposed decoy state method, followed by explanation on the experimental setup in section three. The result is discussed in section four while section five conclude and suggest future works.

The Protocol

An implementation of a weak+vacuum decoy state on the LM05 protocol is similar to the BB84 protocol and SARG04 protocol where in addition to the signal state with mean photon numberμ, two decoy states with mean photon number v and *zero* are introduced. The state with the *zero* intensity is called the vacuum state and is used to precisely obtain the background rate Y_0. With a proper optimization of the parameters involved, the lower bound of the secure key rate R_{1+2} can be estimated. Note that the decoy state is not used as part of the final secure key. Its function is just to detect Eve's attempt (Lo et al 2005) and estimating the secure key rate.As explained in (Abdul

Khir et al 2011a), for the case of single photon gain, we directly used equation from (Ma et al 2005) while for the double photon gain, single photon as well as double photon error rate, we use the one derived for the case of weak+vacuum decoy state from (Shaari et al 2011).

The lower bound gain of single photon state(Q_1)and double photon state (Q_2) aregiven respectively in (Abdul Khir et al 2011a; Abdul Khir 2011b) as :

$$Q_1 \geq Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu v - v^2}\left(Q_v e^v - Q_\mu e^\mu \frac{v^2}{\mu^2} - \frac{\mu^2 - v^2}{\mu^2} Y_0\right) \quad (1)$$

$$Q_2 \geq \frac{\mu^3 e^{-\mu}\left(Q_v e^v - \frac{v^3}{\mu^3} Q_\mu e^\mu - \frac{\mu^3 - v^3}{\mu^3} Y_0 - \frac{v\mu^2 - v^3}{\mu^2} Y_1^U\right)}{v^2\mu - v^3} \quad (2)$$

where Y_1^U is the upper bound of single photon yield given by :

$$Y_1^U = \frac{(2Q_v e^v - 2Y_0 - Y_2^\infty v^2)}{2v} \quad (3)$$

The Q_v is the gain from decoy state and the Y_2^∞ is the double photon yield from infinite case.The upper bound error rate of the single photon (e_1) and double photon (e_2) are given respectively as:

$$e_1^U \leq e_1^U = \frac{(E_v Q_v e^v - e_0 Y_0)\mu^2 - (E_\mu Q_\mu e^\mu - e_0 Y_0)v^2}{Y_1^L(v\mu^2 - \mu v^2)} \quad (4)$$

$$e_2^U \leq e_2^U = \frac{(E_v Q_v e^v - e_0 Y_0)\mu - (E_\mu Q_\mu e^\mu - e_0 Y_0)v}{Y_2^L\left(\frac{1}{2}\mu v^2 - \frac{1}{2} v\mu^2\right)} \quad (5)$$

The lower bound of the key generation rate is given by (Shaari et al 2011) as :

$$R_{1+2} \geq R_{1+2}^L = -Q_\mu f(E_\mu) H(E_\mu) + \sum_{i=1}^{2} Q_i[1 - \tau(e_i)] \quad (6)$$

where

$H(E_\mu)$ is the binary Shannon Entrophy and is given by$H(E_\mu) = -E_\mu \log_2(E_\mu) - (1 - E_\mu)\log_2(1 - E_\mu)$ and $\tau(e)$is the amount bits to be discarded during privacy amplification stage and is given as $\tau(e_1) = \log_2(1 + 4e_1 - 4{e_1}^2)$ for $e_1 < \frac{1}{2}$ and $\tau(e_1) = 1$ if $e_1 \geq \frac{1}{2}$.

Experimental Setup

Optics

The schematic of the experimental setup is depicted in Figure 1.It is the same setup used in (Abdul Khir et al 2012a)which involved decoy states implementation with the R_{12}secure key rate formula. The optical setup at Bob consists of the source and detector package. The source package consistsof two sets of laser source and a Pockels cell (PC1). The first set of laser source whichis used as the signal source consists of LAS1 and LAS2 emitting horizontal and vertical pulse respectively. The second set of the laser source consists of LAS3 and LAS4 also emitting horizontal and vertical pulse respectively. After going through the beam splitters (BS1 and PBS1) and also a spatial filter (SF), each optical pulses are polarization modulated at Pockels cell (PC1) where the horizontal and

vertical pulses are polarization transformed into anti-diagonal or diagonal pulses respectively. This combination prepares the four polarization states for signal and decoy states needed in realizing the LM05 protocol and decoy state implementation. The detector package consists of one Pockels cell (PC4), a Wollaston prism (WOL) and two single photon counting modules (SPCM1 and SPCM2). The optical setup at Alice was a minimal one consists of a beam splitter (BS3) and the flipper (PC2 and PC3). Alice uses the flipper to encode logical bit 1 by triggering it and logical bit 0 by not doing anything. The flipper consists of two Pockels cells (PC2 and PC3) which is capable of orthogonally rotating any of the four polarization states sent by Bob. The purpose of beam splitter (BS3) is to give the effect of control mode which is not implemented in this setup.

Electronics

All active optical components at Bob and Alice including the laser sources, Pockels cells and detectors are controlled by a LabVIEW based program that run and synchronized using a pair of 40 MHz Reconfigurable I/O module of National Instruments (PXI-7833R). The random triggering for state preparations uses software based pseudo-random number generator. The pulses are distributed 50% for signal, 25% for decoy and 25% for vacuum with pulse repetition rate at 0.725 MHz.

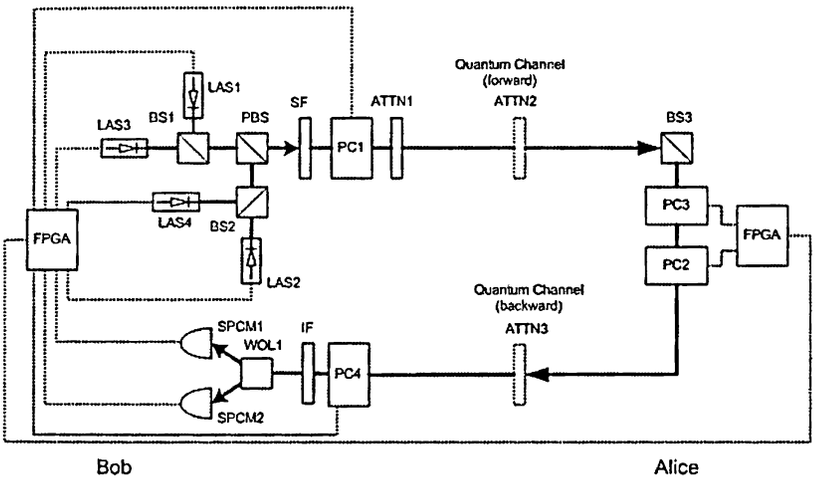


Figure 1. The LM05 and decoy state experimental setup consists of LAS1, LAS2, photon source for signal state; LAS3,LAS4, photon source for decoy state;PBS1, polarization beam splitter; SF, spatial filter; PC1, first Pockels cell; ATTN1, variable attenuator; BS1,BS2 50/50 beam splitter; ATTN2, ATTN3 attenuator; PC2, second Pockels cell; PC3, third Pockels cell; PC4, Fourth Pockels cell; IF1, interference filter; WOL1, Wollaston Prism; SPCM1, H & D detector; SPCM2, V & A detector

Results and Discussion

In the first stage of the experiment, the intrinsic parameters necessary for optimal mean photon number optimization i.e. theη_{Bob} and the$e_{detector}$were measured. These parameters are summarized in Table 1.The η_{Bob}representsthe overall detection efficiency of the system andis the product of the quantum efficiency of the detectors and the internal transmission of the system.The $e_{detector}$ is the QBER when the background noise is negligible. It is obtained by measuring the QBER after sending train of pulses with high meanphoton number. Next, numerical simulation was conducted to find the optimal mean photon number for a particular distance as well as the maximum secure distance capable with this setup. The maximum secure distance is defined as the maximum distance between Bob and Alice before the secure key generation rate hits zero. The optimal mean photon number (μ) at particular distance is the μthat results in the highest key generation rate. However, as noted in (Ma et al 2005), the secure key generation rate does not change much with small changes in μ. Hence, a fixed mean photon number, μ=0.15 for LM05 and mean photon number for signal pulsesμ=0.64 and for decoy pulsesν=0.23were used throughout the experiment.

Table 1 : Intrinsic parameters of the system

Frequency [MHz]	Detector Efficiency (η_{Det})	$e_{detector}$ [%]	Background Rate (Y_0)	Overall intrinsic transmission of the system (η_{Bob})
0.725	0.55	0.045	8.552×10^{-6}	0.072

We took several points corresponding to several channel losses, each with 140 Mbit of samples. The experimental result is shown in Table 2 which consists of channel loss in dB, the signal gain (Q_μ) and QBER (E_μ), the decoy gain (Q_ν) and QBER (E_ν), the background noise Y_0 and finally the secure key generation rate (R^L) calculated using Eq 1 ~ 6. We used error correction efficiency $f(E_\mu) = 1.22$ for secure key rate calculation.The corresponding graph is depicted in Figure 1. Note that for the case of without decoy state, we have made use of the secure key generation rate (R_{LM}) formula in (Lucamarini et al 2007). The theoretical line for the case of when one uses the key rate formula R_{12} in (Abdul Khir 2011b; Abdul Khir 2012a) where the single and double photon contribution were lumped is also presented. This provides sort of a base comparison to better illustrate the improvement achieved and how well the proposed decoy state extension performs.

Table 2 : Experimental results for Q_μ, E_μ, Q_ν, E_ν and Y_0 for six cases of channel loss.

Channel Loss (dB)	Q_μ	E_μ	Q_ν	E_ν	Y_0	R^L
2.19	1.57×10^{-2}	4.75×10^{-2}	5.81×10^{-3}	4.67×10^{-2}	4.30×10^{-6}	3.90×10^{-3}
5.20	4.02×10^{-3}	4.95×10^{-2}	1.45×10^{-3}	4.94×10^{-2}	3.72×10^{-6}	8.44×10^{-4}
7.42	1.39×10^{-3}	5.09×10^{-2}	4.84×10^{-4}	5.45×10^{-2}	4.24×10^{-6}	2.03×10^{-4}
9.51	5.58×10^{-4}	5.42×10^{-2}	2.10×10^{-4}	5.96×10^{-2}	3.37×10^{-6}	7.67×10^{-5}
11.49	2.26×10^{-4}	6.22×10^{-2}	8.64×10^{-5}	6.45×10^{-2}	3.63×10^{-6}	3.22×10^{-5}
13.58	8.17×10^{-5}	8.01×10^{-2}	3.31×10^{-5}	1.23×10^{-1}	3.42×10^{-6}	6.95×10^{-6}

From Figure 2, it is obvious that without decoy state (R_{LM}), a maximum secure distance will reach less than 7 dB channel loss. In contrast, using the proposed weak+vacuum decoy state, the maximum secure distance of the setup was extended by almost double.We verified that at 16.18 dB, the key rate is already negative. The achieved maximum secure distance was also better than the one obtained with the other key rateR_{12} usedin (Abdul Khir et al 2011a) where the single and doublephoton contribution is lumped. We note that the achieved key rate was good since it is not far from the one obtained from the case of theoretical infinite decoy state (R_∞). If one were to use the optimal $\mu$and $\nu$for every distance, this gap will be closer.The result also showed quite a good agreement between the experimental and theoretical result.

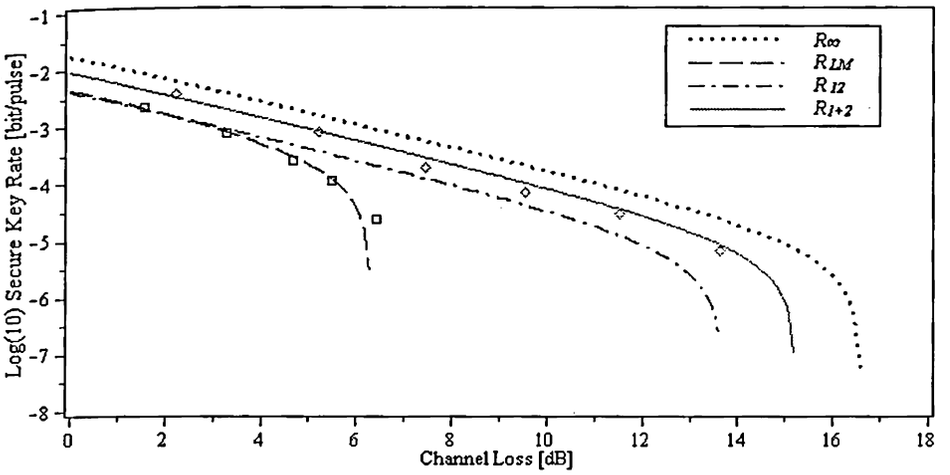


Figure 2, Experimental plots and numerical simulation results for the case ofR_{∞},R_{LM}, R_{12} andR_{1+2}. The dash line is R_{LM}, the dashdot line is the theoretical line for the case of R_{12} using the key rate used in (Abdul Khir et al 2011a), the R_{1+2} is the key rate obtained with formula in Eq. 6 and the dot line is the theoretical curve for the case of infinite decoy state.

Conclusions and Future Works

A QKD system based on a two way protocol namely the LM05 protocol and the decoy state method was successfully demonstrated. Using a better estimation of decoy state parameters has resulted in a better maximum secure distance, closer to the theoretical limit achievable with an infinite decoy state.Besides the weak+ vacuum decoy state used in this work, another practical decoy state method which utilizes only one decoy state was also proposed in (2011b). It is interesting to see this one decoy state protocol in action. We leave this as our future work.

References:

Hwang, W,Y (2003). "Quantum Key Distribution with High Loss: Toward Global Secure Communication", Phys. Rev. Lett. 91, 057901.

Lo, H,K, Ma, X, Chen, K, (2005). "Decoy State Quantum Key Distribution", Phys. Rev.Lett. 94, 230504.

Ma, X, Qi, B, Zhao, Y, Lo, H,K (2005). "Practical decoy state for quantum key distribution",Phys.Rev. A 72 012326.

Zhao, Y, Qi, B, Ma, X, Lo, H,K, Qian, L (2006). "Experimental quantum key distribution with decoy states", Phys Rev. Lett, 96: 070502.

Zhang S,L, Zou, X,B, Jin, C,H, Guo, G,C (2008). "Closing the gap of secure quantum key rate with the Heralded Pair-Coherent States", arXiv:0807.1760v1 [quant-ph]

Zhang S,L, Zou, X,B, Li, C,F, Jin, C,H, Guo, G,C, (2009). "A universal coherent source for quantum key distribution", Chinese Science Bulletin 54, 1863.

Ostermeyer, M, Walenta, N (2008). "On the implementation of a deterministic secure coding protocol using polarization entangled photons," Opt. Commun., 281(17), 4540–4544.

Lucamarini, M, Cere, A, Giuseppe, G,D, Mancini, S, Vitali, D, Tombesi, P (2007). "Two-way Protocol with Imperfect Devices", Open Systems & Information Dynamics, 14(2), 169-178

Shaari, J,S, Lucamarini, M, Wahiddin, M,R,B (2006). "Deterministic six states protocol for quantum communication", Physics Letters A, 358(2), 85-90

Lucamarini, M, Mancini, S (2005)."Secure deterministic communication without entanglement," Phys. Rev. Lett. 94, 140501.

Cere, A, Lucamarini, M, Giuseppe, G,D, Tombesi, P, (2006). "Experimental Test of Two-Way Quantum Key Distribution in the Presence of Controlled Noise"Phys. Rev. Lett. 96, 200501

Kumar, R, Lucamarini, M, Giuseppe, G,D, Natali, R, Mancini, S, Tombesi, P (2008). "Two-way quantum key distribution at telecommunication wavelength", Phys. Rev. A 77 022304

Shaari, J,S,Bahari, I, Ali, S (2011)," Decoy states and two way quantum key distribution schemes",Optic Communications, 284, 697–702

Abdul Khir, M,F, Bahari, I, Ehsan, A,A, (2011a)."Two Way Quantum Key Distribution Protocol with Weak+Vacuum Decoy State", In proceeding of the 2nd IEEE International Conference on Photonic (ICP2011), Kota Kinabalu.

Abdul Khir, M,F, Bahari, I, Ali, S, Shaari, S (2011b). "Weak+Vacuum and One Decoy State with Two Way Quantum Key Distribution Protocol",arXiv:1108.4756v2 [quant-ph].

Abdul Khir, M,F, Mohd Zain, M,N, Suryadi, Saharudin,S, Shaari, S (2012a) "Implementation of two-way free space quantum key distribution", Opt. Eng. 51, 045006.

Abdul Khir, M,F, Mohd Zain, M,N, Bahari, I, Suryadi, Sahbudin, S (2012b)."Implementation of Two Way Quantum Key Distribution Protocol with Decoy State"Optics Communications 285, 842-845

SECURE COMMUNICATION WITH ONE DECOY STATE AND TWO WAY QUANTUM KEY DISTRIBUTION SCHEME

M F Abdul Khir[1,2], M N Mohd Zain[1,2], Iskandar Bahari[3] and S. Shaari[1]
[1]*Photonic Lab, IMEN, Universiti Kebangsaan Malaysia, 43400 UKM Bangi, Malaysia*
[2]*Photonics Technology and Product Development (PTPD), MIMOS Berhad, Technology Park Malaysia, 57000 Kuala Lumpur, Malaysia*
[3]*Advance Analysis and Modelling, MimosBerhad, Technology Park Malaysia, 57000 Kuala Lumpur, Malaysia*
[1,2]*mfared@mimos.my,* [1,2]*zman@mimos.my,* [1,3]*iskandar.bahari@mimos.my,* [1]*sahbudin@eng.ukm.my*

Abstract:

Quantum Key Distribution (QKD) provides a mean for unconditionally secure secret key sharing for secure communication. For a practical QKD system, the recently proposed decoy state protocol has become an essential tool. In this work, we conduct numerical analysis against several bounds for one decoy state with two way QKD protocol and compare their performance in terms of key rate and maximum secure distance.

Introduction

Dependencies over shared information infrastructure particularly the internet has increased the demand for secure communication between two distant parties. For critically confidential data, cryptography plays very important role. While conventional cryptographic techniques rely on computational difficulties and is operated without security proof, Quantum Cryptography or better known as Quantum Key Distribution (QKD) combined with one time pad is shown to be the most likely candidate to provide the unconditionally secure information transfer needed by critical organizations.

However, real life QKD systems face implementation problems such as unavailability of true single photon source. Due to this, most QKD implementations rely on weak coherent pulses which cannot avoid emitting multi photon pulses. Attack such as Photon Number Splitting (PNS) attack has been identified as severely affecting QKD practicality in terms of limiting its maximum secure distance. This threat however was encountered by the discovery of decoy state QKD where one uses several extra states named as decoy states as described by Hwang (2003), Lo et al (2005), and also Ma et al (2005). By monitoring the statistics of the signal and decoy states, Alice and Bob could easily determine Eve's tempering since her attempt unavoidably affects both signal and decoy states statistic. This then reduces the pessimistic assumptions and reduces the amount of bits to be discarded at privacy amplification stage. As a result, the secure key generation rate and maximum secure distance is greatly increased, leading to a practical QKD implementation. Example implementations of decoy state can be seen from the work by Zhao et al. (2006), Schmitt-Manderbach (2007) and Liu et al (2010).

While it has been shown byMa et al (2005) that a special case of two decoy states that is the "weak+vacuum" decoy state where one uses one weak decoy state and the other as vacuum decoy state is optimal for the case of BB84 protocol, in some cases where only one laser source is used such as in "plug and play" QKD system, one need a very good attenuator to obtain a really vacuum state. It is known that there exist difficulties in finding really good attenuator that could totally block photons from laser source (Zhao et al. 2006) . In this case, one may resort to one decoy state. It is then interesting to see how would a one decoy state protocol performs in another variant of QKD protocol that is the two way protocol(Ostermeyer et al 2008; Lucamarini et al 2007; Shaari et al 2006; Lucamarini et al 2005; Cere 2006; Kumar et al 2008).

In this work, we compare three bounds for the case of one decoy state for a two way QKD protocol, specifically the LM05. Using the bounds, we conduct numerical simulation and observe the performance in terms of maximum secure distance. We also include the case of without decoy states as well as the theoretical infinite as base comparison of how would the proposed schemes perform. As such, this letter is organized as follows. We review the bound for the cases of one decoy state in section two. In section three we discuss the numerical simulation result while section four conclude and suggest future works.

The One Decoy State

We assume ideal case of infinite decoy state with channel transmission $t_{AB} = 10^{-\left(\frac{2lAB}{10}\right)}$, overall transmission and detection efficiency $\eta = t_{AB}\eta_{Bob}$,transmittance of i-th photon state $\eta_i = 1-(1-\eta)^i$. Notice the factor of two in channel transmission (t_{AB}) comes from the two way channel loss in a two way QKD protocol.
In the case of one decoy state, Bob and Alice do not know the background rate Y_0 precisely as they do in the case of weak+vacuum decoy state (Ma et al. 2005). This requires them to estimate the upper bound Y_0^U which can directly be imported from Eq. 38 of (Ma et al. 2005). Similarly, the lower bound of single photon yield (Y_1^L) and gain (Q_1^L) can also directly be obtained from (Ma et al. 2005). They are given as follow:

$$Y_0 \leq Y_0^U = \frac{E_\mu Q_\mu e^\mu}{e_0} \tag{1}$$

whereQ_μ and E_μ are respectively gain and QBER from signal state with mean photon number μ.

$$Y_1 \geq Y_1^L = \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - E_\mu Q_\mu e^\mu \frac{\mu^2-\nu^2}{e_0\mu^2}\right) \tag{2}$$

$$Q_1 \geq Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - E_\mu Q_\mu e^\mu \frac{\mu^2-\nu^2}{e_0\mu^2}\right) \tag{3}$$

whereQ_ν is the gain from decoy state with mean photon number ν.

We have derived the lower bound for double photon yield (Y_2) and gain (Q_2) (Abdul Khir et al 2011b) and are given by :

$$Y_2 \geq Y_2^L = \frac{2\mu\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^3}{\mu^3} - E_\mu Q_\mu e^\mu \frac{\mu^3-\nu^3}{e_0\mu^3} - \frac{\nu\mu^2-\nu^3}{\mu^2} Y_1^U\right)}{\nu^2\mu - \nu^3} \tag{4}$$

$$Q_2 \geq Q_2^L = \frac{\mu^3 e^{-\mu}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^3}{\mu^3} - E_\mu Q_\mu e^\mu \frac{\mu^3-\nu^3}{e_0\mu^3} - \frac{\nu\mu^2-\nu^3}{\mu^2} Y_1^U\right)}{\nu^2\mu - \nu^3} \tag{5}$$

whereY_1^U is given by :

$$Y_1^U = \frac{(2Q_\nu e^\nu - 2Y_0^L - Y_2^\infty \nu^2)}{2\nu} \tag{6}$$

Now, for the upper bound of single photon error rate e_1^U, we have two options, one from our previous work (Abdul Khir et al 2011b) and the other from (Ma et al. 2005) which are respectively given as:

$$e_{1B} \leq e_1^U = \frac{E_\nu Q_\nu e^\nu \mu^2 - E_\mu Q_\mu e^\mu \nu^2 - e_0 Y_0^L(\mu^2-\nu^2)}{Y_1^L(\nu\mu^2 - \mu\nu^2)} \tag{7}$$

$$e_{1A} \leq e_1^U = \frac{E_\mu Q_\mu e^\mu}{Y_1^L e_0} \tag{8}$$

The double photon error rate denoted as e_2^U is as given in (Abdul Khir et al 2011b):

$$e_2 \leq e_2^U = \frac{2(E_v Q_v e^v \mu - E_\mu Q_\mu e^\mu v - e_0 Y_0^L(\mu - v))}{Y_2^L(\mu v^2 - v\mu^2)} \tag{9}$$

The secure key rate (R) can be calculated by inserting the resulted Y_1,Q_1, Y_2, Q_2,e_1 and e_2 into key rate formula given by Shaari et al (2011) in Eq 13.

Now, we would like to review another case of one decoy state, mentioned in our previous work (Abdul Khir et al. 2011b) in which we derived the bound using the second approach proposed in (Shaari et al 2011), where the yield for single and double photon were lumped for key rate calculation. In thisway, the lumped lower bound of yield $(Y1 + Y2)^L$ is given as :

$$(Y1 + Y2)^L = \frac{\mu^3 Q_v e^v - (\mu^3 - v^3)\frac{E_\mu Q_\mu e^\mu}{e_0} - v^3 Q_\mu e^\mu + \left(v^3\mu - \frac{1}{2}v^3\mu^2\right)Y_1^L}{\mu^3(v - \frac{1}{2}\frac{v^3}{\mu})} \tag{10}$$

whereY_1^L is from Eq. 2.

The lower bound of effective gain $Q_{12}^L(\mu)$ is given as :

$$Q_{12}^L(\mu) = \left[\frac{(Y1 + Y2)^L}{2}\mu^2 + (Y_1^L\mu - \frac{Y_1^L\mu^2}{2})\right]e^{-\mu} \tag{11}$$

where the $(Y1 + Y2)^L$ and Y_1^L is from Eq.10 and Eq.2 respectively.

The upper bound of effective error rate ε^U is given as :

$$\varepsilon^U = \frac{E_\mu Q_\mu - e_0 Y_0 e^{-\mu}}{Q_{12}^L} \tag{12}$$

The effective gain ($Q_{12}^L(\mu)$) and error rate (ε^U) can be plugged into the following Eq 14 for the lower bound of key generation rate (R_{12}):

$$R \geq R^L = -Q_\mu f(E_\mu)H(E_\mu) + \sum_{i=1}^{2} Q_i[1 - \tau(e_i)] \tag{13}$$

$$R_{12} \geq R_{12}^L = -Q_\mu f(E_\mu)H(E_\mu) + Q_{12}^L[1 - \tau(\varepsilon^U)] \tag{14}$$

where$H(E_\mu)$ is the binary Shannon Entrophy and is given by

$$H(E_\mu) = -E_\mu \log_2(E_\mu) - (1 - E_\mu)\log_2(1 - E_\mu)$$

and$\tau(e)$ as

$$\tau(e) = \log_2(1 + 4e - 4e^2) \text{ for } e < \tfrac{1}{2} \text{ and } \tau(e) = 1 \text{ if } e \geq \tfrac{1}{2}$$

Results and Discussion

As previously mentioned, we have three cases of bounds for one decoy state. Let us denote the first as R_{e1A} where we used Eq 7 for e_1^U estimation and the second as R_{e1B} where we use Eq 8 for e_1^U estimation. They both used Eq 13 to calculate their secure key rate. The third case is where we lump the Y_1 and Y_2 lower bound estimation into $(Y1 + Y2)^L$ and used Eq 14 to calculate the secure key rate. We denote this as R_{12}. In order to gain confidence in our result, we have made use of real experimental data obtained from GYS experiment (Gobby et al. 2004) internal transmission of the system including detection efficiency $(\eta_{Bob}) = 0.045$, erroneous detection probability $(e_{detector}) = 0.033$ and background rate $(Y_0) = 1.7 \times 10^{-6}$. For the error correction efficiency, we used $f(e) =$ 1The result from numerical simulation is depicted in Fig 1. It includes all the three cases as well as the case of without decoy state and the theoretical infinite decoy state. For the case of without decoy state, we based on (Lucamarini et al 2007). We let optimal μ and ν for every distance where μ and ν combination that would yield highest key rate was numerically searched for every distance.

From Fig 1.we can say that all the three cases of one decoy state were able to improve the maximum secure distance of the case of without decoy state. The R_{e1A} was able to extend the maximum secure distance by around 5 km while the $R_{e1B}$was able to extend by 10 km or so. In terms of key rate, prior to around 25 km, both cases perform worse than without decoy state which question the practicality of these bounds at the said region. It is clear that the third case (R_{12}) outperforms the first and second case in key rate as well as maximum secure distance. The fact that the achieved maximum secure distance were quite far from the theoretical infinite case suggest that one should opt for the weak+vacuum case which has been shown in (Abdul Khir et al 2011a) to perform very well close to theoretical infinite case, whenever possible.

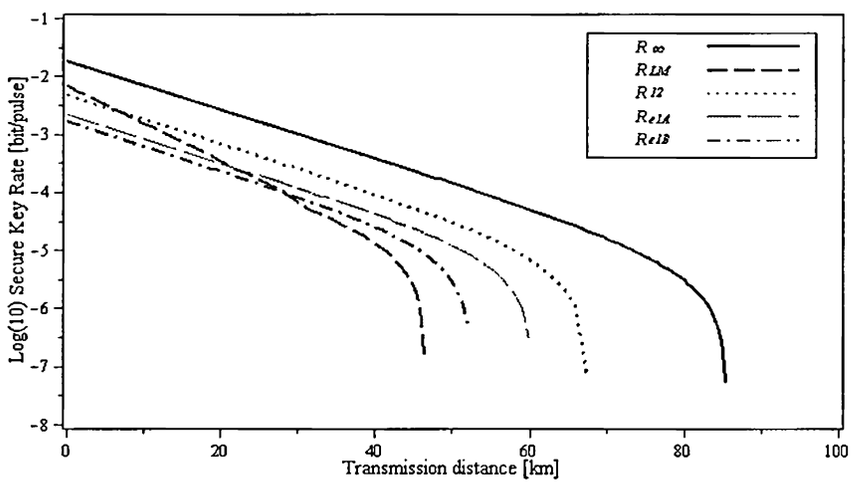


Figure 1 : A plot of secure key generation rate against transmission distance. The data are from GYS (Gobby et al. 2004) experiment. The dash line shows the simulation result of the case of without decoy state. The solid line shows the case with infinite decoy state (the maximum theoretical case). The dotted line is the case ofR_{12}, the long dash is the case of $R_{e1B}$and the dot dash is the case of R_{e1A}.

Conclusion

We have conducted numerical analysis to compare the performance of the three bounds for one decoy states with a two way QKD protocol. The result showed that the bound for one decoy state derived from the case of where single and double photon calculation were combined performs better than the bound when single and double photon contribution was separately calculated, in both key rate as well as maximum secure distance. This however is not as good as the case of weak+vacuumwhich has been shown previously in our previous work (Abdul Khir and Shaari, 2011) to perform very well close to the theoretical infinite case.

References:

Hwang, W,Y (2003). "Quantum Key Distribution with High Loss: Toward Global Secure Communication", Phys. Rev. Lett.91, 057901.

Lo, H,K, Ma, X, Chen, K, (2005). "Decoy State Quantum Key Distribution", Phys. Rev.Lett.94, 230504.
Ma, X, Qi, B, Zhao, Y, Lo, H,K (2005). "Practical decoy state for quantum key distribution",Phys.Rev.A 72 012326.

Zhao, Y, Qi, B, Ma, X, Lo, H,K, Qian, L (2006). "Experimental quantum key distribution with decoy states", Phys Rev. Lett, 96: 070502.

Zhao, Y, Qi, B, Ma, X, Lo, H,K, Qian, L (2006)., "Simulation and implementation of decoy state quantum key distribution over 60km telecom fiber", in Proceedings of IEEE International Symposium on Information Theory (IEEE, 2006), pp. 2094-2098.

Schmitt-Manderbach,T,Weier, H,Fürst, M, Ursin, R, Tiefenbacher, F,Scheidl, T,Perdigues, J, Sodnik, Z,Kurtsiefer, C, Rarity, J.G,. Zeilinger, A, andWeinfurter, H (2007). "Experimental Demonstration of Free-Space Decoy state Quantum Key Distribution over 144 km," Phys. Rev.Lett. 98, 010504.

Liu, Y, Chen, T.Y, Wang, J,Cai, W. Q, Wan, X, Chen, L. K, Wang, J. H, Liu, S. B,Liang, H,Yang, L,Peng, C. Z, Chen, K, Chen, Z. B, and Pan, J. W.(2010). "Decoy-state quantum key distribution with polarized photons over 200 km", Optics Express, Vol. 18, Issue 8, pp. 8587-8594

Ostermeyer, M, and Walenta, N. (2008) "On the Implementation of a Deterministic Secure Coding Protocol using Polarization Entangled Photons", Optics CommunicationsVolume 281, Issue 17, 1 September 2008, Pages 4540-4544

Lucamarini, M, Cere, A, Giuseppe, G,D, Mancini, S, Vitali, D, Tombesi, P (2007). "Two-way Protocol with Imperfect Devices", Open Systems & Information Dynamics, 14(2), 169-178

Shaari, J,S, Lucamarini, M, Wahiddin, M,R,B (2006). "Deterministic six states protocol for quantum communication", Physics Letters A, 358(2), 85-90

Lucamarini, M, Mancini, S (2005)."Secure deterministic communication without entanglement," Phys. Rev. Lett.94, 140501.

Cere, A, Lucamarini, M, Giuseppe, G,D, Tombesi, P, (2006). "Experimental Test of Two-Way Quantum Key Distribution in the Presence of Controlled Noise"Phys. Rev. Lett. 96, 200501

Kumar, R, Lucamarini, M, Giuseppe, G,D, Natali, R, Mancini, S, Tombesi, P (2008). "Two-way quantum key distribution at telecommunication wavelength", Phys. Rev. A 77 022304

Shaari, J,S, Bahari, I, Ali, S (2011)," Decoy states and two way quantum key distribution schemes",Optic Communications, 284, 697–702

Abdul Khir, M,F, Bahari, I, Ehsan, A,A, (2011a)."Two Way Quantum Key Distribution Protocol with Weak+Vacuum Decoy State", In proceeding of the 2nd IEEE International Conference on Photonic (ICP2011), Kota Kinabalu.

Abdul Khir, M,F, Bahari, I, Ali, S, Shaari, S (2011b). "Weak+Vacuum and One Decoy State with Two Way Quantum Key Distribution Protocol",arXiv:1108.4756v2 [quant-ph].

Abdul Khir, M,F, Mohd Zain, M,N, Suryadi,Saharudin,S, Shaari, S (2012a) "Implementation of two-way free space quantum key distribution", Opt. Eng. 51, 045006.

Abdul Khir, M,F, Mohd Zain, M,N, Bahari, I, Suryadi, Sahbudin, S (2012b)."Implementation of Two Way Quantum Key Distribution Protocol with Decoy State"Optics Communications 285, 842-845

Gobby, C, Yuan, Z. L, and Shields, A. J. (2004) Applied Physics Letters, Volume 84, Issue 19, pp. 3762-3764.

IMPLEMENTATION OF KEY-POLICY ATTRIBUTE-BASED ENCRYPTION IN BODY SENSOR NETWORK

Yar-Ling Tan[1], Bok-Min Goi[1], Ryoichi Komiya[1] and Raphael C.-W. Phan[2]
Universiti Tunku Abdul Rahman[1]
Loughborough University[2]
tanyl@mail2.utar.edu.my, raphaelphan.crypt@gmail.com

Abstract:

Body sensor network (BSN) is a set of sensors together with BSN coordinator attached on patients' body to collect vital signs. These vital signs will be sent from patients' smartphone or personal computer via BSN coordinator to the remote healthcare provider's server site. This will enable patients' vital signs to be monitored by healthcare people via internet. However, some security is necessary for the patients' confidential information including vital signs. Therefore, encryption needs to be applied to patient's vital signs. In this paper, we propose an implementation of key-policy attribute-based encryption (KP-ABE) in order to encrypt the vital signs and present an encryption/decryption prototype system of KP-ABE in BSN. Key-policy attribute-based encryption allows fine-grained sharing of encrypted data. It is able to provide differential access rights for different users. Thus, the encryption even allows flexibility in changing access rights of individual users over the encrypted data.

Introduction

The current technology has brought remarkable contribution and advancement to the electronic healthcare devices today. The advancement of electronic healthcare devices is essential for the monitoring and early prevention of various diseases such as heart diseases, diabetes, hypertension, chronic obstructive pulmonary disease (COPD), and other chronic diseases.

Body sensor network [1-3], is one of the small personal electronic healthcare networks which has been studied and tested its availability all over the world. Body sensor network (BSN) is composed of wearable computing device with a set of sensors attached on different part of human body to collect vital signs. The vital signs collected are body temperature, blood pressure, pulse rate (or heart rate), respiratory rate and etc. BSN is a wireless network that enables sensors to send the vital signs to mobile computing device (e.g. smartphone) or a computing unit via BSN coordinator. Then they will be sent to the third party server site to be stored. In this way, patient can be monitored remotely from the hospital [4].

The vital signs stored at the server site will be shared among different users (e.g. doctors, nurses, pharmacies, patient and etc.). Thus, privacy, confidentiality and security issues for these vital signs should be a major concern in this topic. Therefore, it is important for the vital signs to be encrypted before sending to the third party server sites. Encryption is one of the potent approaches to secure vital signs.

Attribute-based encryption (ABE) [5], is a fine-grained access control system, which enable a set of users to have differential access rights. On the other hand, ABE is also flexible in defining the access rights of each user. There are 2 major types of ABE; key-policy attribute-based encryption (KP-ABE) and ciphertext-policy attribute-based encryption (CP-ABE). In this paper, we propose an implementation of KP-ABE scheme to apply the encryption to patient's medical information. KP-ABE encryption time is shorter as compared to CP-ABE. Besides that, KP-ABE has less restriction and limitation onto the authorized user who is able to apply decryption to the encrypted vital signs. Authorized user (e.g. medical operator) is able to perform decryption if his/her access policy matches the attributes assigned onto the encrypted vital signs. In hardware implementation, KP-ABE is also advantageous. KP-ABE scheme is able to realize the lightweight encryption and producing smaller ciphertext size as compared to CP-ABE in a resource constraint device [6]. The medical information includes patient's personal information and vital signs. We have implemented a prototype which is composed of a body sensor network to collect vital signs from human body and a laptop to perform the encryption/decryption of patient's medical information.

Background

In 1984, Shamir introduced a novel type of public encryption scheme called Identity-Based Encryption scheme (IBE) [7], which enable users to securely communicate, verify and exchange each other's signatures without any

exchange of private or public keys. Thus, eliminates the need to keep key directories. Instead of generating a random pair of public/secret key and made the public key known to everyone, the public key can be in a form of any arbitrary string. For example, names, home address, phone number, e-mail address and etc. provided that they can uniquely identify the use which he cannot later deny. In year 2001, Boneh and Franklin proposed the first secure and practical IBE [8] from the Weil pairing on elliptic curves.

In 2005, Sahai and Waters introduced a new type of IBE scheme called Fuzzy Identity-Based Encryption (FIBE) [9]. In IBE, identities are viewed as arbitrary strings. While in FIBE, identities are being viewed as a set of descriptive attributes. FIBE scheme allows a user with private key corresponding to a set of identity, *ID* to decrypt a ciphertext encrypted with the public key, *ID'* if and only if *ID* and *ID'* overlap each other by some distance metric, *d*. Therefore, FIBE system allows a certain amount of error-tolerance in the identities. In this paper, the authors also mentioned on the application of FIBE termed as Attribute-Based Encryption (ABE). In an ABE system, a user's key and ciphertext are labeled with a set of attributes. A particular key can decrypt a particular ciphertext only if there is a match between the attributes of the user's key and ciphertext.

After ABE was first introduced in the work of Sahai and Waters, in year 2006, Goyal et al. proposed the Key-Policy Attribute Based Encryption (KP-ABE) for fine-grained sharing of encrypted data [10]. Encryption of vital signs usually limits the ability of encrypted vital signs to be shared among different users. In other words, the encrypted vital signs can only be selectively shared at a coarse-grained level. For example, in order to perform vital signs decryption, patient needs to give his/her private key to another party. This somehow allows another party to have all the access of the patient's vital signs. Another alternative, patient can act as an intermediary to perform decryption on the relevant vital signs but can be arduous. Both approaches do not seem appealing as they are not practical and inefficient.

Fine-grained sharing of encrypted data enables different authorized users to retrieve and decrypt ciphertext based on their access policy. The access policy embedded in the user's key specifies the type of ciphertext that the user's key is allowed to decrypt. In KP-ABE, each ciphertext is labeled with a set of descriptive attributes, while the access policy is embedded in the user's key. User is able to decrypt a ciphertext if the access policy of user's key matches the descriptive attributes labeled at the ciphertext. KP-ABE scheme is able to grant different access rights to different users.

In year 2007, Bethencourt et al. provides the first construction of a ciphertext-policy attribute-based encryption (CP-ABE) scheme [11]. In CP-ABE scheme, private key is labeled with a set of descriptive attributes, while the access policy is associated with the ciphertext. A user is able to decrypt the ciphertext if his attributes satisfy the access policy associated to the ciphertext. Table 1 summarizes the terminology definition in this section.

Table 1 : Terminology List

Terminology	Definition	Example
Attributes	Identities of a person	Name, home address, e-mail address, identity number, phone number
Access Structure	A policy/structure to define an authorized person	{("Dept of Medical Services" **AND** "Specialist") **AND** ("Kuala Lumpur" OR "Penang") **OR** "Name: Dr. Jehovah"}
Private Key Generator	A trusted third party that handles the issuance of private keys	N/A

Implementation

Body Sensor Network Node

We have implemented 2 types of body sensor nodes which measure temperature and 3D motion. The BSN node can transmit and receive vital signs within the range of approximately 5 meters. Figure 1 shows the body sensor node manufactured by Sensixa Ltd. Company.

Figure 1 : Body Sensor Node

Attribute-Based Encryption Scheme

For our prototype, we have implemented the KP-ABE scheme as this scheme is more suitable than CP-ABE [11]. In KP-ABE scheme as shown in Figure 2, attributes are labeled in the encrypted medical information (vital signs and patient's personal data). Access structure is embedded in the private key. The private key is issued by a trusted private key generator (PKG). This is an advantage of KP-ABE scheme where attributes label in the encrypted medical information can be easily created and altered. The tedious task of access structure creation and alteration is handled by PKG.

The KP-ABE scheme consists of four algorithms [9].

- Setup (1^k): The setup algorithm takes as input a security parameter, 1^k and outputs the public parameters, *PK* and a master key, *msk* which is known only to the private key generator (PKG).
- Enc (*m, PK, γ*): The encryption algorithm takes as input a message, *m*, a set of attributes, γ and the public parameters, *PK*. It outputs the ciphertext, *c*.
- KeyGen (*PK*, msk, $\mathbb{A}$): The key generation algorithm takes as input the public parameters, *PK*, the master key, *msk* and an access policy, $\mathbb{A}$. It outputs the private key, $D_{\mathbb{A}}$.
- Dec (*c*, *PK*, $D_{\mathbb{A}}$): The decryption algorithm takes as input the ciphertext, *c* which was encrypted under the set of attributes, *γ*, the public key parameter, *PK* and the private key, $D_{\mathbb{A}}$ for access control structure, $\mathbb{A}$. It outputs the message *m* if $\gamma \in \mathbb{A}$.

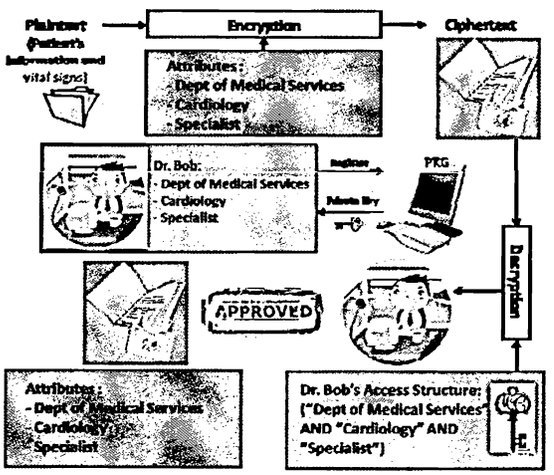


Figure 2 : Key-Policy Attribute-Based Encryption and Decryption

Prototype Setup

We have attached the sensor nodes on the human body as shown in Figure 3 to collect temperature and 3D motion readings. The readings are transmitted to the BSN coordinator which is connected to a laptop. In the laptop, KP-ABE encryption and decryption is performed.

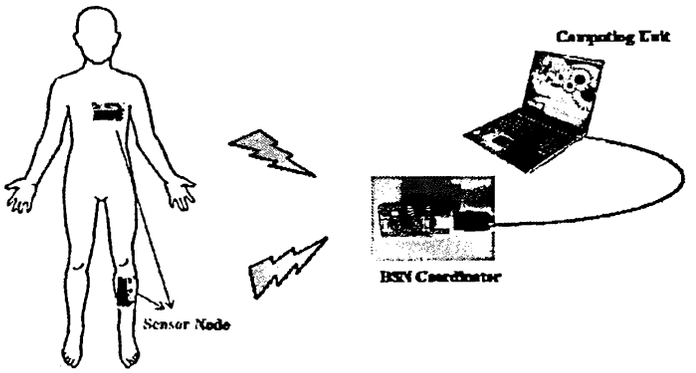


Figure 3 : Prototype configuration

Results of Experiment

Encryption and Decryption without Error

Key-policy attribute-based encryption library (*libcelia*), a subroutine library implementing KP-ABE scheme and kpabe toolkit created by Yao Zheng [12] are used in our implementation. Encryption and decryption are successfully implemented on the patient's medical information. Figure 4 illustrates the process flow of the encryption and decryption. Figure 5 shows the screenshot of encryption and decryption.

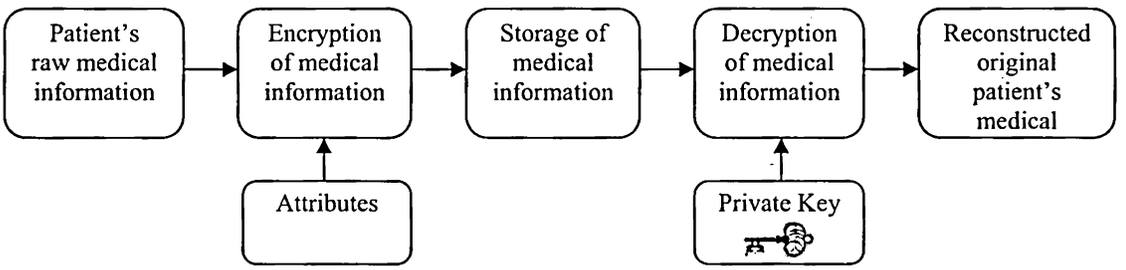


Figure 4 : Diagram of Process Flow of Encryption and Decryption

- *kpabe-setup* : The setup algorithm generates system parameters, a public key, and a master secret key under a set of attributes.
- *kpabe-enc*: Encryption algorithm encrypt medical information of patient under a set of attributes.
- *kpabe-keygen*: The key generation algorithm generates a private key and sends to the authorized medical operators.
- *kpabe-dec*: The decryption algorithm takes as input the encrypted medical information under a set of attributes, the public key parameter and the private key generated by kpabe-keygen. It then outputs the message original file if access structure embedded in the private key matched the attributes.

```
utar@ubuntu:~/kpabe$ kpabe-setup specialist doctor nurse pharmacist personal_info medical_info cost_info malaysia
utar@ubuntu:~/kpabe$ kpabe-enc pub_key vital_signs.csv specialist doctor medical_info malaysia
utar@ubuntu:~/kpabe$ kpabe-keygen -o doctor_key pub_key master_key 'specialist and doctor and medical_info and malaysia'
utar@ubuntu:~/kpabe$ kpabe-dec pub_key doctor_key vital_signs.csv.kpabe
utar@ubuntu:~/kpabe$
```

Figure 5 : Screenshot of encryption and decryption without error

From the screenshot shown in Figure 5, vital signs are being encrypted with a set of attributes. In order to decrypt the encrypted vital signs, the access policy embedded in the private key must match the attributes used to encrypt the vital signs.

Encryption and Decryption with Error

Decryption using incorrect private key

```
utar@ubuntu:~/Desktop/kpabe$ kpabe-setup specialist doctor nurse pharmacist personal_info medical_info cost_info malaysia
utar@ubuntu:~/Desktop/kpabe$ kpabe-enc pub_key vital_signs.csv specialist doctor medical_info malaysia
utar@ubuntu:~/Desktop/kpabe$ kpabe-keygen -o nurse_key pub_key master_key 'nurse and cost_info and malaysia'
utar@ubuntu:~/Desktop/kpabe$ kpabe-dec pub_key nurse_key vital_signs.csv.kpabe
cannot decrypt, attributes in ciphertext do not satisfy policy
utar@ubuntu:~/Desktop/kpabe$
```

Figure 6 : Screenshot of encryption and decryption using incorrect private key

From the screenshot shown in Figure 6, the encrypted vital signs are being decrypted with an incorrect private key. The encrypted vital signs cannot be decrypted and the original vital signs cannot be reconstructed as the embedded access policy in the private key does not satisfy the attributes encrypted in the vital signs.

Decryption using incorrect word

Table 2 : KP-ABE Performance test results with incorrect word

Correct attributes		Wrong attributes	Test results
Name of Doctor	Simon Peter	Simeon Peter	X
Expertise	Cardiology	Cardilojy	X
Department of medical service	Department of heart disease	Department of heard disease	X
Name of hospital	Columbia	Columpia	X

X: original text was not reconstructed

```
utar@ubuntu:~/Desktop/kpabe$ kpabe-keygen -o doctor_peter pub_key master_key 'doctor_simeon_peter and
cardiolojy and hospital_columpia'
Check your attribute universe,
Certain attribute not included!
utar@ubuntu:~/Desktop/kpabe$
```

Figure 7 : Screenshot of private key generation failure due to incorrect wording

From the results shown in Table 2, the private key will not be generated to perform any decryption should there be any incorrect wording. Figure 7 shows the screenshot of private key generation failure due to the incorrect wording usage. This is to ensure that the correct or error free private key is generated before sending the private key to the authorized user.

Conclusions

We present the encryption/decryption prototype system to protect the captured vital signs and personal information of patients. This enables patients' medical data to be remotely monitored from the hospital in secured manner. Body sensor nodes are used in the system to capture vital signs from the human body. We demonstrate that, by using key-policy attribute-based encryption (KP-ABE), patients' medical information can be protected and be shared among different medical operators.

Future work of this project is to connect the current system to a personal health record service provider (PHR). PHR will enable patients to store their encrypted vital signs from home and allow the medical information retrieval of healthcare providers in hospitals.

References:

B. Lo, S. Thiemjarus, R. King and G.Z. Yang (2005). Body Sensor Network - A Wireless Sensor Platform for Pervasive Healthcare Monitoring. *Adjunct Proceedings of the 3rd International Conference on Pervasive Computing, pp.77-80.*

B. Lo and G.Z. Yang (2005). Architecture for Body Sensor Networks. *IEEE Proceedings of the Perspective in Pervasive Computing, pp.23-28.*

B. Lo and G.Z. Yang (2005). Key Technical Challenges and Current Implementations of Body Sensor Networks. *IEEE Proceedings of the 2nd International Workshop on Body Sensor Networks, pp. 1-5.*

R. S. H. Istepanian, E. Jovanov, and Y.T. Zhang (2004). Introduction to the Special Section on M-Health: Beyond Seamless Mobility and Global Wireless Health-Care Connectivity. *IEEE Transactions on Information Technology in Biomedicine. Vol. 8, No. 2.*

A. Sahai and B. Waters (2005). Fuzzy Identity Based Encryption. In *Advances of cryptology – Eurocrypt 2005, LNCS 3494, pp. 457-473.*

Y.L. Tan, B.M. Goi, R. Komiya, S.Y. Tan (2011). A Study of Attribute-Based Encryption for Body Sensor Networks. *Communications in Computer and Information Science, 251(2), pp.238-247.*

A. Shamir (1984). Identity-based cryptosystems and signature schemes. *Advances in Cryptology - Crypto '84, LNCS 0196, pp. 47-53.*

D. Boneh and M. Franklin (2001). Identity-based Encryption from the Weil pairing. *Advances in Cryptology-CRYPTO'01, LNCS 2139, pp. 213–229.*

A. Sahai and B. Waters (2005). Fuzzy Identity Based Encryption. *EUROCRYPT 2005, LNCS 3494, pp. 457–473.*

V. Goyal, O. Pandey, A. Sahai and B. Waters (2006). Attribute Based Encryption for Fine-Grained Access Control of Encrypted Data. *ACM conference on Computer and Communications Security, pp. 89–98.*

J. Bethencourt, A. Sahai and B. Waters (2007). Ciphertext-policy attribute-based encryption. *IEEE Symposium on Security & Privacy, pp.321-334.*

Yao Zheng (2011). Privacy-preserving personal health record system using attribute-based encryption. *Master's thesis. Worcester Polytechnic Institute.*

CAPTCHA HMAC-BASED ONE-TIME PASSWORD (CHOTP) GENERATION

Chin-Tong Tan and Ian K. T. Tan
Faculty of Computing and Informatics, Multimedia University
johnny.tan.shinto88@gmail.com, ian@mmu.edu.my

Abstract:

The Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) is normally used to identify humans from an automated machine. In this paper, we propose a CAPTCHA HMAC-Based One-Time Password (CHOTP) where the CAPTCHA is used for verifying as well as to be used as part of the input in the HMAC-Based One-Time Password (HOTP) generation. User should identify the CAPTCHA challenge and input the value into the HOTP generator, so an input keypad is needed for this purpose. The CHOTP generated by the user is then sent to the server to verify with server generated CHOTP. On the server side, the server will use the correct CAPTCHA answer without knowing the CAPTCHA response from the user to generate HOTP. That is to say, the CAPTCHA response is not delivered through the network. In CHOTP generation, the input CAPTCHA value is used to replace the constant inner pad and outer pad values in the HMAC algorithm. Security is enhanced because of the changes of inner pad and outer pad values based on received CAPTCHA challenge.

Introduction

The security foundation of the classic user authentication with username and password relies on the encryption of the communication between user nodes and servers. This encrypted communication can be intercepted and cryptanalysis can be conducted to deduce the original password. For increased security, passwords are encouraged to be changed frequently. One-Time Password (OTP) generation and use provides a mechanism where intercepted encrypted passwords are practically useless to a cryptanalyst as the password changes each time a user goes through an authentication process.

To ensure data integrity in the transmission, the Hashed Message Authentication Code (HMAC) based One-Time Password (HOTP) is generally used. In order to generate the required output, HOTP requires a one-way hash function such as MD4, MD5 or SHA-1 (Naqvi, Akram, 2011) together with the input message, a secret key, an inner pad value and an outer pad value (Najjar, Najjar, 2006). The output will be similar regardless of the data or format of the inputs (Khan, El-Kharashi, Gebali, Abd-El-Barr, 2007). Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) is generally used to avoid automated registration, access or login. It identifies that the current user as a human by sending a challenge that is readable only by humans. CAPTCHA challenge changes each time it is requested. It leads to every CHATCHA challenge needing to be solved individually whenever it is received.

This paper is organized as follows; Section 2 provides some background to HMAC, other similar enhanced algorithms and CAPTCHA. In Section 3, we present an enhancement of combining CAPTCHA with HOTP together. Finally, we conclude in Section 4.

List of frequent used symbols throughout this paper

b	Bit-length of block	H	Hash function
H	Chaining variable	$ipad$	Inner pad, 0x36 repeated b/8 times
IV	Initial value for hash function	K	Secret key
K^+	Processed secret key for HMAC	l	Number of blocks in m after m is padded
m	Input for HMAC	n	Bit-length of hash result
$opad$	Outer pad, 0x5C repeated b/8 times	$\|\|$	Concatenation
ϕ	Compression function	ψ	Output Transformation

Background

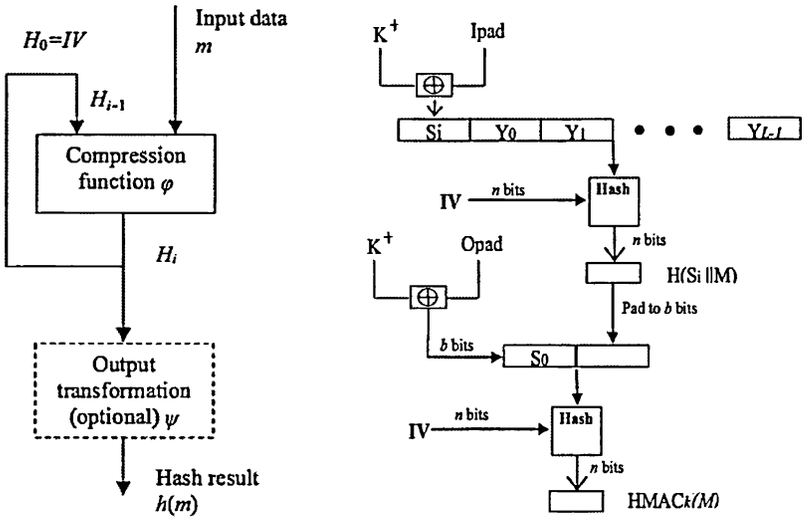
Hash Functions

A hash function accepts a variable length input m and produces a fixed length sequence output. It is a one-way function which means that there is no corresponding function to perform the reverse. The input m will be divided into $m_1, m_2, m_3, \ldots m_t$, where $m = m_1 \| m_2 \| m_3 \| \ldots \| m_t$, and $\|$ is a concatenation symbol. Input m will be appended

with extra bits if it cannot be divided into t blocks equally. The equation below illustrates the workings of the hash function $h(m)$. Figure 1 (a) shows the flow of hash function graphically (Najjar, Najjar, 2006).

$H_0 = IV$,
$H_i = \phi(m_i, H_{i-1})$, for $i = 1,2,\ldots,t$
$h(m) = \psi(H_t)$

where IV is the initial value,
H_i is the chaining variable,
ϕ is the compression function, and
ψ is the output transformation.



(a) Hash Function (b) HMAC Algorithm

Figure 1 : Hash Function and HMAC algorithm (Najjar, Najjar, 2006)

HMAC Algorithm

The HMAC algorithm was created to simplify the handling of keys through the efficiency of the hash function. HMAC algorithm needs secret key K, where the size can vary. The minimum length for K is recommended to be bit-length of hash result, n and maximum is the bit-length of each block of m after m is padded, b. Different hash functions have different bit-length for their hash result (n = 128 bits for MD5, n = 160 bits for SHA-1). For key length that is less than n bits, it will be appended with extra zero bits at the left end of K and form K^+. For key length longer than b, the key will be hashed with the h function and form K^+. No changes if K is at the length of n.

Inner padding, *ipad* and outer padding, *opad* are fixed to 0x36 and 0x5C. These padding are used to XOR with the secret key, K with $b/8$ times and form block S as displayed in figure 1 (b) in the length of b. For S_i which is the XOR of K^+ and *ipad*, it is concatenated with m in $Y_0 \| Y_1 \| \ldots \| Y_{L-1}$ and hashed with IV. The rest is as displayed in figure 1 (b). At the end of the algorithm, the output of the second hash function is the HMAC (Najjar, Najjar, 2006) (Naqvi, Akram, 2011). Following is the formula of HMAC (Najjar, Najjar, 2006) :

$$\text{HMAC}_k(m) = h(K^+ \text{ XOR } opad \| h(K^+ \text{ XOR } ipad \| m$$

HMAC-Based One-Time Password (HOTP)

The output from the HMAC is not the finalized value to be a password. The output from HMAC can be long and cannot be used by the user easily. The output needs to be processed with a truncation function.

For the explanation of the truncation function, HMAC-SHA-1 will be used as the hash function. HMAC-SHA-1 function will output a result that is 20 bytes long. With the string of 20 bytes, the lower 4 bits of the last byte are used as an offset value. These bits will be used as a 10 base digit between 0 and 15 that can represent one byte of data in the HMAC output. 4 bytes from the offset location will then be the truncated value but not finalize. Out of the 4 bytes (32 bits) of result, only the last 31 bits is used and the first bit is masked (M'Raihi, Bellare, Hoornaert, Naccache, Ranen, 2005). This act is to remove the ambiguity of computation on whether it is a signed or unsigned modulo. The output will then be modulo 10 and raised to the power of the number of digits needed. This becomes the final value for the HOTP generation.

However, to protect the HOTP from attack, there is a throttling parameter (M'Raihi, Bellare, Hoornaert, Naccache, Ranen, 2005) to control the available attempts for invalid HOTP matching. The method can be modified using a delay scheme. The delay scheme will not allow the client to send the HOTP to the server within a period of time and that time will extend depending on the number of attempts. This limits the attempts that an attacker can perform.

Enhancement of HOTP

HMAC are vulnerable to brute force attacks and birthday attacks. The brute-force attack will need 2^n computations and $2^{n/2}$ for birthday attack. Birthday attacks use the collision resistance that the same hash function is produced from two messages. Other way is that the attacker captures the sequence of messages and calculates the key from the messages. In order to avoid the attacks on HMAC algorithm, different enhancements have been introduced to increase the security and efficiency of the algorithm.

Najjar M. and Najjar F. (Najjar, Najjar, 2006) introduced the dynamic HMAC (d-HMAC) function to increase the resistance against the brute-force attacks and the birthday attacks. HMAC is not breakable offline by the attacker if the attacker tries to find the collision because of the secret key is unknown. If the attacker observes the sequence of messages generated by the same secret key, the message will be breakable. The d-HMAC uses dynamic values for inner pad (*ipad*) and outer pad (*opad*). Even if the key is the same, the padding value is always different and the HMAC generated will not be easily predictable. If one message is sent to several receivers, the same secret key will be used for every receiver. This is solved by generating different public key for different receivers and the public key will be used as part of the input for HMAC.

To improve the collision resistance of HMAC within the hash function such as MD5 and SHA-1, Davaanayam B. et. al. (Davaanaym, Lee, Lee, Lee, Lim, 2009) suggested the replacement of the hash function with the Ping-Pong-128 stream cipher. The Ping-Pong-128 stream cipher works in two mutually clocking Linear Shift Feedback Registers (LFSR) with a memory bit. The generation of the key stream depends on the feedback values. The output of the Ping-Pong-128 is generated from user's ID and password (Lee, Lim, Lee, 2010). The initial value is generated from the Ping-Pong-128 itself. To protect the Ping-Pong-128 from replay attack, it uses a Time-Event synchronized method. This method will synchronize with the server to maintain its generator matching.

The other enhancement made to increase the security against the brute-force attacks and birthday attacks was to enhance the key with MD6. Before the key K is hashed into K^+, the K is compressed in MD6. MD6 accepts an input message, a secret key, a data block and 2 optional inputs. MD6 accepts this long input in 89 word-length and processes it to output in 16 word-length. The loop of the compression function is adjustable. Naqvi S. I. and Akram A. (Naqvi, Akram, 2011) showed that by increasing the compression rounds, it linearly increased the simulation time of MD6. Compare to MD5 or SHA-1, MD6 generates the most bits out of them, it produces 512 bits compare to 160 bits for SHA-1 and 128 bits for MD5. The key generated is increased in randomness and unpredictability. The enhance algorithm shows that it spends more time in simulating than the original HMAC-MD5 algorithm. It is said that the delay is acceptable as the security of the algorithm increases as well (Naqvi, Akram, 2011).

For these enhanced algorithms, there are some unfavorable circumstances exists for better security. Since there is additional hashing function added to the original HMAC algorithm such as the d-HMAC algorithm and the key hashed with MD6 function, more resources are needed for the additional function. As shown by Naqvi S. I. and Akram A. (Naqvi, Akram, 2011), the HMAC algorithm using the MD6 function requires more time in the HMAC generation, including the adding of public key as an extra input for HMAC generation. For *ipad* and *opad* value changing, more resources are required as these values would require very frequent changes. Ping-Pong-128

algorithm seems to be safer as it improved the collision resistance, but if it is used to implement in hardware, it needs two extra LFSRs in the device.

CAPTCHA

CAPTCHA is a test to differentiate between a computer and human. The test uses distorted characters in image form (as illustrated in figure 2) so that it is difficult to be read by current character recognition technology (von Ahn, Blum, Langford, 2004)(von Ahn, Maurer, McMillen, Abraham, Blum, 2008). CAPTCHA is used to avoid automated programs to misuse the Internet. It works by sending the user a challenge in the form of an image that typically contains some characters. The user, being human, will be able to read it and respond accordingly.

Figure 2 : Distorted word of "morning" (von Ahn, Maurer, McMillen, Abraham, Blum, 2008)

Although there are advanced OCR that is able, to a certain extent, to identify the CAPTCHA distorted characters. von Ahn et. al. has shown that humans spend a few seconds to read and decode the CAPTCHA tests whilst current state of the art OCR would take a longer period which is sufficient for the protection of Internet abose (von Ahn, Maurer, McMillen, Abraham, Blum, 2008).

CAPTCHA Enhanced HOTP

The enhancement proposed in this paper is to increase the security against brute-force attacks and birthday attacks on HOTP. The proposed Hybrid CAPTCHA HOTP (CHOTP) uses CAPTCHA as part of the input for the HOTP generation. Instead of using CAPTCHA as the challenge response for human identification, we propose to use CAPTCHA as part of the input for the encryption. As it would take significant computational resources for a computer (machine) to decode a CAPTCHA image, the decoded message would be unusable for the generation of a limited time OTP.

The flow of the proposed solution will work as follows:

1. Client requests CAPTCHA challenge from server for CHOTP generation.
2. Server replies the CAPTCHA challenge to the client.
3. Client recognizes the CAPTCHA challenge and input the decoded value to the CHOTP generator. Counter for the CHOTP generator is increased as a password is generated.
4. Client replies the server with the CHOTP value generated.
5. The server inserts the correct CAPTCHA value (for the challenge sent) to its corresponding CHOTP generator and generates a CHOTP. The generator counter is increased.
6. The server compares the CHOTP sent from the client with the internally generated CHOTP.

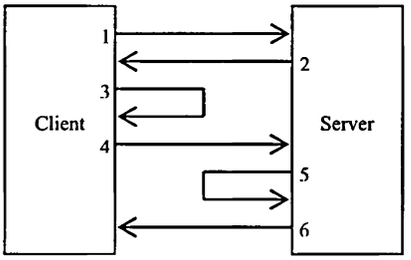


Figure 3 : The Flow of the CHOTP Steps

Enhanced CHOTP Implementation

In the standard of HOTP, the values of *ipad* and *opad* remain constant throughout the whole encryption process. Modifying these values to some other value like d-HMAC function proposed by Najjar (Najjar, Najjar, 2006) would not cause any problem to the encryption. In the proposed solution, CAPTCHA value will be used to replace the default *ipad* and *opad* values. Then the *ipad* and *opad* values will operate as mentioned in the standards. In order to do so, the CAPTCHA value needs to be processed to be used as the *ipad* and *opad* values. The *ipad* and *opad* values are both one-byte length of which a CAPTCHA typical value will be much more significant.

However, note that the CAPTCHA values are generally limited to readable characters and hence it needs to be manipulated to provide a larger range of values for *ipad* and *opad* use. CAPTCHA uses alphanumeric characters, which consists of 26 upper case letters, 26 lower case letters and 10 number letters. This means that each CAPTCHA character will yield 6 bits of data to represent the 62 different possible combinations. As *ipad* and *opad* requires one-byte length each, the CAPTCHA must provide at least 3 characters. Our proposed solution accepts CAPTCHA value is any number of characters.

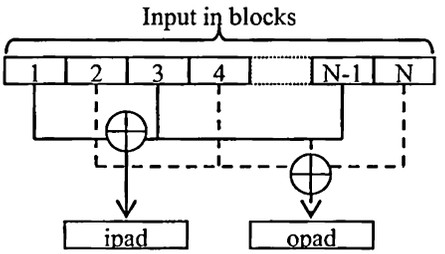


Figure 4 : *ipad* and *opad* generation

The CAPTCHA value must be in N x 16 bits where N must be more than zero. If it is not, append extra zeros to it until it meets the requirements. The final outcome of the manipulation will be in 16 bits. Following will shows how to generate 16 bits output from the input of N x 16 bits:

1. Separate inputs into blocks of one byte
2. *ipad* = XOR of every blocks in odd position
3. *opad* = XOR of every blocks in even position

At the end of all the XOR, 1 byte of data will be generated for *ipad* and another 1 byte for *opad* as illustrated in figure 4. This will replace the default value of the padding and then continue with the rest of the OTP generation that is XOR with the processed secret key and so on.

Conclusion

As the *ipad* and *opad* values remain constant in the standard HOTP generation. These values can be dynamically substituted, similar to d-HMAC (Najjar, Najjar, 2006), with the manipulated CAPTCHA challenge value sent from the server.

In addition to the enhanced security in utilizing a dynamic *ipad* and *opad* values, our proposed CHOTP can identify that the user is a human and hence increases its resilience from brute force attacks and birthday attacks. The CAPTCHA value is also no susceptible to interception as the challenge response value is never delivered back to the server, neither in plain text nor in encrypted form.

There are two main limitations of this approach, the first being that it cannot be used offline as it requires the authenticating server to provide the CAPTCHA challenge response and it is not suitable for hardware based OTP generation. The latter is because it requires significant hardware investments in not only providing a screen to display the CAPTCHA challenge response image but also additional key pads to allow the users to enter the CAPTCHA value for the *ipad* and *opad* generation prior to generating the OTP value.

Potential future work stems from one of the major issues with CAPTCHA in that users make mistakes on reading the CAPTCHA challenge. Although this can be addressed with the use of reCAPTCHA (von Ahn, Maurer, McMillen, Abraham, Blum, 2008), our current proposed solution is not suitable for the implementation of reCAPTCHA. This is because the server generator will need to know which of the two words (or both) provided by reCAPTCHA are correct. The user generator would also need to identify the correct response and generate the appropriate CHOTP from it.

References:

von Ahn, L., Blum, M., Langford, J. (2004). Telling humans and computers apart automatically. *Communication of the ACM*, 47(2) 56-60.

von Ahn, L., Maurer, B., McMillen, C., Abraham, D., Blum, M. (2008). reCAPTCHA: human-based character recognition via web security measures. *Science Magazine*, 321(5895), 1465-1468.

Davaanaym, B., Lee, Y. S., Lee, H.J., Lee, S.G., Lim, H.T. (2009). A ping pong based one-time password authentication system. *Fifth International Joint Conference on INC, IMS and IDC (NCM'09)*, 574-579.

Lee, Y.S., Lim, H.T., Lee, H.J. (2010). A study on efficient OTP generation using stream cipher with random digit. *In Proceedings of the 12th International Conference on Advance Communication Technology (ICACT)*, 2, 1670-1675.

Khan, E., El-Kharashi, M.W., Gebali, F., Abd-El-Barr, M. (2007). Design and Performance Analysis of a Unified, Reconfigurable HMAC-Hash Unit. *IEEE Transactions on Circuits and Systems I*, 54(12), 2683-2695.

Najjar, M., Najjar, F. (2006). d-HMAC Dynamic HMAC function, *In Proceedings of International Conference on Dependability of Computer Systems (DepCos-RELCOMEX '06)*. 119-126.

Naqvi, S.I., Akram, A. (2011), Pseudo-random key generation for secure HMAC-MD5. *In Proceedings of the 3rd International Conference on Communication Software and Networks (ICCSN)*, 573-577.

M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., Ranen, O. (2005), HOTP: an HMAC-based one-time password algorithm. *Internet RFC4226.*

ATTRIBUTE FOR LIGHTWEIGHT INTRUSION DETECTION SYSTEM TO DETECT PHISHING ATTACK

Cik Feresa Mohd Foozy, Rabiah Ahmad and Mohd Faizal Abdollah
Center for Advanced Computing Technology(C-ACT)
Faculty of Information Communication Technology
University Technical Malaysia Melaka
p031020001@student.utem.edu.my, rabiah@utem.edu.my, faizalabdollah@utem.edu.my

Abstract:

Phishing is a type of technical-based social engineering attack and the popularity of Internet usage by using computer handheld devices such as smart mobile and tablet PC, also contribute to the rising cyber attack every year. There are few detection tools and mechanisms has been introduces to detect this attack on computer handheld devices. One of the detection mechanism is lightweight Intrusion Detection System(IDS). Lightweight IDS is a second layer protection for attack and it can implement at any type of handheld computer devices platform. Since the lightweight IDS architecture must be small and simple, the monitoring and detection components that contain rule set also must suited with the host architecture. Moreover, rule set also is an important part for detection component. Thus, this paper proposed phishing attribute taxonomy and general studies on phishing detection attribute as preliminary study to develop rule set for website phishing.

Keywords- Intrusion Detection System; Lightweight; Rule Set; Security

Introduction

Browsing Internet in a public places by using computer handheld devices such as tablet computer, smart phone, notebook and others is becomes a lifestyle these days. Additionally, the popularity of social networks or instant messaging makes everyone connected is become a phenomenon to everyone. Because of these interesting devices and unlimited usage of networks every day it can contribute to cyber security risk. According to News Strait Times by Suparmaniam [1], a Malaysian online news paper, the security threats in Malaysia have increased more than 100 per cent over the past three years. The security threat is include phishing and hacking.

Intrusion Detection System (IDS) is one of the security system that can detect attack and according to Amiri et al.[2], IDS is one of effective way to have higher security in computer or network. Moreover, basic component for IDS are monitoring, detection and alert. Rule set can be implemented on IDS and it usually will execute for attack detection purpose. By implementing rule set on detection engine, it capable to detect the intrusion on the host or network. This paper will review previous studies on phishing and listed rule set attributes as preliminary study to develop lightweight IDS on computer handheld device.

Phishing

Phishing is a type of social engineering[3] and there are few phishing technique to enter the phishing web site, by past spam filtering and browser protection. URL shortening is type of method to create phishing URLs and this technique is commonly used to phish handheld computers[4]. Moreover, Dhinakaran et al.[5] found out that phishing email come from different source of IP address.

According to SOPHOS [6], fishing can classify into four categories such as pharming, vishing, smishing and twishing. Pharming is a method of phishing using the fraudulent of website. Vishing is technique used voice. Moreover, smishing or SMS phISHING is a method that using phone services via short messaging services (SMS) to scam people and finally is twishing or TWitter phISHING is a method that scams using Twitter which is one of the popular social networking sites today.

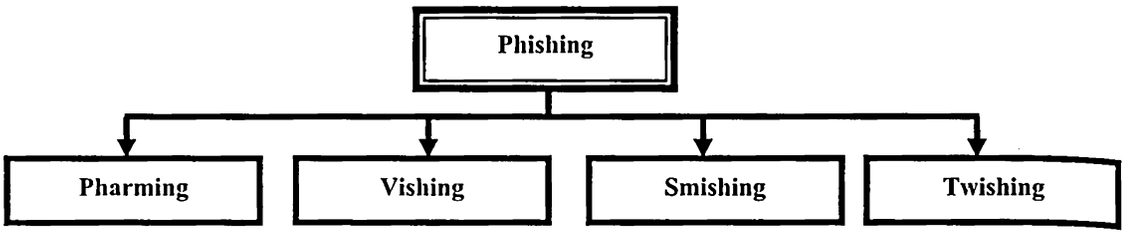


Figure 1 : Phishing Category [6]

Salem et al. [7], categorized phishing technique into five major technique to accomplish this attack. The techniques are Impersonate, Forward Attack, Pop-up attack, Voice Phishing and Mobile Phishing. Moreover, Soni et al. [8] listed the criteria of phished website should have URL & Domain Identity, Security & Encryption, Source Code & Java script, Page Style & Contents, Web Address Bar and Social Human Factor.

Phishing Attack on Computer Handheld Devices

Example of handheld computer devices are PDA, Palm Pilot, Tablet PC and Smart Mobile [9]. There are few types of attack those usually attacking computer handheld devices such as trojan horse, vishing, phishing and DoS. Based on Table 1, phishing usually detect tablet PC and smart mobile. Since IDS has been applied to detect several attacks on network and host. Thus the implementation lightweight IDS on handheld computers has been proposed to detect phishing attack on handheld computer devices.

Table 1 : Attack Analysis on Handheld Computer (Item Found=Type of Technical-based Social Engineering Attack)

Handheld Type / **References**	PDA	Palm Pilot	Tablet PC	Smart Mobile
Freundenthal et al.[10]		Trojan Horse		
Mulliner [11]	Vishing			
Beck and Zhan [12]			Phishing	
Li et al. [13]				DoS
Leavitt,[14]				Phishing

Phishing Attack Defense Mechanism on Computer Handheld Devices

Few suggestion from McDowell [15] for phishing prevention are don't send sensitive information over the Internet before checking a website's security, user must make sure URL of a website is correct such as spelling or domain, install and update anti-virus software, firewalls and email filters to reduce some of this traffic and finally using anti-phishing.

Rule Set Attribute to Detect Phishing Attack

According to [16], rule set is a set of rules in IDS that transform the rules into action on packets in the data stream according to the configuration of router software processes. Table 2 shows the attribute that has been proposed by several researchers to detect email phishing.

Shreeram [17] proposed a rule set to detect phishing attack using genetic algorithm and the attribute for the rule set to detect phishing is IP-Based URLs . Moreover, Salem[7] have proposed a rule set in the studies for awareness program and artificial intelligent tools to detect phishing email. There are several attribute that Salem[7] has implemented in the studies such as IP, Scripts, Multi domain, salutation, warning and security and also fake *http* links. Liping et al. [18] examine seven features for phishing email detection such as links, invisible link, non-matching URL, forms, body blacklist word and subject blacklist word. In addition, Pamunuwa et al.[19], the attribute that has been proposed to detect phishing email by using IDS in the studies are IP_Based URLs, non-matching URLs, HTML, Cross Site Image and all image that not cross site.

Table 2 : Rule set Attribute for Phishing emails (Item Found=√)

References / Rule Set Attribute	Shreeram[17]	Salem[7]	Liping [18]	Pamunuwa et al.[19]
IP-Based URLs	√	√		√
Scripts		√	√	
Multi domain		√		
Salutation		√		
Warning and security		√		
Fake *Https* links		√		
Total Links			√	
Number Invisible Links			√	
Non Matching URLs			√	√
Forms			√	
Body Black List Words			√	
Subject Black List Words			√	
HTML				√
Cross Site Image				√
All image that not cross site				√

Alnajim and Munro [20] studies on phishing detection on website and the rule set attribute in the studies are IP-Based URLs, Host name and blacklist phishing URL. Moreover, Zhou et al.[21] also proposed to detect phishing attack and there are three types attribute that been used in the rule set such as IP-Based URLs, domain name and host name. Moreover, Aburrous et al.[22] has listed several criteria to detect phishing and the technique that has been applied is fuzzy technique. Six attributes has been implemented such as IP-based URLs, domain name, blacklist phishing URL, abnormal request URL, abnormal URK anchor and abnormal DNS recor. Additionally, a popular anti-phishing SpoofGuard has been discuss by Huajun et al [23] and the author also studies several criteria to detect phishing by analyzing IP-Based URLs, domain name, link and image check. Table 3 below, listed all the attribute for web site phishing detection by previous studies.

Table 3 : Rule set Attribute for Phishing Web Sites (Item Found=√)

References / Rule Set Attribute	Alnajim and Munro [20]	Zhou et al.[21]	Aburrous et al.[22]	Huajun et al [23]
IP-Based URLs	√	√	√	√
Domain Name		√	√	√
Link				√
Image Checks				√
Host Name	√	√		
Blacklist Phishing URL	√		√	
Abnormal Request URL			√	
Abnormal URL Anchor			√	
Abnormal DNS record			√	

Lightweight Intrusion Detection System (IDS)

Intrusion Detection System (IDS) is one of the security system that can detect attack and according to Amiri et al.[2], IDS is one of effective way to have higher security in computer or network. In order to have secured IDS, many issues need to be considered such as data collection, data pre-processing, intrusion recognition, reporting and response[24]. However, to develop a lightweight IDS, the architecture need to be small, simple and secure in order to implement it on host or component of network that have limited storage or processing.

Several researchers have been done for simple architecture, effectiveness, scalability and easily to deploy. Wen et al. [25] ,Sheng et al. [26] and Azmandian et al.[27] study about IDS in the alert fusion. Sivatha Sindhu et al.[28] using soft computing techniques to detect anomalies in the network, Alsaleh and Van Oorschot [29] focus on network scanner signature based detection, Li et al. [30] develope an algorithm for feature selection in lightweight IDS. Moreover, Deng [31] and Li et al.[32] done a lightweight study on wireless sensor network. For handheld computers such as Android, Shabtai et al.[33], Shabtai et al.[34], Schmidt et al.**[35]**, Schmidt et al. [36]and Aubrey-Derrick Schmidt [37] also have done few studies lightweight IDS on android. However, these studies are not focusing on phishing attack and this paper will identify email and website phishing attributes for rule set to detect phishing attack on computer handheld devices.

Result and Conclusion

As a preliminary study to develop a set of rules for lightweight IDS to detect phishing attack, the attack attributes need to identify. In this paper, two analyses on email and website phishing attribute rule set have been done in order to identify the common attribute that has been used by previous studies Figure 2 shows phishing taxonomy attribute that listed from Table 2 and Table 3. It shows that many attributes for rule set that has been implemented to detect phishing on emails and website. However, the most efficient phishing attribute rule set need to identify so that it can be applied in lightweight phishing IDS on computer handheld devices.

Table 2 listed the email phishing attribute that has been implemented by the researchers on phishing detection, it shows that, IP-Based URLs, Scripts and Non-Matching URL has more than one item type occurrences. Moreover, for website phishing in Table 3, IP-Based URLs, Domain Name, Host Name and Blacklist Phishing URL are frequently implemented in phishing detection to detect the phishing. Figure 2, is Phishing attribute taxonomy that has been develop based on the email and website analysis (Table 2 and Table 3). However, for Smishing and Vishing attribute is not included in this paper and it will be as our future studies and the outcome of this paper will be our future work to develop lightweight phishing detection rule set.

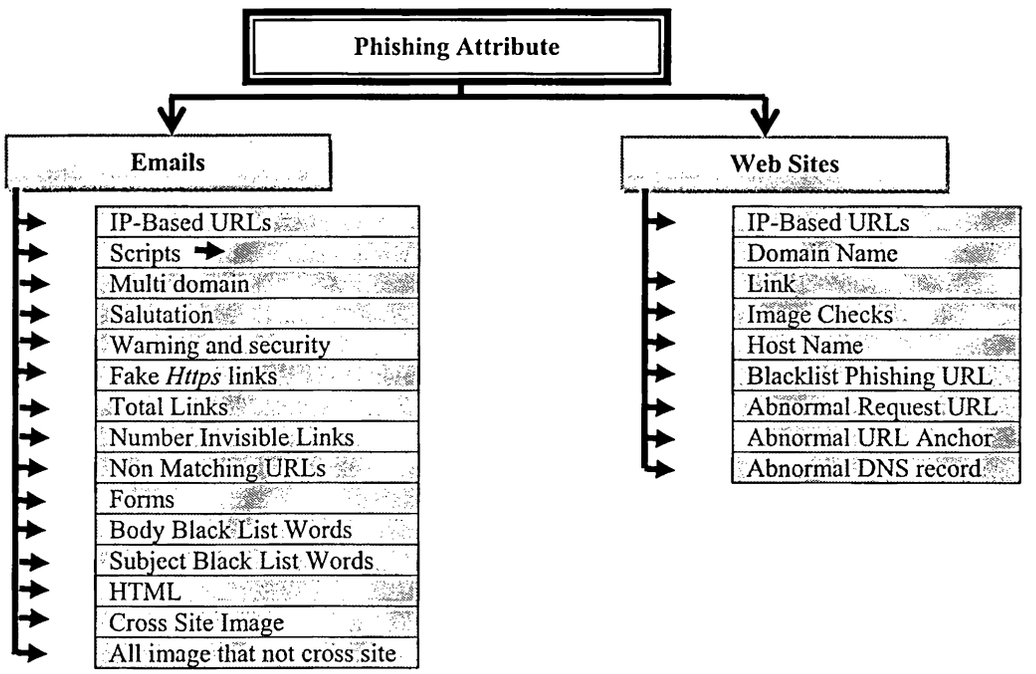


Figure 2 : Phishing Attribute Taxonomy

Acknowledgement

The authors would like to thank Universiti Tun Hussein Onn Malaysia (UTHM) and Ministry of Higher Education Malaysia for supporting this research.

References:

Suparmaniam, S., *Cyber Security Threats Double*, in *News Strait Times*. 2011.

Amiri, F., et al., *Mutual information-based feature selection for intrusion detection systems.* Journal of Network and Computer Applications, 2011. 34(4): p. 1184-1199.

Stone, A., *Natural-Language Processing for Intrusion Detection.* Computer, 2007. 40(12): p. 103-105.

Rasmussen, G.A.a.R., *Global Phishing Survey:Trends and Domain Name Use in 2H2010.* 2011.

Dhinakaran, C., L. Jae Kwang, and D. Nagamalai. *"Reminder: please update your details": Phishing Trends.* in *Networks and Communications, 2009. NETCOM '09. First International Conference on.* 2009.

SOPHOS, *Security Threat Report: 2010.* 2010.

Salem, O., A. Hossain, and M. Kamala. *Awareness Program and AI based Tool to Reduce Risk of Phishing Attacks.* in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on.* 2010.

Soni, P., S. Firake, and B.B. Meshram, *A phishing analysis of web based systems*, in *Proceedings of the 2011 International Conference on Communication, Computing; Security.* 2011, ACM: Rourkela, Odisha, India. p. 527-530.

Stonemetz, J., K. Ruskin, and R. Prasad, *Handheld Devices Anesthesia Informatics.* 2009, Springer New York. p. 409-424.

Freundenthal, M., S. Heiberg, and J. Willemson. *Personal security environment on Palm PDA.* in *Computer Security Applications, 2000. ACSAC '00. 16th Annual Conference.* 2000.

Mulliner, C., *Security of Smart Phones*, in *Department of Computer Science.* 2006, University of California Santa Barbara: CA.

Beck, K. and J. Zhan. *Phishing Using a Modified Bayesian Technique.* in *Social Computing (SocialCom), 2010 IEEE Second International Conference on.* 2010.

Li, Y., C. Jing, and J. Xu, *A New Distributed Intrusion Detection Method Based on Immune Mobile Agent*, in *Life System Modeling and Intelligent Computing*, K. Li, et al., Editors. 2010, Springer Berlin / Heidelberg. p. 233-243.

Leavitt, N., *Mobile Security: Finally a Serious Problem?* Computer, 2011. 44(6): p. 11-14.

McDowell, M. *Avoiding Social Engineering and Phishing Attacks.* 2009 [cited 2011 8th June]; Available from: http://www.us-cert.gov/cas/tips/ST04-014.html.

Network, J. *Configuring IDS Rule Sets.* 2010 [cited 2011 8th June]; Available from: http://www.juniper.net/techpubs/en_US/junos10.4/topics/usage-guidelines/services-configuring-ids-rule-sets.html.

Shreeram, V., et al. *Anti-phishing detection of phishing attacks using genetic algorithm.* in *Communication Control and Computing Technologies (ICCCCT), 2010 IEEE International Conference on.* 2010.

Liping, M., et al. *Automatically Generating Classifier for Phishing Email Prediction.* in *Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on.* 2009.

Pamunuwa, H., D. Wijesekera, and C. Farkas, *An Intrusion Detection System for Detecting Phishing Attacks*, in *Secure Data Management*, W. Jonker and M. Petkovic, Editors. 2007, Springer Berlin / Heidelberg. p. 181-192.

Alnajim, A. and M. Munro. *An Approach to the Implementation of the Anti-Phishing Tool for Phishing Websites Detection.* in *Intelligent Networking and Collaborative Systems, 2009. INCOS '09. International Conference on.* 2009.

Zhou, C.V., et al. *A Self-Healing, Self-Protecting Collaborative Intrusion Detection Architecture to Trace-Back Fast-Flux Phishing Domains.* in *Network Operations and Management Symposium Workshops, 2008. NOMS Workshops 2008. IEEE.* 2008.

Aburrous, M., et al. *Intelligent Phishing Website Detection System using Fuzzy Techniques.* in *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on.* 2008.

Huajun, H., T. Junshan, and L. Lingxi. *Countermeasure Techniques for Deceptive Phishing Attack.* in *New Trends in Information and Service Science, 2009. NISS '09. International Conference on.* 2009.

Wu, S.X. and W. Banzhaf, *The use of computational intelligence in intrusion detection systems: A review.* Applied Soft Computing, 2010. **10**(1): p. 1-35.

Wen, S., W. Zhou, and Y. Xiang, *CAFS: A Novel Lightweight cache-based scheme for large-scale intrusion alert fusion.* Concurrency Computation Practice and Experience, 2011. **12**(15).

Sheng, W., X. Yang, and Z. Wanlei. *A Lightweight Intrusion Alert Fusion System.* in *High Performance Computing and Communications (HPCC), 2010 12th IEEE International Conference on.* 2010.

Azmandian, F., et al., *Virtual machine monitor-based lightweight intrusion detection.* SIGOPS Oper. Syst. Rev., 2011. **45**(2): p. 38-53.

Sivatha Sindhu, S.S., S. Geetha, and A. Kannan, *Decision tree based light weight intrusion detection using a wrapper approach.* Expert Systems with Applications, 2011.

Alsaleh, M. and P.C. Van Oorschot. *Network scan detection with LQS: A lightweight, quick and stateful algorithm.* 2011.

Li, Y., et al., *Building lightweight intrusion detection system using wrapper-based feature selection mechanisms.* Computers & Security, 2009. **28**(6): p. 466-475.

Deng, J., R. Han, and S. Mishra, *INSENS: Intrusion-tolerant routing for wireless sensor networks.* Computer Communications, 2006. **29**(2): p. 216-230.

Li, G., J. He, and Y. Fu, *Group-based intrusion detection system in wireless sensor networks.* Computer Communications, 2008. **31**(18): p. 4324-4332.

Shabtai, A., U. Kanonov, and Y. Elovici, *Intrusion detection for mobile devices using the knowledge-based, temporal abstraction method.* Journal of Systems and Software, 2010. **83**(8): p. 1524-1537.

Shabtai, A., et al., *"Andromaly": a behavioral malware detection framework for android devices.* Journal of Intelligent Information Systems, 2010: p. 1-30.

Schmidt, A.-D., et al., *Monitoring smartphones for anomaly detection.* Mob. Netw. Appl., 2009. **14**(1): p. 92-106.

Schmidt, A.D., et al. *Static Analysis of Executables for Collaborative Malware Detection on Android.* in *Communications, 2009. ICC '09. IEEE International Conference on.* 2009.

ON THE HASTAD'S ATTACK TO $LUC_{4,6}$ CRYPTOSYSTEM

[1]Wong Tze Jin, [1]Hailiza Kamarulhaili and [2]Mohd. Rushdan Md Said
[1]*School of Mathematical Sciences, Universiti Sains Malaysia, Penang, Malaysia*
[2]*Institute for Mathematical Research, Universiti Putra Malaysia, Selangor, Malaysia.*
sherlock.wong.tj@gmail.com, hailiza@cs.usm.my, rushdan@math.upm.edu.my

Abstract:

The $LUC_{4,6}$ cryptosystem is a system analogy to RSA cryptosystem and extended from LUC and LUC_3 cryptosystems. Therefore, the security problem of the $LUC_{4,6}$ cryptosystem is based on integer factorization which is similar to RSA, LUC and LUC_3 cryptosystems. The Hastad's attack is one of the polynomial attack which relied on the polynomial structure of RSA-type cryptosystem. In this paper, Hastad's Theorem will be used to solve a system of multivariate modular equations and Coppersmith Theorem will be used to find a root of a modular equation. Thus, the number of plaintexts which are required to succeed the attack can be found.

Introduction

The fourth and sixth order of LUC cryptosystem or $LUC_{4,6}$ cryptosystem [Wong, 2007] had been proposed in 2007. This cryptosystem is analogous to the RSA cryptosystem and extended from LUC and LUC_3 cryptosystems. The $LUC_{4,6}$ cryptosystem was derived from the fourth order linear recurrence relation which is related to Quartic polynomial and based on the Lucas function.

The security problem for $LUC_{4,6}$ cryptosystem is based on integer factorization which is similar to RSA, LUC and LUC_3 cryptosystems. The Hastad's attack is one of the polynomial attack which relied on the polynomial structure of RSA-type cryptosystem. Therefore, the Hastad's attack is able to solve the underlying intractable problem which the attack do not factor the RSA- modulus, n for the $LUC_{4,6}$ cryptosystem directly. It used the other solution to recover the plaintext.

In 1986, Hastad showed that using RSA with low public exponent is insecure if the users are sending linearly related plaintexts over a large network [Hastad]. Therefore, Hastad develop a technique to solve a system of univariate modular equations to succeed his attack. Besides that, Coppersmith proposed a new method for finding a root of a modular equation [Coppersmith], which turned out to be a better way to succeed a successful attack in 1996.

In this paper, the Hastad's attack will be extended on the $LUC_{4,6}$ cryptosystem. The $LUC_{4,6}$ cryptosystem will be presented in Section 2. The theorems which are used in the attack will be presented in Section 3. In section 4, the Hastad's attack on the $LUC_{4,6}$ cryptosystem will be proposed and discussed. Finally, the conclusion had been make in the last section.

$LUC_{4,6}$ Cryptosystem

A N-th order linear recurrence of Lucas function is a sequence of integers T_k defined by

$$T_k = \sum_{i=1}^{N} (-1)^{i+1} a_i T_{k-i}, \tag{1}$$

with initial values T_0, T_1, ... , T_{N-1} and a_i are coefficients in N-th order polynomial,

$$x^N + \sum_{i=1}^{N-1} (-1)^i a_i x^{N-i} + a_N = 0. \tag{2}$$

The $LUC_{4,6}$ cryptosystem was set out based on the Lucas sequence V_k derived from the quartic polynomial, $x^4 - m_1 x^3 + m_2 x^2 - m_3 x + 1 = 0$, where (m_1, m_2, m_3) constitutes the plaintexts. Then, the encryption function is defined by

$$\begin{aligned} & E(m_1, m_2, m_3) \\ & \equiv (V_e(m_1, m_2, m_3, 1), \\ & \quad V_e(m_2, m_1 m_3 - 1, {m_1}^2 + {m_3}^2 - 2m_2, m_1 m_3 - 1, m_2, 1), \\ & \quad V_e(m_3, m_2, m_1, 1)) \bmod n \\ & \equiv (c_1, c_2, c_3) \bmod n, \end{aligned} \tag{3}$$

where $n = pq$ and the encryption key, e relative prime to $p-1$, $q-1$, $p+1$, $q+1$, p^2+p+1, q^2+q+1, p^3+p^2+p+1, and q^3+q^2+q+1. Besides that, $V_e(m_1, m_2, m_3, 1)$ and $V_e(m_3, m_2, m_1, 1)$ are the e-th term of the fourth order Lucas sequence and $V_e(m_2, m_1 m_3 - 1, {m_1}^2 + {m_3}^2 - 2m_2, m_1 m_3 - 1, m_2, 1)$ is e-th term of the sixth order Lucas sequence.

To decipher the plaintexts, the receiver must know or be able to compute the Euler totient function $\Phi(n)$ for the purpose to compute the decryption key is (d, n) where d is the inverse of e mod $\Phi(n)$. The Euler totient function $\Phi(n)$ for this case can be defined as

$$\Phi(n) = \bar{p} \cdot \bar{q} \tag{4}$$

where

$$\bar{p} = \begin{cases} p^3 + p^2 + p + 1, & \text{if } f(x) \text{ modulo } p \text{ is an irreducible quartic polynomial} \\ p^3 - 1, & \text{if } f(x) \text{ modulo } p \text{ is an irreducible cubic polynomial times a linear factor} \\ p^2 - 1, & \text{if } f(x) \text{ modulo } p \text{ is an irreducible quadratic polynomial times two linear factors} \\ p + 1, & \text{if } f(x) \text{ modulo } p \text{ is two irreducible quadratic polynomials} \\ p - 1, & \text{if } f(x) \text{ modulo } p \text{ is four linear factors} \end{cases}$$

with $f(x) = x^4 - c_1 x^3 + c_2 x^2 - c_3 x + 1$. Similarly for $\bar{q}$.

Thus, the decryption function define as

$$\begin{aligned} & D(c_1, c_2, c_3) \\ & \equiv (V_d(c_1, c_2, c_3, 1), \\ & \quad V_d(c_2, c_1 c_3 - 1, {c_1}^2 + {c_3}^2 - 2c_2, c_1 c_3 - 1, c_2, 1), \\ & \quad V_d(c_3, c_2, c_1, 1)) \bmod n \\ & \equiv (m_1, m_2, m_3) \bmod n, \end{aligned} \tag{5}$$

which recovers the original plaintexts (m_1, m_2, m_3).

Methodology

The Hastad's attack is used Hastad's Theorem to show that using RSA with low public exponent is insecure if the users are sending linearly related plaintexts over a large network [Hastad].

Theorem 1 (Hastad's Theorem): Let $N = \prod_{i=1}^{k} n_i$ and $n = \min_{1 \le i \le k} n_i$. Given a set of k equations $\sum_{j=0}^{\delta} a_{i,j} x^j \equiv 0 \bmod n_i$ where the moduli n_i are pairwise relatively prime and $\gcd\left(\left\langle a_{i,j} \right\rangle_{j=0}^{\delta}, n_i\right) = 1$ for all i. Then it is possible to find $x < n$ in polynomial time if $N > 2^{(\delta+1)(\delta+2)/4} (\delta+1)^{\delta+1} n^{\delta(\delta+1)/2}$.

Proof: See [Joye], page 42, Corollary 3.2.■

In 1996, Coppersmith extended the result from Hastad's theorem that eventually becomes the Coppersmith's theorem [Coppersmith]. This theorem is specific for a monic integer polynomial of degree δ.

Theorem 2 (Coppersmith's Theorem): Let a monic integer polynomial $P(x)$ of degree δ and a positive integer N of unknown factorization. In time polynomial in $\log N$ and δ, we can find all integer solutions x_0 to $P(x_0) \equiv 0 \bmod N$ with $|x_0| < N^{1/\delta}$.

Proof: See [Coppersmith], page 159, Corollary 2.■

Joye had improved the Hastad's theorem as follows [Joye]:

Theorem 3: Consider a system of k modular polynomial equations of degree $\leq \delta$ with l variables given by

$$\sum_{j_1,j_2,\ldots,j_l=0}^{j_1+j_2+\cdots+j_l\leq\delta} a_{i,j_1,j_2,\ldots,j_l} x_1^{j_1} x_2^{j_2} \ldots x_l^{j_l} \equiv 0 \bmod n_i \,, \tag{6}$$

for $i = 1, \ldots, k$ and where $x_1, \ldots, x_l < n$ and $n = \min_{1\leq i\leq k} n_i$. Let $N = \prod_{i=1}^{k} n_i$, $f = \sum_{m=1}^{\delta} m \binom{m+l-1}{m}$ and $g = \sum_{m=0}^{\delta} \binom{l+m-1}{m}$, if the moduli n_i are coprime, then $\gcd\left(\left\langle a_{i,j_1,j_2,\ldots,j_l}\right\rangle_{j_1,j_2,\ldots,j_l}^{j_1+j_2+\cdots+j_l\leq\delta}, n_i\right) = 1$ for $i = 1,\ldots, k$ and if

$$N > 2^{g(g+1)/4} g^g n^f \,, \tag{7}$$

the result is in polynomial time a real-valued equation which is equivalent to Equation (6).
Proof: See [Joye], pages 40-42, Theorem 3.1.■

Attack on LUC4,6 Cryptosystem

Suppose that $N = \prod_{i=1}^{k} n_i$ and $n = \min_{1\leq i\leq k} n_i$. Let m_1, m_2 and m_3 are a set of the plaintexts of $LUC_{4,6}$ cryptosystem, then $m_{1,i} \equiv \alpha_i m_1 + \beta_i \bmod n_i$, $m_{2,i} \equiv \alpha_i m_2 + \beta_i \bmod n_i$, and $m_{3,i} \equiv \alpha_i m_3 + \beta_i \bmod n_i$. Therefore, the ciphertexts are

$$c_{1,i} \equiv V_{e_i}(\alpha_i m_1 + \beta_i, \alpha_i m_2 + \beta_i, \alpha_i m_3 + \beta_i, 1) \bmod n_i \,, \tag{8}$$

$$\begin{aligned} c_{1,i} \equiv V_{e_i}(&\alpha_i m_2 + \beta_i, (\alpha_i m_1 + \beta_i)(\alpha_i m_3 + \beta_i) - 1, (\alpha_i m_1 + \beta_i)^2 + (\alpha_i m_3 + \beta_i)^2 - 2(\alpha_i m_2 + \beta_i), \\ &(\alpha_i m_1 + \beta_i)(\alpha_i m_3 + \beta_i) - 1, \alpha_i m_2 + \beta_i, 1) \bmod n_i \,, \end{aligned} \tag{9}$$

$$c_{3,i} \equiv V_{e_i}(\alpha_i m_3 + \beta_i, \alpha_i m_2 + \beta_i, \alpha_i m_1 + \beta_i, 1) \bmod n_i \,. \tag{10}$$

Since the Hastad'd attack is relied on the polynomial structure, then the Lucas sequence should be transform to polynomial. In this situation, the Dickson polynomial [Dickson] is able to transform it. That mean, the fourth order and sixth order of Dickson polynomials and Lucas sequences both are equivalent.

Proposition 1: The fourth order Lucas sequence are equivalent to the three variables of Dickson polynomials, which is defined as

$$V_{e_i}(x,y,z,1) = D_{e_i}(x,y,z,1)$$
$$= \sum_{i=0}^{\left\lfloor \frac{e_i}{2} \right\rfloor} \sum_{j=0}^{\left\lfloor \frac{e_i}{3} \right\rfloor} \sum_{k=0}^{\left\lfloor \frac{e_i}{4} \right\rfloor} \left(\frac{e_i(-1)^{i+k}}{e_i - i - 2j - 3k} \right) \binom{e_i - i - 2j - 3k}{i + j + k} \binom{i + j + k}{i + j} \binom{i + j}{i} x^{e_i - 2i - 3j - 4k} y^i z^j, \quad (11)$$

where $2i + 3j + 4k \le e_i$.

Proof: See [Wong ,2011], page 44, Proposition 3.5. ■

Proposition 2: The sixth order Lucas sequence is equivalent to the five variables of Dickson polynomials, which is define as

$$V_{e_i}(x_1,x_2,x_3,x_4,x_5,1) = D_{e_i}(x_1,x_2,x_3,x_4,x_5,1)$$
$$= \sum_{i_1=0}^{\left\lfloor \frac{e_i}{2} \right\rfloor} \sum_{i_2=0}^{\left\lfloor \frac{e_i}{3} \right\rfloor} \sum_{i_3=0}^{\left\lfloor \frac{e_i}{4} \right\rfloor} \sum_{i_4=0}^{\left\lfloor \frac{e_i}{5} \right\rfloor} \sum_{i_5=0}^{\left\lfloor \frac{e_i}{6} \right\rfloor} \left(\frac{e_i(-1)^{i_1+i_3+i_5}}{e_i - i_1 - 2i_2 - 3i_3 - 4i_4 - 5i_5} \right)$$
$$\times \binom{e_i - i_1 - 2i_2 - 3i_3 - 4i_4 - 5i_5}{i_1 + i_2 + i_3 + i_4 + i_5} \binom{i_1 + i_2 + i_3 + i_4 + i_5}{i_1 + i_2 + i_3 + i_4} \binom{i_1 + i_2 + i_3 + i_4}{i_1 + i_2 + i_3} \quad (12)$$
$$\times \binom{i_1 + i_2 + i_3}{i_1 + i_2} \binom{i_1 + i_2}{i_1} x_1^{e_i - 2i_1 - 3i_2 - 4i_3 - 5i_4 - 6i_5} x_2^{i_1} x_3^{i_2} x_4^{i_3} x_5^{i_4},$$

where $2i_1 + 3i_2 + 4i_3 + 5i_4 + 6i_5 \le e_i$.

Proof: See [Wong ,2011], page 45-46, Proposition 3.6. ■

By Proposition 1and Proposition 2, equations (8), (9), and (10) can be considered as polynomials in m_1, m_2 and m_3 of degree e_i.

For Hastad's Theorem, there is a variable to be considered. However, the $LUC_{4,6}$ cryptosystem had three variables. Therefore, there are necessary to modify the Hastad's Theorem.

Corollary 1: Let $N = \prod_{i=1}^{k} n_i$ and $n = \min_{1 \le i \le k} n_i$. Given a set of k equations

$$\sum_{j_1, j_2, j_3 = 0}^{j_1 + j_2 + j_3 \le \delta} a_{i, j_1, j_2, j_3} x_1^{j_1} x_2^{j_2} x_3^{j_3} \equiv 0 \bmod n_i \quad (13)$$

where the moduli n_i are pairwise relatively prime and $\gcd\left(\left\langle a_{i,j_1,j_2,j_3} \right\rangle_{j_1,j_2,j_3}^{j_1+j_2+j_3 \le \delta}, n_i \right) = 1$ for all i. Then it is possible to find $x < n$ in polynomial time if

$$N > 2^{\frac{(\delta+1)(\delta+2)(\delta+3)(\delta+4)(\delta^2+2\delta+3)}{144}} \left(\tfrac{1}{6}(\delta+1)(\delta+2)(\delta+3) \right)^{\frac{1}{6}(\delta+1)(\delta+2)(\delta+3)} n^{\frac{1}{8}\delta(\delta+1)(\delta+2)(\delta+3)}. \quad (14)$$

Proof: In three variables case for Theorem 3,

$$f = \sum_{m=1}^{\delta} m \binom{m+2}{m} = \frac{1}{8}\delta(\delta+1)(\delta+2)(\delta+3), \quad (15)$$

and

$$g = \sum_{m=0}^{\delta} m\binom{m+2}{m} = \frac{1}{6}\delta(\delta+1)(\delta+2)(\delta+3). \tag{16}$$

Then, substitute Equations (15) and (16) into Equation (7), get Equation (14). ■

Corollary 2: In the $LUC_{4,6}$ cryptosystem, a set of k linearly related plaintexts can be recovered if

$$k > \tfrac{1}{8}e(e+1)(e+2)(e+3) \tag{17}$$

and

$$n_i > 2^{\frac{(e+1)(e+2)(e+3)(e+4)(e^2+2e+3)}{144}}\left(\tfrac{1}{6}(e+1)(e+2)(e+3)\right)^{\frac{1}{6}(e+1)(e+2)(e+3)}, \tag{18}$$

where $e = \max_{1\le i\le k} e_i$.

Proof: The proving for this corollary is to verify that the conditions of Corollary 1 are fulfilled. From the k sets of ciphertexts, there exist k equations

$$P_{1,i}(m_1,m_2,m_3) \equiv D_{e_i}(\alpha_i m_1+\beta_i, \alpha_i m_2+\beta_i, \alpha_i m_3+\beta_i, 1) - c_{1,i} \equiv 0 \bmod n_i, \tag{19}$$

$$\begin{aligned} P_{1,i}(m_1,m_2,m_3) \equiv\ & V_{e_i}(\alpha_i m_2+\beta_i, (\alpha_i m_1+\beta_i)(\alpha_i m_3+\beta_i)-1, \\ & (\alpha_i m_1+\beta_i)^2+(\alpha_i m_3+\beta_i)^2-2(\alpha_i m_2+\beta_i), \\ & (\alpha_i m_1+\beta_i)(\alpha_i m_3+\beta_i)-1, \alpha_i m_2+\beta_i, 1) - c_{2,i} \bmod n_i \\ \equiv\ & 0 \bmod n_i, \end{aligned} \tag{20}$$

$$P_{3,i}(m_1,m_2,m_3) \equiv D_{e_i}(\alpha_i m_3+\beta_i, \alpha_i m_2+\beta_i, \alpha_i m_1+\beta_i, 1) - c_{3,i} \equiv 0 \bmod n_i. \tag{21}$$

Suppose that the moduli n_i are pairwise coprime and also that the coefficients of polynomials $P_{1,i}(m_1,m_2,m_3)$, $P_{2,i}(m_1,m_2,m_3)$, and $P_{3,i}(m_1,m_2,m_3)$ are relatively prime to n_i; otherwise the plaintexts can be recovered by factoring n_i.

Since $k > \frac{1}{8}e(e+1)(e+2)(e+3)$ and $n_i > 2^{\frac{(e+1)(e+2)(e+3)(e+4)(e^2+2e+3)}{144}}\left(\frac{1}{6}(e+1)(e+2)(e+3)\right)^{\frac{1}{6}(e+1)(e+2)(e+3)}$, it follows

$$N = \prod_{i=1}^{k} n_i \ge \prod_{2}^{\frac{1}{8}e(e+1)(e+2)(e+3)+1} n_i > 2^{\frac{(e+1)(e+2)(e+3)(e+4)(e^2+2e+3)}{144}}\left(\tfrac{1}{6}(e+1)(e+2)(e+3)\right)^{\frac{1}{6}(e+1)(e+2)(e+3)} n^{\frac{1}{8}e(e+1)(e+2)(e+3)} \tag{22}$$

where $n = \min_{1\le i\le k} n_i$. ■

Coppersmith based variation method is based on the Coppersmith's theorem which is defined in Theorem 2. With this method, sending more than e linearly related plaintexts that are encrypted via RSA or LUC cryptosystem with encryption key, e and RSA-moduli n_i is dangerous. However, this method cannot be directly applied to $LUC_{4,6}$ cryptosystems. This is because one of the conditions in Coppersmith's theorem is that the polynomial, which is analyzed should be a monic polynomial, but the polynomials in $LUC_{4,6}$ cryptosystems are multivariable polynomials.

Nevertheless, Julta improved the theorem to multivariable polynomials [Julta] in 1998. In that article, the author states the following:

"Let $P(x_1,\ldots,x_m) \equiv 0 \bmod N$ be a modular multivariable polynomial equation, in m variables, and total degree k with a root $x_{0,i}$, for $1 \le i \le m$. Let $|x_{0,i}| < N^{\alpha_i}$, $\sum \alpha_i < 1/k$ and k linear independent integer polynomial equations (in m variables) of total degree polynomial in $mk \log N$, in polynomial time in $mk \log N$, such that each of the equations has $x_{0,i}$ as a root."

Therefore, all integer solution $x_{0,i}$ to $P(x_1,\ldots,x_m) \equiv 0 \bmod N$ can be found with $|x_{0,i}| < N^{1/k}$.

Based on Corollary 2, the number of plaintexts are required to succeed the Hastad'd attack for the $LUC_{4,6}$ cryptosystem can be found. The comparison of the requirement of the number of plaintexts between RSA, LUC, LUC_3 and $LUC_{4,6}$ had been shown in Table 1.

Table 1 : The number of plaintexts, k required to succeed the Hastad's Attack

e	3	5	7	11	13	17	19
RSA	7	16	29	67	92	154	191
LUC	7	16	29	67	92	154	191
LUC_3	21	71	169	573	911	1939	2661
$LUC_{4,6}$	46	211	631	3004	5461	14536	21946

Table 1 show that the requirement of the number of plaintexts to succeed the Hastad's attack for the $LUC_{4,6}$ cryptosystem is the highest. That mean the $LUC_{4,6}$ cryptosystem is more secure than RSA, LUC and LUC_3 cryptosystems. For $LUC_{4,6}$ cryptosystem, if public key, $e = 19$, at least 21946 plaintexts is required to hack the $LUC_{4,6}$ cryptosystem using Hastad's attack. If the cryptosystem is 128-bit, how many number of plaintext is required? It is almost 504 bits of number.

Conclusion

For $LUC_{4,6}$ cryptosystem, Dickson polynomial is enabling the Lucas sequence to transform into multivariate polynomial. When the plaintexts transform from the sequence to the polynomial, then the number of plaintexts are required to succeed the Hastad'd attack can be found. By Coppersmith based variation and the statement from Julta, we can conclude that the result of sending more than e linearly related plaintexts that are encrypted via $LUC_{4,6}$ cryptosystem with encryption key, e and RSA-moduli n_i is dangerous.

References:

Coppersmith, D (1996). Finding a Small Root of a Univariate Modular Equation. *Lecture Notes in Computer Science* 1070, 155-165.

Dickson, L.E (1897). The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *The Annals of Mathematics* 11(1/6): 65–120; 161–183.

Hastad, J (1986). On using RSA with low exponent in a public key network. *Lecture Notes in Computer Science,* 218, 404-408.

Joye, M (1997). *Security Analysis of RSA-type Cryptosystems*. PhD Thesis, Universite Catholique de Louvain, Belgium.

Julta, C.S (1998). On Finding Small Solutions of Modular Multivariate Polynomial Equations. *Lecture Notes in Computer Science,* 1403:158-170.

Wong, T.J., Said, M.R.M., Atan, K.A.M. and Ural, B. (2007). The Quartic Analog to the RSA Cryptosystem. *Malaysian Journal of Mathematical Sciences* 1(1), 63-81.

Wong, T.J. (2011). *A RSA-type Cryptosystem Based on Quartic Polynomials*, PhD Thesis, Universiti Putra Malaysia, Malaysia.

A NEW SPATIAL-DOMAIN STEGANOGRAPHIC METHOD FOR COLORED IMAGES

Samer Atawneh and Putra Sumari
Univeristi Sains Malaysia (USM)
satawneh@yahoo.com, putras@cs.usm.my

Abstract:

As vast communication networks like Internet become popular, and with thousands of digital files are downloaded and uploaded daily, information hiding techniques increasingly become widespread, and secure communications become a greater concern. Steganography plays an increasing role in the security of transmitting confidential information. This paper presents a new hiding technique that exploits the spatial domain of colored-raw images to hide high capacity of secret information. The cover image is virtually divided into disjoint parts with each part's size equals the size of the secret message. Each pixel from the secret message is to be hidden in the best pixel among the corresponding pixels' bytes in the parts of the cover image. The Experimental results are presented and show that the proposed method gives high embedding capacity and reserves the image quality.

Introduction to Steganography

The art of hiding secret, confidential, messages within digital media files like text, audio, image, and video in such a way that other parties except the intended recipient(s) can't notice the hidden message is widely known as steganography. Only the intended recipient can extract the hidden message correctly from the stego-media. As derived from Greek, steganography means "Covered Writing".

Steganography has a variety of applications; some of the most interesting ones are authentication, ownership protection, annotation [2], TV broadcasting, medical images systems [3, 4, 5], and enhanced data structures [6]. Also, steganography could be used for dissident and criminal organizations [7].

Nowadays, steganography has important roles in security field. Hundreds of steganographic tools and methods were developed to increase the privacy and security of multimedia files. Both steganography and cryptography are used to protect information. The cryptography is used to scramble a message, using a crypto-key, so it becomes meaningless. Two disciplines can be used together and give a system that can benefit of the advantages of both. Better security can be reached if the secret information is encrypted before hiding it. The practice of altering a media, in an imperceptible way, to add information about that media is known as watermarking [7]. Watermarks have many properties, most important are imperceptible and do not get separated or removed when media is converted or transformed [7].

Figure 1 below shows the main processes of steganography:

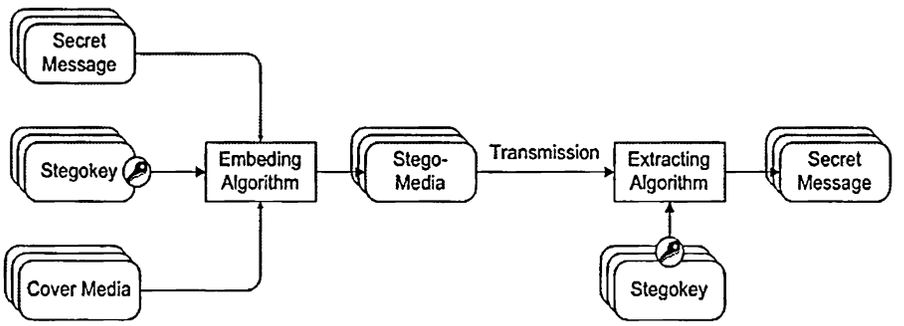


Figure 1 : Steganography technique

Different properties characterize the strength and weakness of steganographic methods; the most important are capacity, robustness, imperceptibility, undetectability, and security [7, 8, 9]. The size of message that can be hidden relative to the size of the carrier is known as capacity. One of the main challenges of steganography is to hide high

capacity. Robustness means that the hidden information can be reliably extracted after the cover-media has been modified. The hidden information should be Imperceptible and does not introduce a significant degradation in the quality of the cover-media. The embedded information is undetectable if the stego-media is consistent with the carrier. The embedding algorithm is said to be secure if the embedded information cannot be removed beyond reliable detection by the targeted attacks.

Based on the available information for analysis, different types of steganographic attacks can be defined; some of them are known-cover attack, steganography-only attack, known-message attack, and known-steganography attack [10]. Discovering the presence of hidden messages is known as steganalysis. The two main categories of steganalysis are targeted and blind [7].

The paper is organized as follows: Section 2 describes different information hiding techniques. Section 3 shows the proposed technique to hide in colored images. Section 4 concludes the paper.

Information Hiding Techniques

Steganographic methods can be categorized in different ways. Abbas Cheddad in his survey paper [11] gives a standard categorization by grouping the methods into spatial domain, frequency domain, and adaptive techniques. Adaptive methods are considered as special cases as they can be implemented in spatial or frequently domains. Other scholars categorize steganographic techniques according to the cover-media that is used in hiding [12]. Here, steganographic methods can be grouped into 5 different categories: Text steganography, Audio steganography, Image steganography, Video steganography, and Protocol steganography. Others also use executable files as covers for steganography.

Steganography in text has three main techniques [1]: line-shift coding where text lines are shifted vertically to encode the document uniquely. Word-shift coding where code-words are coded into a document by shifting the horizontal locations of words within text lines, while maintaining a natural spacing appearance. Feature coding where certain text features are altered, or not altered, depending on the codeword.

Digital images are one of the most popular media on the Internet; they are good candidates of cover media for secret communication. When hiding data into an image, the values of pixels in the image are modified according to the data to be embedded [13].

Any image, text or anything that can be embedded in a bit stream can be hidden in an image. Image-based steganography has come quite far in recent years with the development of fast, powerful graphical computers. An image can be represented as an array of numbers that represent light intensities at various points (pixels). These pixels make up the image's raster data. Each pixel contains information as to the intensity of the three primary colors, red, green, and blue. This information can be stored in a single byte (8 bits) or in three bytes (24 bits). For example, in an 8-bit image, white is represented by the binary value 11111111 and black by the binary value 00000000. In 24-bit image, each byte corresponding to one of the three colors and each three-byte value fully describes the color and luminance values of one pixel [1]. A high resolution image, 1024 x 768 pixels and 24-bit color can hide approximately 2.36 MBs of data. Thus high resolution images are preferred for use as cover images because they have the most space to hide information in.

To enable embedded information in an image to be imperceptible, the image should be distorted as slightly as possible. Usually, the more we embed data into an image, the more the image is distorted [13]. It is important to use images that do not contain large blocks of a solid color, as the changed bits in the solid area are easier to detect [1]. Care needs to be taken in the selection of the carrier image, so that changes to the data will not be visible in the stego-image. Common images should not be used.

The most well known techniques to information hiding in images are least significant bit (LSB) substitution, and masking and filtering techniques. LSB is a simple approach to embedding information in an image. But image manipulation can destroy the hidden information in this image. Applying LSB technique to each byte of an 8-bit image, only one bit can be encoded into each pixel, as each pixel is represented by one byte. Applying LSB technique to each byte of a 24-bit image, three bits can be encoded into each pixel, as each pixel is represented by

three bytes. Masking and filtering techniques are mostly used in 24 bit and grayscale images. These hide information in a way similar to watermarks on actual paper and are sometimes used as digital watermarks [12].

Ching-Chiuan Lin [13] proposed a new scheme for embedding a message into a grayscale image and obtain minimal image distortion for applications which need a high-visual-quality stego-image. Cheng-Hsing Yang [14] proposed a new scheme for embedding data in an image using pixel value differencing (PVD). The PVD scheme embeds data by changing the difference value between two adjacent pixels so that more data is embedded into two pixels located in the edge area, than in the smooth area. Two pairs of pixels in a block are processed at the same time instead of processing a pair of pixels as in [15].

The most well known techniques to information hiding in audio are least significant bit insertion, phase coding, spread spectrum coding, and echo hiding [1]. As data is stored in the least significant bit of images, binary data can be stored in the least-significant bit of audio files. This method has poor immunity to manipulation. Factors such as channel noise and re-sampling can easily destroy the hidden signal.

Video steganography can be used to design the large-capacity security communication based on steganography systems. Consequently, video steganography and steganalysis are becoming the next hotspot in the area of information security [16].

Digital video files are collection of images and sounds, so most of the known techniques of image-based and audio-based steganography can be applied to digital video files [12]. One advantage of video file is the large amount of information that can be hidden inside it. With continuous flow of information in the digital video file, any distortions (if exists) might be unobserved by human eyes. Hiding information in digital video files can be done using different techniques. The popular and simple technique is the LSB, where the LSB bit of one byte in the frame is used to hide the secret information. DCT (Discrete Cosine Transform) technique changes the video file by altering values of certain parts of the frames.

Hiding Grayscale Images in Colored-Raw Images Technique

One of the main issues in steganography is to have high capacity (high payload) without degrading the quality of the stego-image. It is a challenge because embedding more information can destroy the quality of the image. Therefore, in this paper we present a new hiding technique that exploits the spatial domain of colored-raw images to hide high capacity of secret information. The cover image is virtually divided into disjoint parts with each part's size equals the size of the secret message. Each pixel from the secret message (the gray-scale image) is to be hidden in the best pixel among the corresponding pixels' bytes in the parts of the cover image. Selecting the best pixel to hide in depends on a predefined threshold after calculating the minimum difference between the selected pixels.

Suppose that the pixel from the secret image to be hidden is m_{ij} and the cover is divided into n different parts, then m_{ij} is compared with the three bytes of each corresponding pixel c_{ij} in the n parts. Let the threshold t be the maximum accepted difference between the pixel's value to embed and one of the corresponding pixel's values of the cover. For imperceptibility matter, t should be as small as possible. Select one of the best pixel's bytes to embed m_{ij}. Best pixels' bytes are the bytes that give minimum t, i.e. $|c_{ij}$ ' byte $- m_{ij}| \leq t$. After determining the set of all best pixels' values for each pixel m_{ij}, selecting one of them for embedding process can be randomly or depends on predefined criteria.

As a numerical example, suppose that the pixel m_{ij} to embed has a value 250, and the three bytes for each of the corresponding pixels are: 230, 248, 249; 260, 248, 170; 271, 202, 210; 254, 211, 201; 228, 210, 239; 232, 235, 240; 252, 190, 210; 273, 233, 217; and 253, 211, 250 (Here the cover image is divided into 9 parts). Suppose that the threshold t is selected to be 2, i.e. the maximum difference between m_{ij} and any corresponding c_{ij}'s byte doesn't exceed 2. Then the set of best pixels' values for m_{ij} is {248, 249, 248, 252, 250}. Here, any criteria can be used to select one of these values to embed the pixel 250.

Figure 2 shows the pixel (i,j) in the embedding image and the corresponding 9 pixels in the cover image.

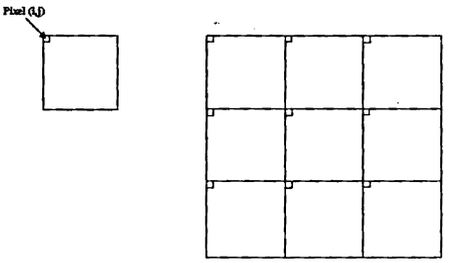


Figure 2 : Embedding a pixel in one byte of the corresponding pixels of the cover

Figure 3 below shows the used embedding grayscale image. Figure 4 shows the colored cover image to embed in before the embedding process, and Figure 5 shows the stego-image after embedding. The Experimental results show that the proposed method gives high embedding capacity and reserves the image quality (PSNR = 48.0601 dB).

Figure 3 : The embedding image (LENA image)

Figure 4 : The cover image before embedding (PEPPERS image)

Figure 5: The cover image after embedding (the stego-media), PSNR = 48.0601

Conclusion

In this paper we presented a new hiding algorithm that exploits the spatial domain of colored images to hide high capacity of secret information. The cover image is virtually divided into disjoint parts with each part's size equals the size of the secret message. Each pixel from the secret image is to be hidden in the best pixel among the corresponding pixels' bytes in the parts of the cover image. The Experimental result with PSNR equals 48.0601 dB shows that the proposed method reserves the image quality and gives high embedding capacity.

References:

Atawneh, S. (2006). A New Algorithm for Hiding Gray Images using Blocks, Information and Communication Technologies, *ICTTA '06. 2nd, vol.1, pp.1484-1488, 0-0 0 doi: 10.1109/ICTTA.2006.1684601* URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1684601&isnumber=35470

Wu, M. Liu, B. (2003). Data hiding in image and video. I. Fundamental issues and solutions. *Image Processing, IEEE Transactions*), 685-695.

Cheddad A., Condell J., Curran K., Kevitt P. (2008). Enhancing Steganography in Digital Images, *Canadian Conference on Computer and Robot Vision*, pp. 326-332.

Al-Qershi O. M., Khoo B. E. (2011). High capacity data hiding scheme for medical images based on difference expansion, *The Journal of Systems and Software*, pp. 105–112.

Lou D., Hu M., Liu J. (2009) Multiple layer data hiding scheme for medical images, *Computer Standards & Interfaces*, pp. 329–33.

Wayner, P. (2009). Disappearing cryptography: information hiding: steganography & watermarking. *Morgan Kaufmann*, Third Edition.

Cox I. J., Miller M. L., Bloom J. A., Fridrich J., Kalker T. (2008). Digital Watermarking and Steganography. (Second Edition).

AL-Ani, Z. K., Zaidan, A., Zaidan, B. and Alanazi, H. (2010). Overview: Main fundamentals for steganography. *Arxiv preprint arXiv:1003.4086).*

Lin E. T., Delp E. J. (1999). A Review of Data Hiding in Digital Images, Proceedings *of the Image Processing, Image Quality, Image Capture Systems Conference (PICS '99)*, Savannah, Georgia, pp. 274-278.

Das, S., Bandyopadhyay, B. and Sanyal, S. (2008). Steganography and Steganalysis: different approaches. *International Journal of Computers, Information Technology and Engineering (IJCITAE), 2).*

Cheddad, A., Condell, J., Curran, K. and Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing,* 90), 727-752.

Bandyopadhyay S. K., Bhattacharyya D., Ganguly D., Mukherjee S., Das P. (2008). A Tutorial Review on Steganography, *International Conference on Contemporary Computing (IC3-2008),* Noida, India, pp. 105-114.

Lin C. (2011). An information hiding scheme with minimal image distortion, Computer Standards & Interfaces, *In Press, Corrected Proof, Available online 21 February 2011,* ISSN 0920-5489, DOI: 10.1016/j.csi.2011.02.003.

Yang C., Weng C., Tso H., Wang S. (2011). A data hiding scheme using the varieties of pixel-value differencing in multimedia images, *Journal of Systems and Software,* Volume 84, Issue 4, The Ninth International Conference on Quality Software, Pages 669-678, ISSN 0164-1212, DOI: 10.1016/j.jss.2010.11.889.

Wu, D.C., Tsai, W.H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters* 24, 9–10, 1613–1626.

Su Y., Zhang C., Zhang C. (2011). A video steganalytic algorithm against motion-vector-based steganography, *Signal Processing,* In Press, Corrected Proof, Available online 24 February 2011, ISSN 0165-1684, DOI: 0.1016/j.sigpro.2011.02.012.

DIGITAL WATERMARKING: A COUNTERFEITING AND PIRACY DETERRENCE

R. F. Olanrewaju[1], Othman Khalifa[1] and Akram M. Zeki[2]
[1]*Department of Electrical & Computer Engineering, Faculty of Engineering,*
[2]*Faculty Information & Communication Technology,*
International Islamic University Malaysia
Kuala Lumpur Malaysia,
[1]*frashidah@yahoo.com*

Abstract:

Counterfeiting and piracy are among substantial oldest problems associated with intellectual properties. With the advent of interconnected networks nowadays, the problems are expanding in scope and magnitude as well as increasing economic and social impact. The negative impacts of this development on associated industries and their employees have raised economic, health, safety and security concerns for both governments and consumers. Digital Watermarking (DW), an imperceptibly altering of host media to embed message or marks about the host itself can be effectively used to limit the scope of counterfeiting and piracy of digital media. This paper presents statistically, the extent of piracy and counterfeiting on digital media especially on software, music, e-books and pharmaceutical products. It also presents the current research finding and output of curbing piracy through the applications of watermarking to enhance owner's ability to detect and respond to misuse of digital media. The result of findings indicated that digital watermarking can help deter piracy and authenticate digital media extensively.

Keywords- digital watermarking; counterfeiting; digital piracy; software watermarking .

Introduction

Counterfeiting and piracy of intellectual properties are often pointed to as an indispensable problems across the globe, virtually in all sectors of the global economy, though more intense in some region than others. Pirated and counterfeit products are produced and sold in underground economies or in markets where they go unregulated and escape normal tax and tariff payments (BASCAP, 2009). Such products expose consumers to health, safety and quality risks and impose costs on society at large, in terms of employment, crime and social services.
Currently over millions of digital images, songs, games, software and videos are copied illegally during file-sharing over the networks. Right owners such as Software engineers, artists, writers and producers have been searching for ways to protect their creations, discoveries and inventions. Digital Rights Management (DRM) systems that prevent copying have raised fair use issues, This is because they do not only block copying illegally but prevent legitimate consumers from making back-up copies [1]. These challenges prompted significant research to develop efficient methods to protect copyright and authentication messages in digital media in order to prevent forgery and impersonation (Olanrewaju, 2011).

One of the oldest and common tools available for protecting copyrighted material and intellectual properties is by means of encryption. Encryption protects contents particularly during transmission of data from sender to receiver. However, once it reaches a recipient and decrypted, the protection ends and the data can be copied and redistributed without further complications. Moreover, encryption cannot help the developer or software vendor to monitor how legitimate customers handle the multimedia content after decryptions (Busch, Graf, Wolthusen, and Zeidler, 2000; Olanrewaju, Khalifa, Abdalla and Aburas, 2010). This is because the object loses its protection once it is decrypted and can then be distributed, freely. Consequently, mishandling of sensitive information cannot be prevented effectively by this traditional means. Figure 1 shows how image is illegally copied after decryption.

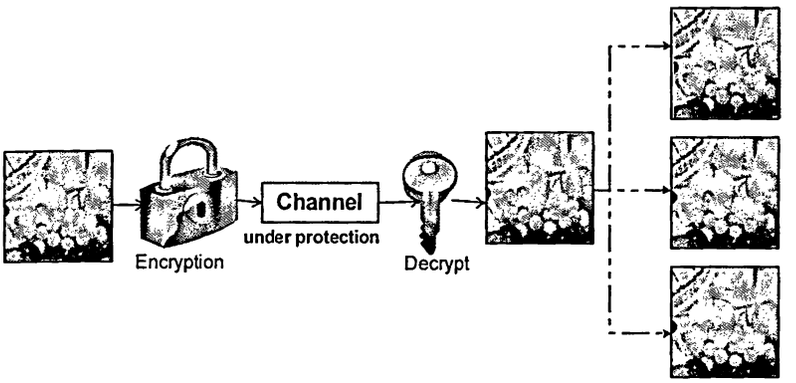


Figure 1 : Lost of protection after decrypting digital image (Source; Olanrewaju et al 2010)

Watermarking, in contrast, have been used for centuries to prove the authenticity of bank notes, postage stamps and documents (Olanrewaju 2011). Recently, Digital Watermarking (DW) is a tool use to fight against digital piracy, to authenticate and verify the integrity of digital media. Though watermarking does not prevent copying, but depending on the application, it helps both consumers and producers to differentiate what content is authentic and what is counterfeit. DW is also use in monitoring and tracking illegal copies of digital media, filtering, communicating copyright message and deter alteration of multimedia content (Hirakawa & Iijima, 2011; Olanrewaju, Khalifa, Abdulla, & Khedher, 2011).

DW which provides a continual digital identity for audio, video, images and texts is currently deployed in billions of audio, video, image and print objects and hundreds of millions of watermarked enabled applications (Digital Watermarking Alliance, 2010). Figure 2 shows the block diagram of DW scheme with embedding and extracting block.

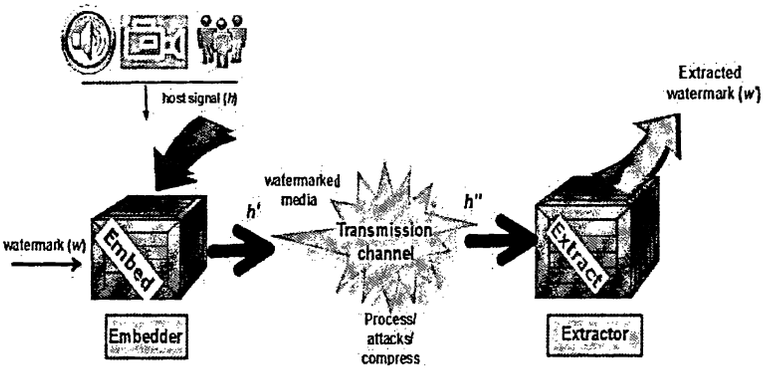


Figure 2 : Generic Digital watermarking scheme with embedding and extracting block

Digital watermarking has become a matter of more concern over the past few years and preferable to other traditional method of protecting data integrity and authentication of information resources. This is due to crucial features such as imperceptibility, inseparability of the content from the watermark, and intrinsic ability to undergo same transformation experienced by the host signal, which digital watermark possesses. This preference has been established to provide improved security (Olanrewaju, Aburas, Khalifa & Abdalla, 2009).

Factors Affecting Production and Consumption of Counterfeit and Pirated Goods.

Digitization of audio visual media has made it worse for pirated and counterfeit goods. In this digital era recording technology, copied of audio material is same as the original copy while the quality of the copied media are still good. Another factor is the acceleration of the Global digital growth rate. For example Digital music revenues companies grew by 8 per cent globally in 2011 to an estimated US$5.2 billion compares to growth of 5 per cent in

2010. Furthermore, digital channels are now accounting for an estimated 32 per cent of record company revenues globally, up from 29 per cent in 2010 (IFPI, 2012; Lovorgna, 2012). The proportion of digital sale revenues is as shown in Figure 3.

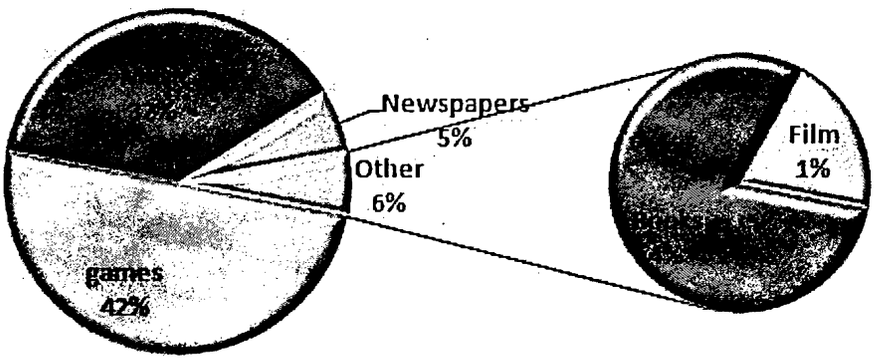


Figure 3 : Proportion of industries' global revenues coming from digital sales (2011), Source (*PWC Global Entertainment & Media Outlook and IFPI*)

Furthermore, on the consumer side, the readily availability of latest and most popular realise of new items such as buying it earlier than the licensed copies appeared (CD/DVD/software/audio-video cassettes). In music, it has a relatively low price and low risk of persecution. While producer of pirated goods are attracted to low cost of production as well as low legal risk.

Another factor is the Patents, the rationale behind patents was to provide an incentive for creative inventors to share their inventions with the nation as a whole. However, it seems that the patents system is broken. The cost of pursuing or defending against a patent lawsuit starts at about $2million, making patents almost exclusively for only large corporations (Orion, 2011).

Other contributing factors are globalization of international trade, lack of public education, sophistication of technology and means of communications that make pirates product fast and easy to buy and sell, as well as development of reprographic technologies (Croze, 2007).

Real Cost Of Piracy and Counterfeiting

The fight against digital media piracy and counterfeiting remains a critical issue all over the globe. The negative impact of this development on associated industries is very high that it is very difficult to quantify the exact cost of damages and it effect on the economy. It is difficult to assess precisely the real scale of the phenomenon of counterfeiting and piracy (Blakeney, 2009) due to primarily lack of available data and incomplete data on the extent and value of counterfeit trade. Counterfeiting and piracy are illicit activities, which makes data on them inherently difficult to obtain and has resulted in assessments.

Since counterfeiting operates outside the law, estimating the exact level of counterfeiting and the harm it brings is extremely challenging. Illegal businesses do not report any information on their activities to any government agency and therefore measures of the size of illegal businesses, such as total illegal sales or the income earned by these businesses must be estimated by indirect methods ().

This view is shared by recent studies and reports produced by the Organization for Economic Cooperation and Development (OECD) and the United States Government Accountability Office (Villarroel, 2010). According to 2008 report by the OECD, " We rely excessively on fragmentary and anecdotal information; where data are lacking, unsubstantiated opinions are often treated as fact." (Mencher 2010). The United States Government Accountability Office (GAO) also highlights the absence of measurement of both the negative and positive impacts of piracy. According to its report, the lack of official studies and analysis is due to the fact that governments have not yet set up appropriate institutions for systematic data analysis (GAO, 2010).

The U.S. Department of Commerce and FBI officials noted that they rely on industry statistics and do not conduct any original data gathering. Because industry associations do not always disclose their proprietary data sources and methods, consequently, they may be reluctant to disclose the extent of counterfeiting because it may cause consumers to lose confidence (Mencher, 2010). Therefore, due to lack of data or incomplete data, calculating the real economic losses with respect to counterfeiting and piracy often involve certain hypothesis and assumptions, as a result, the loss estimates are highly sensitive to the assumptions or hypothesis used.

According to a recent study carried out by TERA Consultants for the International Chamber of Commerce in 2010, it highlights that the European creative industries lost approximately 10 billion Euros and more than 185,000 jobs in 2008 because of digital piracy (TERA Consultants, 2010). In a similar report published by the International Intellectual Property Alliance (IIPA), the losses suffered by the US industry, for unlicensed software only increased from 7,287 million dollars to 9,515 million dollars between 2006 and 2010 (BSA, 2011). It was also found that 60 per cent of e-book downloads in Germany are illegal (IFPI, 2012).

With regard to music, despite the 940% increase in digital sales since 2004, the total music market has decreased by 30% during that period because of piracy (IFPI, 2010). IPSOS also established that the UK audiovisual sector lost £531 million in 2008 due to "copyright theft" (Villarroel, 2010). Furthermore, study by Frontier economics, found that, for every 1% increase in crime caused by counterfeiting, the UK economy would loss €1.7 billion, with about €4.1 billion in lost taxes and 380,000 jobs destroyed (BASCAP, 2009).

The economic damage caused to authors and artists by piracy varies according to the business model of exploitation of copyright. Piracy has harmed both local well as international authors and right holders. Besides the economic losses suffered by authors and artists, which can be included in the losses of cultural industries, other damages related to the infringements of their moral rights (Villarroel , 2010).

The commercial value of software piracy grew 14 percent globally in 2009 to a record total of $58.8 billion (BSA, 2011), as depicted in Figure 4 for pirated software in the developed market and the emerging market. Figure 5 shows the percentage of software pirate rate between 2009 and 2010 based on region. It can be seen from Figure 4 that the effects of counterfeiting and piracy are more pronounced in emerging markets than developed market. This could be due to, relatively weak enforcement. Developed markets include Australia, US, Canada, Japan, New Zealand, South Korea, Taiwan and Western Europe while emerging markets is other countries.

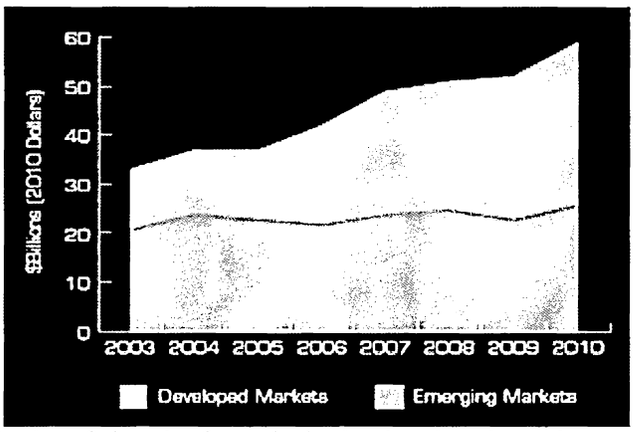


Figure 4 : Commercial value of pirated software in the developed market and emerging market (source 14)

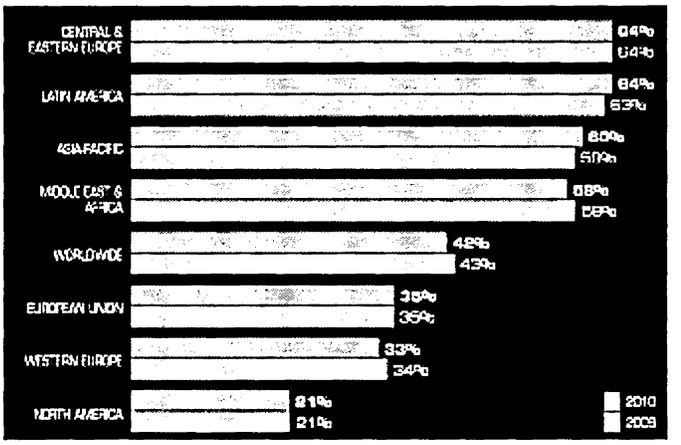


Figure 5 : The percentage of PC software pirate rate between 2009 and 2010 based on region (source 14)

As shown in Figure 6, the Sales of personal computers surged 14 percent globally in 2010, compared with just 4 percent in the previous year. On the strength of that robust growth, businesses and consumers bought nearly $95 billion worth of PC software but illegally installed another $59 billion worth. This means that for every dollar spent on legitimate software in 2010, an additional 63 cents worth of unlicensed software also made its way into the market.

In Malaysia, it has been devastating issue in music industries. Firstly, there is reduction in sale due to availability of pirated CDs, DVDs, cassettes etc. This is supposed to be a legitimate sale of the music industry. Additionally, the effect of loss of confidence of the record companies in local investment and hence the drop in expenditure for local recordings. And as such, the drop in investment has in actual fact doubled the impact of the loss of sales from piracy and perpetuated the contraction of the local music business. In the music and film in industries, the cost of piracy to the local music industry is over $200million per year, and this has led to drop in 'physical music' sales from 20 to 25% in 2008 (Koester, 2008; RIM, 2009). As a result of this, major record industries such as EMI Records shut down its operations in Malaysia (Jiun, 2009).

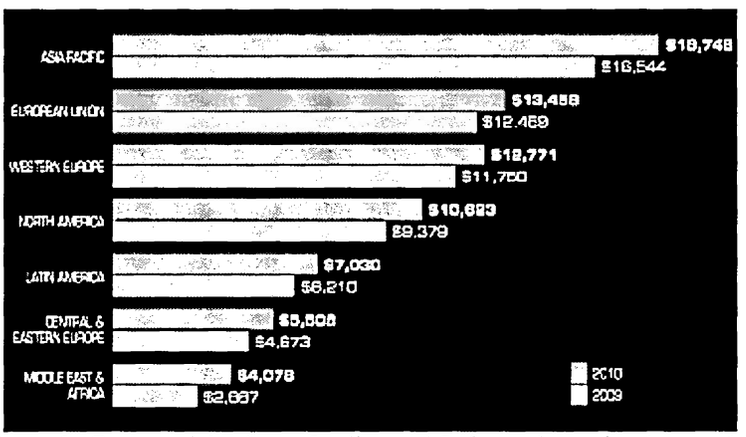


Figure 6 : Commercial values of unlicensed Software by region (source 14)

The theft of sound recordings costs the U.S. economy $12.5 billion lost in revenue, approximately 71,000 jobs and more than $2 billion in wages to U.S. workers (Siewick 2007). Camcorder Piracy causes massive losses to Film Producers. A vast number of movies are stolen from the screen by professional camcorder pirates, who use video cameras to illicitly copy movies during exhibition in a movie theatre. These copies are then distributed to pirate "dealers" throughout the world and over the Internet (IIPA, 2011).

In the medical and pharmaceutical industries, "The U.S.-based Center for Medicine in the Public Interest predicts that counterfeit drug sales will reach $75 billion globally in 2010, an increase of more than 90% from 2005."(Counterfeiting Facts, 2009). The World Health Organization says that up to 10% of medicines worldwide are counterfeit, which is a deadly hazard that could be costing the pharmaceutical industry $46 billion a year (GIPC, 2011).

Curbibing Counterfeiting & Piracy Through Digital Watermarking

Watermarking In Books, Music And Film Industries

Although the main motivation behind the digital watermarking is the protection of copyright, however its applications are not that restricted. There are a number of possible applications for digital watermarking technologies and these increases rapidly. They include broadcast monitoring, fingerprinting, indexing and covert communication (De Strycker, et al., 2002; Liu, Lu and Peng, 2008). Embedding watermarks into commercial advertisements will facilitate effective monitoring such as whether the advertisements are broadcast at the correct instants by means of an automated system. The system receives the broadcast and searches these watermarks identifying where and when the advertisement was broadcast.

The same process can be used for video and sound clips. Musicians and actors may request to ensure that they receive accurate royalties for broadcasts of their performances. Fingerprinting is a novel approach to trace the source of illegal copies. It gives content owners a means of determining exactly where and when a piece of the content leaves its authorized distribution path. The owner of the digital data may embed different watermarks in the copies of digital content customized for each recipient. In this manner, the owner can identify the customer by extracting the watermark in the case the data is delivered to third parties.

Watermarking are also used in indexing such as indexing of video mail, where comments can be embedded in the video content; indexing of movies and news items, where markers and comments can be inserted that can be used by search engines (Lancini, Mapelli, & Tubaro, 2002).

E-commerce has also benefited a lot from a variety of watermarking-based content identification applications which allow consumers to instantly locate and purchase legal, downloadable music tracks. Where customer listen to a song through phone, or access reviews and even purchase tickets simply by "reading" a movie or concert poster or a print advertisement with an enabled phone (Kale, 2008).

With the proliferation of Smartphone nowadays, the newspapers and magazines uses watermarks to add digital content to prints by using Smartphone applications to connect the printed page to the Web. Particularly among consumer magazines, such as The Oregonian (Oregolive, 2011), which is using digital watermarks from the Digimarc™ publishing platform to offer print readers daily content of added value. The Oregonian, for instance, uses a small smartphone image to indicate extra digital content. Readers can download a free Oregonian-branded Digimarc app, which, when pointed at the icon, instantly recognizes the image to launch content such as videos and slide shows (Behling, 2011).

Another application of watermarking is in the field of data security, whereby watermarks are used for certification, authentication, and conditional access. Certification is an important issue for official documents, such as identity cards or passports. Beside applications in the fields of copyright protection, authentication and security, digital watermarks can also serve as invisible labels and content links. For example, photo development laboratories may insert a watermark into the picture to link the print to its negative, thus easing the process of searching for the negative of a given print, where one can scan the print and extract the information about the negative (Olanrewaju, 2011)

Watermarking in Medical and Pharmaceutical industries

The current trend in watermarking is in the e-health environment for medical safety. This is achieved by embedding the date and the patient's information in medical images for safety and security measure, medical content

verification and medical image fidelity (Al-Qershi & Khoo, 2011; Maeder, Dowling, Nguyen, Brunton, & Nguyen, 2008; R. Olanrewaju, Khalifa, Hashim, Zeki, & Aburas, 2011). Recently, protecting pharmaceutical product from counterfeiting has emerged using watermarking technology. Cases of Internet "pharmacy" sales are rife with counterfeits, when a widely advertised product sold at a brand name website like EBay, is found to be fake (Basta, 2010).

An example of technology to curb such situation is the Catalent Pharma Solutions making available the DigiTrack technology of DigiMarc Corp (McGee, 2009). This technology involves imposing an invisible watermark, which can be read by either a purpose-built hand held reader or even a Web-enabled Smartphone, in printed surfaces. JDSU and Armark have developed micro-taggants-small bits of inert material that can contain a number or symbol on their surface, which can be added to tablet coatings (or packaging inks). The watermarks are none interacting with the formulation of pharmaceutical ingredients. Such technologies have been approved by Food and Drug Administration (Buckley and Olson, 2005; Dwan, 2002)

Watermarking in Software industries

Digital software watermarking involves hiding of steganographic messages (signals) in the software code. Watermarks enable the purchaser to verify the authenticity of the software's supplier and to detect tampering (Busch,, 2000). If a watermark is unique to a particular copy of the code, it also acts as a fingerprint which, if detected on another copy of the software, indicates that one of the two copies was pirated.
In recent days, watermarks are used as Software guards. These guards can be embedded in the software code itself, and can perform simple tasks such as checksum calculation/validation and code repair. Additionally, in some software program, watermarks include monitoring programs that perform execution-time checks to ensure the software has been legitimately licensed. It monitor reports any license violations to the software vendor or a third party. Such monitoring programs often perform additional spyware functions, such as tracking and reporting user activities to advertisers who have paid the software vendor for use of the vendor's customers' (Goertzel and Hamilton, 2011).

Researchers are investigating strong watermarking techniques to degrade performance or prevent execution of illicit software copies. Software watermarking technology thus also provides a means of license enforcement.

Conclusion

From the statistics gathered in the literature, it was observed that counterfeiting and piracy are long standing problems that have negative effect on the society. If the problem is not addressed properly, innovation and growth will be undermined and criminal networks will expand financially. More so, in countries where counterfeiting and piracy is widespread, this may affect foreign investment and could lower and affect relations with trading partners.
Current research shows that one of the technological solutions to these challenges is watermarking of digital media. Digital watermarking has proved to curb the situation of piracy and counterfeiting significantly, it has made it easy to authenticate, deter counterfeit, verify, and make digital media distribution processes harder to subvert. The latest watermarking technology especially in the health sector proved that in the future piracy in medical and pharmaceutical industries will be reduced considerably. Additionally, Policymakers should consider the potential benefits of improving Intellectual property Right, IPR enforcement in developing countries while public education could also be effective means of combating counterfeiting and piracy as well.

References:

Al-Qershi, O. M., & Khoo, B. E. (2011). Authentication And Data Hiding Using a Hybrid Roi-Based Watermarking Scheme For Dicom Images. *Journal Of Digital Imaging, 24*(1), 114-125.

BASCAP, (2009), The Impact of Counterfeiting on Governments and Consumers , A Report Commissioned By Bascap: Executive Summary.

Basta, N. (2010). How the many anticounterfeiting measures on the market today could turn into a means of connecting with patients Pharmaceutical Commerce. <Http://Www.Pharmaceuticalcommerce.Com/Frontend/1396brand_Protection_Anticounterfeiting_Pedigree_Taggants_Blis.Html>

Blakeney, M. (2009) "Policy Responses to the Involvement of Organized Crime in Intellectual Property Offences", Fifth Session, of WIPO Advisory Committee on Enforcement, 2009 (WIPO/ACE/5/5).

Busch, C., Graf, F., Wolthusen, S. and Zeidler, A. (2000)., " A System for Intellectual Property Protection. Fraunhofer Institute ", 2000. At: . *<http://www. igd. fhg. de/igd-a8>*

BSA, (2011). "Eight Annual BSA Global Software", 2010 Piracy Study,

BSA, (2009)*"Seventh Annual BSA/IDC Global Software 09 Piracy Study,"* (2010), PC Software Piracy Rates and Commercial Value of Unlicensed Software, pp. 14-15. , Accessd 15th February 2010 <http://portal.bsa.org/globalpiracy2009/pr/pr_malaysia.pdf>

Buckley M. L. and Olson, W. C. (2005) *High Tech, High Stakes; Using Technology to Smash the Fakes Trade,* In WORLDfocus: Fighting IP Theft; pp. 30-33, 2005. At: http://www.insurereinsure.com/files/News

Counterfeiting Facts and Stats, (2009) "Protection from Brand Infection,__CMO Council", <http://www.cmocouncil.org/programs/current/protection/protection_couterfeit_stats.asp>

Croze, D. (2007), Counterfeiting and Piracy The Worldwide Phenomenon, "Using Market Research to Develop Effective IPR Campaigns" APEC – IPR Workshop, World Intellectual Property Organization (WIPO)

Digital Watermarking Alliance (2010), <http://www.digitalwatermarkingalliance.org/docs/presentations/dwa_presentation.pdf>

Dwan, B, (2002). "Counterfeit And Fraud, Computer Fraud & Security", 2, pp. 11.

GAO, (2010). *"Intellectual Property, Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods"*

Goertzel K. M. and Hamilton, B. A, (2011) "Protecting Against Predatory Practices", *Protecting Software Intellectual Property Against Counterfeiting and Piracy*

Hirakawa, M., & Iijima, J. (2011). *A Study On Integrated Mobile Service Using Digital Watermark For Various Information Carriers.*

IFPI, (2010). "Digital Music Report 2010". At: <http://www.ifpi.org/content/library/DMR2010.pdf.>

IFPI, (2012), IFPI Digital Music Report 2012 , *Key Facts And Figures, Accessed April 2012, http://www.ifpi.org/content/library/DMR2012_key_facts_and_figures.pdf*

IIPA, (2011). SPECIAL 301 REPORT 301 Malaysia On Copyright Protection And Enforcement, 2011, <http://www.iipa.com>

Jiun, Y. H. (2009). Knocked Out By The Knock-Offs. *The Recording Industry Association Of Malaysia.* Retrieved From Http://Www.Rim.Org.My/Main/Index.Php?Option=Com_Content\&Task=View\&Id=259&Itemid=1

Koester, C. (2008). Combating Music Piracy: The Recording Industry's Legal.

Lancini, R., Mapelli, F., & Tubaro, S. (2002). *A Robust Video Watermarking Technique In The Spatial Domain. Lavorgna M., (2012). Digital Music Report 2012, at Http://Www.Audiostream.Com/Content/Digital-Music-Report-2012.*

Maeder, A., Dowling, J., Nguyen, A., Brunton, E., & Nguyen, P. (2008). Assuring Authenticity Of Digital Mammograms By Image Watermarking. *Digital Mammography*, 204-211.

Mencher, J. (2010,) ."Counterfeiting and Piracy: Can It Be Quantified?"

McGee, A. P., (2009). "Catalent offers The Anti-Counterfeiting Digitrack™ Digital Watermarking System to Trace, Track and Authenticate", *Catalent Pharma Solutions*. pp. 1-2.

Olanrewaju, R., Khalifa, O. O., Hashim, A. H., Zeki, A. M., & Aburas, A. (2011). Forgery Detection In Medical Images Using Complex Valued Neural Network (Cvnn). *Australian Journal Of Basic And Applied Sciences, 5*(7), 1251-1264.

Olanrewaju, R. F., Khalifa, O. O., Aisha Abdulla, Akram M. Z. Khedher. (2011a) Detection of Alterations in Watermarked Medical Images using Fast Fourier Transform and Complex-Valued Neural Network, *International Conference on Mechatronic*, presented at Le gend Hotel, Kuala Lumpur, Malaysia, 17th -19th May, 2011.(IEEE Xplore® digital library).

Olanrewaju, R. F. (2011)., Development of An Intelligent Digital Watermarking Algorithm Via Safe Region", Unpublished PhD thesis, International Islamic University Malaysia.

Oregonlive (2011), The Oregonian, Http://Www.Oregonlive.Com/Oregonian/

Orion E. , (2011), Patents Are Getting Out Of Hand, Column Software Patents Are As Foolish As Trying To Catch The Wind , The Inquirer, http://www.theinquirer.net/inquirer/opinion/2134341/patents-getting-hand.

PhysOrg.com, "Robust watermarking offers hope against Digital Piracy", 2008. At: <http://www.physorg.com/news147701945.html>

Rim. (2009). Antipiracy Efforts Slow In 2008 Retrieved From Http://Www.Rim.Org.My/Main/Index.Php?Option=Com_Content\&Task=View\&Id=253\&Itemid=1

Siewick, E. S., (2007) The True Cost of Sound Recording Piracy to the U.S. Economy, Institute for Policy Innovation Report #188.

TERA Consultants (2010), , *Building a Digital Economy: The importance of Saving Jobs in the EU's Creative Industries,* March 2010. At: <http://www.teraconsultants.fr/assets/publications/PDF/2010-Mars-Etude_Piratage_TERA_full_report-En.pdf>

Villarroel, L. (2010). "Piracy: Current Trends and Non-Legislative Measures To Counteract It", Intergovernmental copyright committee, 14th Session of the Commmitte of Universal Copyright Convention as Revised 1971.

DIHEDRAL GROUP CODES OF SMALL ORDERS

[1]Denis Wong Chee Keong and [2]Ang Miin Huey
[1]*Department of Applied Mathematics and Actuarial Science, Faculty of Engineering and Science, Universiti Tunku Abdul Rahman Setapak, Off Jalan Genting Kelang, 53300, Kuala Lumpur.*
[2]*School of Mathematical Sciences, Universiti Sains Malaysia, 11800 Pulau Pinang, Malaysia*
deniswong@utar.edu.my, mathamh@cs.usm.my

Abstract:

Error correction or detection has become an important issue with the problem of reliable communication over noisy channels. Since then error correction or detection group codes have been a focus of interest in the mathematical community in relating codes structures by using algebraic structures to investigate the internal properties. Group algebra codes gained interest after S.D. Berman showed in 1967 that cyclic codes and Reed Muller codes can be studied as ideals in a group algebra FG, where F is a finite field and G is considered, in each case, a finite cyclic group and a 2-group respectively. On the other hands, one of the first investigations of non-Abelian group algebra code was done by F.J. Macwilliams. The study of group codes as an ideal in a group algebra has been developed long time ago. If char(F) does not divides |G|, then FG is semisimple, and hence decomposes into a direct sum $FG = \oplus_i FGe_i$ ***where*** FGe_i ***are minimal ideals generated by the idempotent*** e_i***. The idempotent*** e_i ***provides some useful information on determining the minimum distance of group codes. In this paper, we study dihedral group codes generated by linear idempotents and nonlinear idempotents for dihedral groups of order 6, 8 and 12. Our primary task is to determine the parameters of these families of group codes in order to obtain codes which near to attain the Singleton bound.***

Introduction

Most objects in this paper are represented in term of group algebra FG. The group algebra $FG = \left\{ \sum_{g \in G} a_g g \mid a_g \in F \right\}$ is the free F – module over a finite group G where G can be regarded as an F – basis for FG. The addition and scalar multiplication are defined as follows. For any $u = \sum_{g \in G} \lambda_g g$, $v = \sum_{g \in G} \beta_g g \in FG$ and $\lambda \in F$, $u + v = \sum_{g \in G} (\lambda_g + \beta_g) g$ and $\lambda u = \sum_{g \in G} (\lambda \lambda_g) g$. Moreover, multiplication in G induces multiplication in FG as $u.v = \sum_{k \in G} \gamma_k k$ where $\gamma_k = \sum_{gh=k \in G} \lambda_g \beta_h$. By these operations, FG is an associative F – algebra with identity $1 = 1_F 1_G$ where 1_G and 1_F are the identity elements of G and F, respectively. G can be viewed as contained in FG, and hence the elements of G constitute the coding basis for codes viewed as subspaces of FG. We view G as $\sum_{g \in G} g$ in FG. Moreover, for $A = \sum_{g \in G} a_g g \in FG$, define $A^{(-1)} = \sum_{g \in G} a_g g^{-1}$. For more information on group algebra, please refer (Passman, 1977).

Recently, P. Hurley and T. Hurley (Hurley, 2007) study group ring codes from the view of zero divisors and unit in group rings in which case the codes defined may not be ideal. In this paper, we study codes defined over group algebra, which happen to be an ideal. A group algebra code in FG is defined as a one-sided (left or right) ideal in FG. If G is cyclic or Abelian, then every ideal in FG is the cyclic or Abelian code, respectively. See (Berman, 1967) and (Berman, 1989) for more details on cyclic and abelian group codes, and (How and Denis, 2004) for a class of nonabelian group codes. The studies of group algebra code in FG depended solidly on the choices of F and G. In general, we can study group algebra code in FG from the following point of views: If gcd(char(F), $|G|$) = 1, then FG is semisimple (refer Theorem 15.2 in (Isaacs, 1997)), that is, FG is a direct sum of some minimal ideals, say $FG = \oplus_{j=1}^{s} I_j$. Each I_j is generated by an idempotent e_j, i.e., $I_j = FGe_j$. Let $M = \{e_j\}_{j=1}^{s}$. Any ideal I of FG is a direct sum of some of the I_j, say $I = \oplus_{k=1}^{t} I_{j_k}$, $t \le s$. We say that I is generated by $\{e_{j_k}\}_{k=1}^{t}$. Let $\mu = M \setminus \{e_{j_k}\}_{k=1}^{t}$. Then $I = \{u \in FG \mid u e_{j_r} = 0 \ \forall e_{j_r} \in \mu\}$. For technical reason, we denote I by I_μ. Note that μ plays the role of parity check matrix defining a linear code, and so we expect to derive some information about the minimum distance of I_μ from μ. Recall some notation and definitions: The length n of a group code $I_\mu \lhd FG$ is defined to be $|G|$. The weight of any

element $u = \sum_{g \in G} \lambda_g g$ is equal to $|\{\lambda_g | \lambda_g \neq 0\}|$ and is denoted by wt(u). If I_μ has dimension k (as a vector space over F) and minimum distance $d = d(I_\mu)$ (= min{wt(u) | $0 \neq u \in I_\mu$}), then I_μ is called an (n, k, d)–group code. For more information on coding theory, please refer (Sloane and Macwilliam, 1978). In this paper, we consider group codes defined over dihedral groups. Some basics properties of nonabelian group codes will be derived in Section 2, then attention will be drawn to derive some properties in dihedral group. Finally, in Section 3, the minimum distance of dihedral groups of length 6, 8 and 12 will be studies and hence obtain group codes which near to attain the Singleton bound.

Preliminary

From now onward, we adapt the following definition.

Definition 2.1 Let G be a group and F be a field such that gcd(char(F), $|G|$) = 1. If E is the set of all idempotents of FG and $\mu \subseteq E$, then the group code generated by μ is $I_\mu = \{u \in FG \mid ue = 0 \ \forall \ e \in \mu\}$.

Lemma 2.2 The group codes I_μ define in Definition 2.1 is a linear code over F.

To obtain the dimension of I_μ, we need the following results.

Theorem 2.3. (Theorem 8.7; James and Liebeck, 1993) Let K be a finite group of order n, and F be an algebraically closed field with gcd(char(F), $|G|$) = 1. Then $FK \cong Mat_{n_1}(F) \oplus ... \oplus Mat_{n_s}(F)$, where $n = n_1^2 + ... + n_s^2$. FK has exactly s nonisomorphic irreducible modules, of dimensions $n_1, ..., n_s$, and s is the number of conjugacy classes of K.

Remark 2.4. Since $FG = \left(\underset{e_i \in E_L}{\oplus} FGe_i\right) \oplus \left(\underset{e_j \in E_N}{\oplus} FGe_j\right)$ where E_L is the set consists of all linear idempotents in FG and E_N is the set consists of all nonlinear idempotents in FG; and further $E = E_L \cup E_N$. Note that if $e_i \in E_L$, then dim(FGe_i) = 1; and if $e_i \in E_N$, then dim(FGe_i) = 2. (Section 18.3; James and Liebeck, 1993) Therefore, if $\mu = \mu_L \cup \mu_N$ where $\mu_L \subseteq E_L$ and $\mu_N \subseteq E_N$, then $\dim(I_\mu) = \dim(FG) - |\mu_L| - 2^2 |\mu_N|$.

For any positive integer $n \geq 2$, the dihedral group of order $2n$ can be represented as $D_{2n} = \{r^i s^j \mid 0 \leq i \leq n-1, 0 \leq j \leq 1, r^n = s^2 = 1, rs = sr^{-1}\}$. The next theorem on the number of conjugacy classes of D_{2n} can be found in (Section 18.3; James and Liebeck, 1993).

Theorem 2.5. The conjugacy classes of D_{2n} is as follows:

(i) If n is odd, then D_{2n} has $\frac{1}{2}(n+3)$ conjugacy classes: $\{1\}, \{r, r^{-1}\}, ..., \{r^{(n-1)/2}, r^{-(n-1)/2}\}, \{s, rs, ..., r^{n-1}s\}$.

(ii) If n is even and $n = 2m$, then D_{2n} has $m + 3$ conjugacy classes:

$$\{1\}, \{r^m\}, \{r, r^{-1}\}, ..., \{r^{m-1}, r^{-(m-1)}\}, \{r^{2j}s : 0 \leq j \leq m-1\}, \{r^{2j+1}s : 0 \leq j \leq m-1\}.$$

By using Theorem 2.5 and results from (Chapter 13, 14 and 15; James and Liebeck, 1993), we obtain the following lemma. Note that D_{2n}' denote the commutator subgroup of D_{2n}.

Lemma 2.6. Let D_{2n} be the dihedral group of order $2n$, where n is any integer, then

(a) $$|Irr(D_{2n})| = \begin{cases} \frac{1}{2}(n+3), & \text{if } n \text{ is prime,} \\ \frac{1}{2}(n+6), & \text{if } n = 2p, \text{ where } p \text{ is any prime.} \end{cases}$$

(b) $D_{2n}' = \begin{cases} \langle r \rangle, & \text{if } n \text{ is prime,} \\ \langle r^2 \rangle, & \text{if } n = 2p, \text{ where } p \text{ is a prime.} \end{cases}$

(c) D_{2n} has $\left| D_{2n} / D_{2n}' \right|$ linear characters, where

$$\left| D_{2n} / D_{2n}' \right| = \begin{cases} 2, & \text{if } n \text{ is prime,} \\ 4, & \text{if } n = 2p, \text{ where } p \text{ is a prime.} \end{cases}$$

(d) D_{2n} has ϖ non-linear characters, where $\varpi = \begin{cases} \dfrac{n-1}{2}, & \text{if } n \text{ is prime,} \\ \dfrac{n-2}{2}, & \text{if } n = 2p, \text{ where } p \text{ is a prime.} \end{cases}$

Proof. Part (a) is just a direct consequence from the fact that the number of irreducible characters is equal to the number of conjugacy classes. For part (b), since $\left| D_{2n} / \langle r \rangle \right| = 2$ and so $D_{2n} / \langle r \rangle$ is abelian, then $D_{2n}' \subseteq \langle r \rangle$, refer Theorem 3.10 in (Isaacs, 1992). If n is prime, then $D_{2n}' = 1$ or $D_{2n}' = \langle r \rangle$. If $D_{2n}' = 1$, then D_{2n} is abelian which is impossible. Therefore, we conclude that $D_{2n}' = \langle r \rangle$. Next, assume $n = 2p$, where p is a prime. Note that $\left| D_{2n} / \langle r^2 \rangle \right| = \left| D_{2n} / \langle r \rangle \right| \left| \langle r \rangle / \langle r^2 \rangle \right| = 4$ and so $D_{2n} / \langle r^2 \rangle$ is abelian, then $D_{2n}' \subseteq \langle r^2 \rangle$. Since $\left| \langle r^2 \rangle \right| = p$, then either $D_{2n}' = 1$ or $D_{2n}' = \langle r^2 \rangle$, and hence the result will follows directly. Part (c) follows from part (b). Part (d) follows directly from part (a) and (c). **Q.E.D.**

Lemma 2.7. If $\mu_1 \subseteq \mu_2$, then $I_{\mu_2} \subseteq I_{\mu_1}$ and so $d(I_{\mu_1}) \leq d(I_{\mu_2})$.

Proof. If $u \in I_{\mu_2}$, then $ue = 0$ for all $e \in \mu_2$. Since $\mu_1 \subseteq \mu_2$, then $ue = 0$ for all $e \in \mu_1$ and so $u \in I_{\mu_1}$. For the second assertion, assume $d(I_{\mu_2}) = t$. If $u \in I_{\mu_2}$ with wt(u) = t and $wt(u) \leq wt(v)$, $\forall v \in I_{\mu_1}$, then $d(I_{\mu_1}) = t$. On the other hand, if $u \in I_{\mu_2}$ with wt(u) = t and $wt(u) > wt(v)$, for some $v \in I_{\mu_1}$, then $d(I_{\mu_1}) < t$. Thus, the result follows directly. **Q.E.D.**

Minimum Distance of Dihedral Group Codes

Codes defined over FD_6

Let $H = \langle r \mid r^3 = 1 \rangle$ and so $D_6 = H \cup sH$. From Lemma 2.6, D_6 consists of three irreducible characters (two are linear and one is nonlinear), and each of these characters will correspond to a unique idempotent (refer Proposition 14.10; James and Liebeck, 1993) as follows:

$$\chi_1 \leftrightarrow e_1 = \frac{1}{6}(H + sH), \ \chi_2 \leftrightarrow e_2 = \frac{1}{6}(H - sH) \text{ and } \chi_3 \rightarrow e_3 = 1 - \frac{1}{3}H.$$

Let $u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 s + \lambda_5 rs + \lambda_6 r^2 s$ be any elements in FD_6, $\lambda_i \in F$ for $i = 1, 2, 3, 4, 5, 6$, then

$$ue_1 = \left(\sum_{i=1}^{6} \lambda_i \right) e_1 \tag{1}$$

$$ue_2 = \left(\sum_{i=1}^{3} \lambda_i - \sum_{i=4}^{6} \lambda_i \right) e_2 \tag{2}$$

$$ue_3 = \frac{1}{3}[(2\lambda_1 - \lambda_2 - \lambda_3) + (-\lambda_1 + 2\lambda_2 - \lambda_3) r + (-\lambda_1 - \lambda_2 + 2\lambda_3) r^2 \tag{3}$$

$$+ (2\lambda_4 - \lambda_5 - \lambda_6)\, s + (-\lambda_4 + 2\lambda_5 - \lambda_6)\, rs + (-\lambda_4 - \lambda_5 + 2\lambda_6)\, r^2 s]$$

Lemma 3.1. Let e_1, e_2 and e_3 be those idempotents in FD_6 as constructed above, then:

(i) $d\left(I_{\{e_i\}}\right) = 2$ for $i = 1,2$.

(ii) $d\left(I_{\{e_3\}}\right) = 3$.

Proof. We prove part (i) for the case $i = 1$. The case $i = 2$ can be proved in a similar manner. Assume $u = \lambda g \in I_{\{e_1\}}$ for any $g \in D_6$ and $0 \neq \lambda \in F$ such that $wt(u) = 1$. By equation (1), $ue_1 = \lambda e_1 \neq 0$. Hence, we conclude that $u = \lambda g \notin I_{\{e_1\}}$ and so $d\left(I_{\{e_1\}}\right) \geq 2$. Clearly, $u = g - h \in I_{\{e_1\}}$ for any distinct $g, h \in D_6$ because by equation (1), $ue_1 = (1-1)e_1 = 0$ and so $d\left(I_{\{e_1\}}\right) = 2$.

For part (ii): if $u = \lambda g \in I_{\{e_3\}}$ with $wt(u) = 1$, then $0 \neq \lambda \in F$. However, by using equation (3), $ue_3 = \lambda g e_3 \neq 0$ and so $u = \lambda g \notin I_{\{e_3\}}$ which implies $d\left(I_{\{e_3\}}\right) > 1$. Next, we check whether $I_{\{e_3\}}$ consist of codewords of weight 2. Assume $u = \lambda_1 g_1 + \lambda_2 g_2 \in I_{\{e_3\}}$ such that $wt(u) = 2$, then we have either $g_1, g_2 \in H$, $g_1, g_2 \in sH$ or $g_1 \in H$ and $g_2 \in sH$. For each of these possibilities, by using equation (3), we will obtain a set of equations in terms of λ_1 and λ_2, and upon solving will give the solution $\lambda_1 = \lambda_2 = 0$ which is impossible. Thus, $d\left(I_{\{e_3\}}\right) > 2$. Finally, consider $u = H$, then $ue_3 = H\left(1 - \frac{1}{3}H\right) = H - H = 0$ and so $u = H \in I_{\{e_3\}}$ and hence $d\left(I_{\{e_3\}}\right) = 3$. **Q.E.D.**

From Lemma 3.1 and Remark 2.4, we see that $I_{\{e_i\}}$ is a $(6,5,2)$ – group code for $i = 1,2$ which attain the singleton bound and so are *MDS* codes. However, $I_{\{e_3\}}$ is a $(6,2,3)$ – group code which is not an *MDS* code.

Theorem 3.2. Let e_1, e_2 and e_3 be those idempotents in FD_6, then:

(i) $d(I_{\{e_1,e_2\}}) = 2$.

(ii) $d(I_{\{e_i,e_3\}}) = 6$ for $i = 1,2$.

Proof. By Lemma 2.7 and Lemma 3.1, we notice that $d\left(I_{\{e_i,e_j\}}\right) \geq 2$ for all $i \neq j$, $i = 1,2$ and $j = 2,3$. For part (i), if $u = \lambda_4 s + \lambda_5 rs$, $\lambda_4 \neq 0$ and $\lambda_5 \neq 0$, then by using equation (1) and (2), $ue_1 = (\lambda_4 + \lambda_5)\, e_1$ and $ue_2 = (-\lambda_4 - \lambda_5)\, e_2$ then $ue_1 = ue_2 = 0$ if and only if $\lambda_4 = -\lambda_5$. Hence, $u = \lambda_4 s + \lambda_5 rs \in I_{\{e_1,e_2\}}$. Therefore, $d(I_{\{e_1,e_2\}}) = 2$.

For part (ii), the proof will be similar. We need to find an element with weight equal to 6. It can be checked that there are no codewords with weight less than 6 in $I_{\{e_2,e_3\}}$. We now check that $u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 s + \lambda_5 rs + \lambda_6 r^2 s$ is a word of $I_{\{e_2,e_3\}}$. By using equation (2) and (3), we obtain

$$ue_2 = (\lambda_1 + \lambda_2 + \lambda_3 - \lambda_4 - \lambda_5 - \lambda_6)\, e_2 \text{ and}$$

$$ue_3 = \frac{1}{3}[(2\lambda_1 - \lambda_2 - \lambda_3) + (-\lambda_1 + 2\lambda_2 - \lambda_3)\, r + (-\lambda_1 - \lambda_2 + 2\lambda_3)\, r^2$$
$$+ (2\lambda_4 - \lambda_5 - \lambda_6)\, s + (-\lambda_4 + 2\lambda_5 - \lambda_6)\, rs + (-\lambda_4 - \lambda_5 + 2\lambda_6)\, r^2 s].$$

Thus, $ue_2 = ue_3 = 0$ if and only if

$$\lambda_1 + \lambda_2 + \lambda_3 - \lambda_4 - \lambda_5 - \lambda_6 = 0 \quad \text{(i)}$$

$$\left.\begin{array}{l} 2\lambda_1 - \lambda_2 - \lambda_3 = 0 \\ -\lambda_1 + 2\lambda_2 - \lambda_3 = 0 \\ -\lambda_1 - \lambda_2 + 2\lambda_3 = 0 \end{array}\right\} \quad \text{(ii)}$$

$$\left.\begin{array}{l} 2\lambda_4 - \lambda_5 - \lambda_6 = 0 \\ -\lambda_4 + 2\lambda_5 - \lambda_6 = 0 \\ -\lambda_4 - \lambda_5 + 2\lambda_6 = 0 \end{array}\right\} \quad \text{(iii)}$$

The unique solution for (ii) is $\lambda_1 = \lambda_2 = \lambda_3 \neq 0$ and for (iii) is $\lambda_4 = \lambda_5 = \lambda_6 \neq 0$. Hence, from (i), $\lambda_1 + \lambda_1 + \lambda_1 - \lambda_4 - \lambda_4 - \lambda_4 = 0$ which implies that $\lambda_1 = \lambda_4 \neq 0$. Therefore, we obtain a nonzero solution and so $d(I_{\{2,3\}}) = 6$. **Q.E.D.**

In Theorem 3.2, we have constructed two families of group codes, $I_{\{1,2\}}$ is a $(6,4,2)-$ *MDS* group code and $I_{\{1,3\}}$ is a $(6,1,6)-$ group code for $i = 1,2$.

Codes defined over FD_8

Let $H = \langle r \mid r^4 = 1 \rangle$ and so $D_8 = H \cup sH$. Note that $K = \langle r^2 \mid r^4 = 1 \rangle \leq H$. From Lemma 2.6, we see that D_8 consists of 5 irreducible characters, in which case, four of them are linear characters and one is nonlinear character. Each of this character will correspond to a unique idempotent as follows:

(a) Idempotents correspond to linear characters:

$$\chi_1 \leftrightarrow e_1 = \frac{1}{8}(H + sH),\ \chi_2 \leftrightarrow e_2 = \frac{1}{8}(H - sH),\ \chi_3 \leftrightarrow e_3 = \frac{1}{8}(1-r)(1+s)K, \text{ and}$$

$$\chi_4 \leftrightarrow e_4 = \frac{1}{8}(1-r)(1-s)K.$$

(b) Idempotents correspond to the nonlinear character χ_5 of degree 2:

$$\chi_5 \rightarrow e_5 = \frac{1}{4}(2-2r^2) = \frac{1}{2}(1-r^2).$$

Let $u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 r^3 + \lambda_5 s + \lambda_6 rs + \lambda_7 r^2 s + \lambda_8 r^3 s$ be any element in FD_8 such that $\lambda_i \in F$ for i = 1, 2, 3, 4, 5, 6, 7 and 8, then

$$ue_1 = \left(\sum_{i=1}^{8} \lambda_i\right) e_1 \tag{4}$$

$$ue_2 = \left(\sum_{i=1}^{4} \lambda_i - \sum_{i=5}^{8} \lambda_i\right) e_2 \tag{5}$$

$$ue_3 = \left(\sum_{i=1,3,5,7} \lambda_i - \sum_{i=2,4,6,8} \lambda_i\right) e_3 \tag{6}$$

$$ue_4 = \left(\sum_{i=1,3,6,8} \lambda_i - \sum_{i=2,4,5,7} \lambda_i\right) e_4 \tag{7}$$

$$\begin{aligned} ue_5 = \frac{1}{2}[&(\lambda_1 - \lambda_3) + (\lambda_2 - \lambda_4) r + (-\lambda_1 + \lambda_3) r^2 + (-\lambda_2 + \lambda_4) r^3 \\ &+ (\lambda_5 - \lambda_7) s + (\lambda_6 - \lambda_8) rs + (-\lambda_5 + \lambda_7) r^2 s + (-\lambda_6 + \lambda_8) r^3 s] \end{aligned} \tag{8}$$

Lemma 3.3. Let $\mu = \{e_1, e_2, e_3, e_4\}$, where e_1, e_2, e_3 and e_4 are the linear idempotents in FD_8, if $\beta \subseteq \mu$, then $d(I_\beta) = 2$.

Proof. If $\beta \subseteq \mu$, then there are four cases to be considered, which are $|\beta| = 1$, 2, 3, or 4. From Lemma 2.7, we only need to show that $d(I_\beta) = 2$ for $|\beta| = 4$. If $|\beta| = 4$, then e_1, e_2, e_3, e_4 are all in β. If $u = \lambda_i g_i$, $\lambda_i \neq 0$ and $wt(u) = 1$, then $ue_1 = \lambda_i e_1 \neq 0$, $ue_2 = (\lambda_i\ \chi_2(g_i))\ e_2 \neq 0$, $ue_3 = (\lambda_i\ \chi_3(g_i))\ e_3 \neq 0$ and $ue_4 = (\lambda_i\ \chi_4(g_i))\ e_4 \neq 0$. Hence, $u = \lambda_i g_i \notin I_\beta$ indicates that $d(I_\beta) \geq 2$. Next, consider $u = \lambda_1 + \lambda_3 r^2$, by using equation (4) to (7):

$$ue_1 = (\lambda_1 + \lambda_3)\ e_1,\ ue_2 = (\lambda_1 + \lambda_3)\ e_2,\ ue_3 = (\lambda_1 + \lambda_3)\ e_3 \text{ and } ue_4 = (\lambda_1 + \lambda_3)\ e_4.$$

$ue_1 = ue_2 = ue_3 = ue_4 = 0$ if and only if $\lambda_1 = -\lambda_3 \neq 0$. Clearly, $u \in I_\beta$ and so $d(I_\beta) = 2$. **Q.E.D.**

From this lemma, we immediately conclude that if $\beta \subseteq \mu$, then I_β is a $(8, 8-|\beta|, 2)-$ group code. Furthermore, I_β is a *MDS* code if and only if $|\beta| = 1$. The next result can be proved by using similar method as Lemma 3.3.

Lemma 3.4. Let $\mu = \{e_5\}$ where e_5 is the nonlinear idempotent in FD_8, then $d(I_{\{e_5\}}) = 2$. Furthermore, let $u = \lambda_i g_i + \lambda_j g_j$, $\lambda_i \neq 0$ and $\lambda_j \neq 0$ with $g_i \neq g_j \in D_8$, then $u \in I_{\{e_5\}}$ if and only if $g_i, g_j \in H$.

Theorem 3.5. Let $\mu = \{e, e_5\}$ where e is any one of the linear idempotents and e_5 is the nonlinear idempotent in FD_8, then $d(I_\mu) = 4$ and so I_μ is a $(8,3,4)-$ group code.

Proof. Without loss of generality, we only prove for the case $\mu = \{e_1, e_5\}$. By Lemma 2.7 and Lemma 3.3, we know that $d(I_\mu) \geq 2$. By the second statement in Lemma 3.4, if $u = \lambda_i g_i + \lambda_j g_j$, $\lambda_i \neq 0$ and $\lambda_j \neq 0$, then either g_i, g_j in H or g_i, g_j in sH or one in H and the other in sH will not produce a codeword in I_μ. This follows from equations (4) and (8) in which always gives the solution $\lambda_i = \lambda_j = 0$. Next, for $u = \lambda_i g_i + \lambda_j g_j + \lambda_k g_k$, $\lambda_i \neq 0$ and $\lambda_j \neq 0$ and $\lambda_k \neq 0$, we have either g_i, g_j, g_k all lies in H (resp. sH) or g_i, g_j lies in H (resp. sH) but g_k lies in sH (resp. H). For both cases, by using equations (4) and (8), u is not contained in I_μ. Finally, if $u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 r^3$, $\lambda_1 \neq 0$, $\lambda_2 \neq 0$, $\lambda_3 \neq 0$ and $\lambda_4 \neq 0$, then $ue_1 = (\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4)\, e_1$ and $ue_5 = (\lambda_1 - \lambda_3)\, e_5 + (\lambda_2 - \lambda_4)\, re_5$. Thus, $ue_1 = ue_5 = 0$ if and only if $\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = 0$ and $\lambda_1 - \lambda_3 = 0$ and $\lambda_2 - \lambda_4 = 0$. The only solution for the above is $\lambda_1 = \lambda_3 \neq 0$ and $\lambda_2 = \lambda_4 \neq 0$, So, $\lambda_1 + \lambda_2 + \lambda_1 + \lambda_2 = 0$ implies that $2\lambda_1 + 2\lambda_2 = 0$ and so $\lambda_1 = -\lambda_2 \neq 0$. Thus, we obtain a set of nonzero solution and so $u \in I_\mu$. In other word, $d(I_\mu) = 4$. **Q.E.D.**

Theorem 3.6. Let e_1, e_2, e_3, e_4, e_5 be the idempotents in FD_8, then $d(I_{\{e_i, e_j, e_5\}}) = 4$, where $i, j = 1, 2, 3, 4$, $i \neq j$.

Proof. By Lemma 2.7 and Theorem 3.5, we only need to show that there exists a codeword of weight 4 in $I_{\{e_i, e_j, e_5\}}$, where $i, j = 1, 2, 3, 4$, $i \neq j$. Since most calculations are routined, then we only state a codeword of weight 4 in each group code.

(i) $u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 r^3 \in I_{\{e_1, e_2, e_5\}}$.

(ii) $u = \lambda_1 + \lambda_3 r^2 + \lambda_5 s + \lambda_7 r^2 s \in I_{\{e_1, e_3, e_5\}}$.

(iii) $u = \lambda_1 + \lambda_3 r^2 + \lambda_6 rs + \lambda_8 r^3 s \in I_{\{e_1, e_4, e_5\}}$.

(iv) $u = \lambda_1 + \lambda_3 r^2 + \lambda_6 rs + \lambda_8 r^3 s \in I_{\{e_2, e_3, e_5\}}$.

(v) $u = \lambda_1 + \lambda_3 r^2 + \lambda_6 rs + \lambda_7 r^2 s \in I_{\{e_2, e_4, e_5\}}$.

(vi) $u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 r^3 \in I_{\{e_3, e_4, e_5\}}$. **Q.E.D.**

Corollary 3.7. $d(I_{\{e_i, e_j, e_k, e_5\}}) = 8$, where $i, j, k \in \{1, 2, 3, 4\}$, $i \neq j \neq k$.

Proof. The proof is similar to Theorem 3.6, and so without loss of geneality we consider only $\mu = \{e_1, e_2, e_3, e_5\}$, in the case of $\mu = \{e_1, e_2, e_5\}$, $d(I_{\{e_1, e_2, e_5\}}) = 4$, thus we may assume that the code generated by $\mu = \{e_1, e_2, e_3, e_5\}$ has minimum distance greater than or equal to 4.

By using equations (4), (5), (6) and (8), it can be shown that no codeword of weight 4, 5, 6, and 7 in $I_{\{e_1, e_2, e_5\}}$ and so we only exhibit there is an element of weight 8 in $I_{\{e_1, e_2, e_5\}}$.

If $u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 r^3 + \lambda_5 s + \lambda_6 rs + \lambda_7 r^2 s + \lambda_8 r^3 s$, $\lambda_i \neq 0$ for $i = 1, 2, 3, \ldots, 8$, then

$ue_1 = (\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7 + \lambda_8)\, e_1$, $ue_2 = (\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 - \lambda_5 - \lambda_6 - \lambda_7 - \lambda_8)\, e_2$,

$ue_3 = (\lambda_1 - \lambda_2 + \lambda_3 - \lambda_4 + \lambda_5 - \lambda_6 + \lambda_7 - \lambda_8)\, e_3$ and

$$ue_5 = \frac{1}{2}[(\lambda_1 - \lambda_3) + (\lambda_2 - \lambda_4)\, r + (-\lambda_1 + \lambda_3)\, r^2 + (-\lambda_2 + \lambda_4)\, r^3 + (\lambda_5 - \lambda_7)\, s + (\lambda_6 - \lambda_8)\, rs + (-\lambda_5 + \lambda_7)\, r^2 s + (-\lambda_6 + \lambda_8)\, r^3 s].$$

Thus, $ue_1 = ue_2 = ue_3 = ue_5 = 0$ if and only if $\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7 + \lambda_8 = 0$,

$\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 - \lambda_5 - \lambda_6 - \lambda_7 - \lambda_8 = 0$,

$\lambda_1 - \lambda_2 + \lambda_3 - \lambda_4 + \lambda_5 - \lambda_6 + \lambda_7 - \lambda_8 = 0$,

$\lambda_1 = \lambda_3$, $\lambda_2 = \lambda_4$, $\lambda_5 = \lambda_7$ and $\lambda_6 = \lambda_8$.

Hence,

$\lambda_1 + \lambda_2 + \lambda_5 + \lambda_6 = 0$ (i)

$\lambda_1 + \lambda_2 - \lambda_5 - \lambda_6 = 0$ (ii)

$\lambda_1 - \lambda_2 + \lambda_5 - \lambda_6 = 0$ (iii)

Upon solving (i) to (iii), we will obtain nonzero solution. Hence, $u \in I_{\{e_1,e_2,e_3,e_5\}}$ and so $d\left(I_{\{e_1,e_2,e_3,e_5\}}\right)=8$.

Codes defined over FD_{12}

D_{12} consists of six irreducible characters, four are linear characters and two are nonlinear characters. Each of this character will correspond to a distinct idempotent in the following way.

(a) Idempotents correspond to linear characters:

$$\chi_1 \leftrightarrow e_1=\frac{1}{12}\left(\sum_{i=0}^{5} r^i(1+s)\right),\ \chi_2 \leftrightarrow e_2=\frac{1}{12}\left(\sum_{i=0}^{5} r^i(1-s)\right),\ \chi_3 \leftrightarrow e_3=\frac{1}{12}\left(\sum_{i=0}^{5}(-r)^i(1+s)\right) \text{ and}$$

$$\chi_4 \leftrightarrow e_4=\frac{1}{12}\left(\sum_{i=0}^{5}(-r)^i(1-s)\right)$$

(b) Idempotents correspond to nonlinear characters:

$$\chi_5 \leftrightarrow e_5=\frac{1}{6}\left(2-r-r^2\right)(1+r^3) \text{ and } \chi_6 \leftrightarrow e_6=\frac{1}{6}(2-r-r^2)(1-r^3)$$

Let $u=\sum_{i=1}^{6}\lambda_i r^{i-1}+\sum_{j=7}^{12}\lambda_j r^{j-7}s$ be any elements in FD_{12} such that $\lambda_i \in F\ \forall\ 1\le i\le 12$, then

$$ue_1=\left(\sum_{i=1}^{12}\lambda_i\right)e_1 \tag{9}$$

$$ue_2=\left(\sum_{i=1}^{6}\lambda_i+\sum_{j=7}^{12}\left(-\lambda_j\right)\right)e_2 \tag{10}$$

$$ue_3=\left(\sum_{i=1,3,5,7,9,11}\lambda_i+\sum_{j=2,4,6,8,10,12}\left(-\lambda_j\right)\right)e_3 \tag{11}$$

$$ue_4=\left(\sum_{i=1,3,5,8,10,12}\lambda_i+\sum_{j=2,4,6,7,9,11}\left(-\lambda_j\right)\right)e_4 \tag{12}$$

$$\begin{aligned} ue_5=\frac{1}{6}[&(2\lambda_1-\lambda_2-\lambda_3+2\lambda_4-\lambda_5-\lambda_6)+(2\lambda_1-\lambda_2-\lambda_3+2\lambda_4-\lambda_5-\lambda_6)\,r^3\\ &+(-\lambda_1+2\lambda_2-\lambda_3-\lambda_4+2\lambda_5-\lambda_6)\,r+(-\lambda_1+2\lambda_2-\lambda_3-\lambda_4+2\lambda_5-\lambda_6)\,r^4\\ &+(-\lambda_1-\lambda_2+2\lambda_3-\lambda_4-\lambda_5+2\lambda_6)\,r^2+(-\lambda_1-\lambda_2+2\lambda_3-\lambda_4-\lambda_5+2\lambda_6)\,r^5\\ &+(2\lambda_7-\lambda_8-\lambda_9+2\lambda_{10}-\lambda_{11}-\lambda_{12})\,s+(2\lambda_7-\lambda_8-\lambda_9+2\lambda_{10}-\lambda_{11}-\lambda_{12})\,r^3s\\ &+(-\lambda_7+2\lambda_8-\lambda_9-\lambda_{10}+2\lambda_{11}-\lambda_{12})\,rs+(-\lambda_7+2\lambda_8-\lambda_9-\lambda_{10}+2\lambda_{11}-\lambda_{12})\,r^4s\\ &+(-\lambda_7-\lambda_8+2\lambda_9-\lambda_{10}-\lambda_{11}+2\lambda_{12})\,r^2s+(-\lambda_7-\lambda_8+2\lambda_9-\lambda_{10}-\lambda_{11}+2\lambda_{12})\,r^5s] \end{aligned} \tag{13}$$

$$\begin{aligned} ue_6=\frac{1}{6}[&(2\lambda_1+\lambda_2-\lambda_3-2\lambda_4-\lambda_5+\lambda_6)-(2\lambda_1+\lambda_2-\lambda_3-2\lambda_4-\lambda_5+\lambda_6)\,r^3\\ &+(\lambda_1+2\lambda_2+\lambda_3-\lambda_4-2\lambda_5-\lambda_6)\,r-(\lambda_1+2\lambda_2+\lambda_3-\lambda_4-2\lambda_5-\lambda_6)\,r^4\\ &+(-\lambda_1+\lambda_2+2\lambda_3+\lambda_4-\lambda_5-2\lambda_6)\,r^2-(-\lambda_1+\lambda_2+2\lambda_3+\lambda_4-\lambda_5-2\lambda_6)\,r^5\\ &+(2\lambda_7+\lambda_8-\lambda_9-2\lambda_{10}-\lambda_{11}+\lambda_{12})\,s-(2\lambda_7+\lambda_8-\lambda_9-2\lambda_{10}-\lambda_{11}+\lambda_{12})\,r^3s\\ &+(\lambda_7+2\lambda_8+\lambda_9-\lambda_{10}-2\lambda_{11}-\lambda_{12})\,rs-(\lambda_7+2\lambda_8+\lambda_9-\lambda_{10}-2\lambda_{11}-\lambda_{12})\,r^4s\\ &+(-\lambda_7+\lambda_8+2\lambda_9+\lambda_{10}-\lambda_{11}-2\lambda_{12})\,r^2s-(-\lambda_7+\lambda_8+2\lambda_9+\lambda_{10}-\lambda_{11}-2\lambda_{12})\,r^5s \end{aligned} \tag{14}$$

We sumarize our results in the following theorem. Indeed most of them can be proved by using similar argument as for group codes in FD_6 and FD_8.

Theorem 3.8. Let $\mu_L=\{e_1,e_2,e_3,e_4\}$ and $\mu_N=\{e_5,e_6\}$ be all idempotents in FD_{12} which is defined as above.

(a) If $\beta\subseteq\mu_L$, then $d\left(I_\beta\right)=2$.

(b) If $\beta\subseteq\mu_N$ and $|\beta|=1$, then $d\left(I_\beta\right)=2$.

(c) If $\beta=\{e_i,e_5\}$, then $d\left(I_{\{e_i,e_5\}}\right)=2$ *only if* $i=1$ *or* 2, and $d\left(I_{\{e_i,e_5\}}\right)=4$ *only if* $i=3$ *or* 4.

(d) If $\beta=\{e_i,e_6\}$, then $d(I_{\{e_i,e_6\}})=4$ *only if* $i=1$ *or* 2, and $d(I_{\{e_i,e_6\}})=2$ *only if* $i=3$ *or* 4.

(e) $d\left(I_{\mu_N}\right)=3$.

(f) $d(I_{\{e_1,e_2,e_5\}}) = d(I_{\{e_3,e_4,e_6\}}) = 2$.

(g) $d(I_{\{e_3,e_4,e_5\}})= d(I_{\{e_1,e_2,e_6\}}) = 4$.

(h) $d(I_{\{e_1,e_3,e_5\}}) = d(I_{\{e_1,e_4,e_5\}})= d(I_{\{e_2,e_3,e_5\}}) = d(I_{\{e_2,e_4,e_5\}}) = 6$.

(i) $d(I_{\{e_i,e_5,e_6\}}) = 6$ *for* $i = 1, 2, 3, 4$.

(j) $d(I_{\{e_i,e_j,e_k,e_5\}}) = 6$, *where* $i, j, k = 1, 2, 3, 4$, $i \neq j \neq k$.

(k) $d\left(I_{\{e_1,e_2\}\cup\mu_N}\right)= d\left(I_{\{e_3,e_4\}\cup\mu_N}\right) = 6$.

(l) $d(I_{\{e_1,e_3\}\cup\mu_N}) = d(I_{\{e_2,e_4\}\cup\mu_N}) = 12$.

(m) If $\beta \subseteq \mu_N$ and $|\beta|=1$, then $d\left(I_{\mu_L\cup\beta}\right)=6$.

References:

S.D. Berman (1989). Parameter of Abelian Codes in the Group Algebra *KG* of $G = \langle a\rangle \times \langle b\rangle$, $a^p = b^p = 1$, p is prime, over a finite field *K* with a primitive p^{th} root of unity and related MDS-Codes. *Contempary Math.* Vol 93.

S.D.Berman (1967). Semisimple Cyclic and Abelian Codes, II. *Kibernetika* 3, 21-30.

How Guan Aun and Denis Wong Chee Keong (2004). Group Codes Defined Using Extra-Special p-Group of Order p^3. *Bull. Malays. Math. Sci. Soc*, (2) 27, 185-205.

P. Hurley and T. Hurley (2007), Module codes in group rings, Proc. IEEE Int. Symp. On Information Theory (ISIT).

P. Hurley and T. Hurley (2007), Codes from Zero-divisors and units in group rings, Int. J. Inform, and Coding Theory 1., 57 – 87.

I.M. Isaacs, *Algebra, A Graduate Course.* Brooks/Cole Publishing. Pacific Grove, California, 1992.

G. D. James and M. W. Liebeck (1993). *Representations and Characters of groups*, Cambridge University Press.

F.J. Macwilliam (1969). Codes and ideals in group algebras, in *Combinatorial Mathematics and its Applications*, R.C. Bose and T.A. Dowling, eds., *Chapel Hill: Univ. North Carolina Press*, 317-328.

D.S. Passman (1977), *The Algebraic Structure of Group Rings.* New York: Wiley.

N.J.A. Sloane and F.J. Macwilliam (1978), *The Theory of Error Correcting Codes.* Amsterdam, The Netherlands: North-Holland.

IEEE 802.15.4 SECURITY ANALYSIS

[1]Saif Al-alak, [2]Zuriati Ahmad Zukarnain, [2]Azizol Abdullah and [2]Shamala Subramaniam
[1]*Computer Science Dept. College of Science for Women Babylon University*
[2]*Department of Communication Technology and Networks, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia*
Saif.shareefy@gmail.com, zuriati, azizol, shamala@fsktm.upm.edu.my

Abstract:

IEEE 802.15.4 standard is a platform which has been used in wireless sensor network specifications and applications. AES-CCM security mode is adopted by IEEE 802.15.4 with single secret key. The strength of the key is measured by its logarithm. However, brute force attack can break AES secret key in a reasonable time within high speed new technology computers. In this paper we analyze Multiple Key-Protocol-Advanced Encryption Standard to show its improvement for key strength against secret key breaking. The analyzing of our work shows that the nonce length of the message in IEEE 802.15.4 is increased for different level of security.

Keywords: AES, CCM, IEEE 802.15.4, Multi-level security, nonce, time complexity.

Introduction

Recently, the wireless sensor networks are employs in many life fields. IEEE 802.15.4[1] standard is used as a platform for many specifications and applications. ZigBee wireless sensor is one of the most interesting specification which is IEEE 802.15.4 based. Now, the ZigBee[2] technology is used in building and developing automation, smart energy, healthcare, and telecommunication services.

The IEEE 8015.4 standard adopted Advanced Encryption Standard (AES) [3] in CCM*[4] security mode for the message confidentiality and message authenticity. The secret key length for AES algorithm is set to 128-bit. Brute force attack[5] is used to break the secret key of AES algorithm. Secret key strength and security system complexity can be increased by using Multiple-Key Protocol (MKP) [6], which is provide multiple keys for the node depending on its security level. In this paper we analyze the strength of secret key belong to MKP in terms of time complexity. The IEEE 802.15.4 message has a possibility of replay attack. For this purpose the nonce is used to ensure no message replay attack. The length of nonce is related to the message size,[7][8] that means the length of nonce is reduced by message size incremental and vice versa. The strength of nonce is improved when its length increased and vice versa. The MKP increased the strength of nonce as shown in the analyzing results in the next sections. The objective of this paper is to show the security improvement over IEEE 802.15.4 standard by implementing MKP-AES.

The next section defines security options of IEEE 802.15.4. The third section explains AES algorithm. The fourth section explains CCM security mode. The fifth section analyzes MKP in terms of key strength and nonce length. The sixth section computes the nonce length for different levels of security of varies message size.

IEEE 802.15.4 Security

IEEE 802.15.4 is a Low Rate Wireless Personal Area Network (LR-WPAN). It consists of two layers: physical (PHY) and media access control (MAC). The standard provides security protection for its transferred message. In MAC sub layer the messages are ciphered before sending and deciphered when receiving by AES algorithm in Counter mode (CTR) [8]. Data integrity is computed using Cipher Block Chaining – Message Authentication Code (CBC-MAC algorithm)[8]. The nonce is used to protect message against replay attack. The standard employs a combination of CTR mode and CBC-MAC algorithm is known as CCM* mode. The standard provides different choices of security by optionally run either one of the algorithms CBC-MAC with different key length (32, 64, and 128) and AES-CTR as such in table 1.

Table 1 : IEEE802.15.4 security options

Security Option	*Algorithms*
No	None
MIC-32	CBC-MAC: key 32-bit
MIC-64	CBC-MAC: key 64-bit
MIC-128	CBC-MAC: key 128-bit
CTR	AES-CTR
AES-CCM-32	AES-CTR and CBC-MAC: key 32-bit
AES-CCM-64	AES-CTR and CBC-MAC: key 64-bit
AES-CCM-128	AES-CTR and CBC-MAC: key 128-bit

AES

Rijndael [9] is a symmetric cryptosystem that announced by NIST as advance encryption standard. AES employs a single secret key with length 128, 192, and 256-bit. The block size is set to 128-bit for all different key length. AES encrypts a message by performing sequence of transformations on the blocks of message. Also key rounding is done in another sequence of transformation. The length of the key specifies number of rounding. The key rounds are 10, 12 and 14 for 128, 192 and 256-bit key length respectively. AES decrypts a ciphered message by applying a sequence of transformations that inversing the ciphering operation to get the original message.

AES Ciphering

AES Block ciphering runs a sequence of functions that will change the value of bytes of blocks. The sequence of transformations is repeated on each block many times based on the key length. The ciphering transformations include the following tasks:

- SubBytes: In this transformation, each byte is replaced with another byte from substitution table which is called S-box as illustrated in figure 1(a).
- ShiftRows: The transformation performs a cyclically shifting for the last three rows of input block over different number of bytes (offset) as shown in figure 1(b).
- MixedColumns: This transformation considers each column to be multiply by a specified matrix to produce new column this can be seen in figure 1(c).
- AddRoundKey: Each column of input block is XOR with one column of the state key to produce new block as seen in figure 1(d).

AES Key Expansion

The secret key is expanded to schedule for each round. The key is treated as 4-byte words. The expansion transformations are following:

- SubWord: This transformation uses the S-box to substitute each byte with new one.
- RotWord: The transformation applies a cyclic permutation on input key.
- Rcon[i]: The round constant word array is XOR with key to produce a new schedule key.

AES Deciphering

In deciphering operation all the transformations in the ciphering operation are inversed to produce the original message.

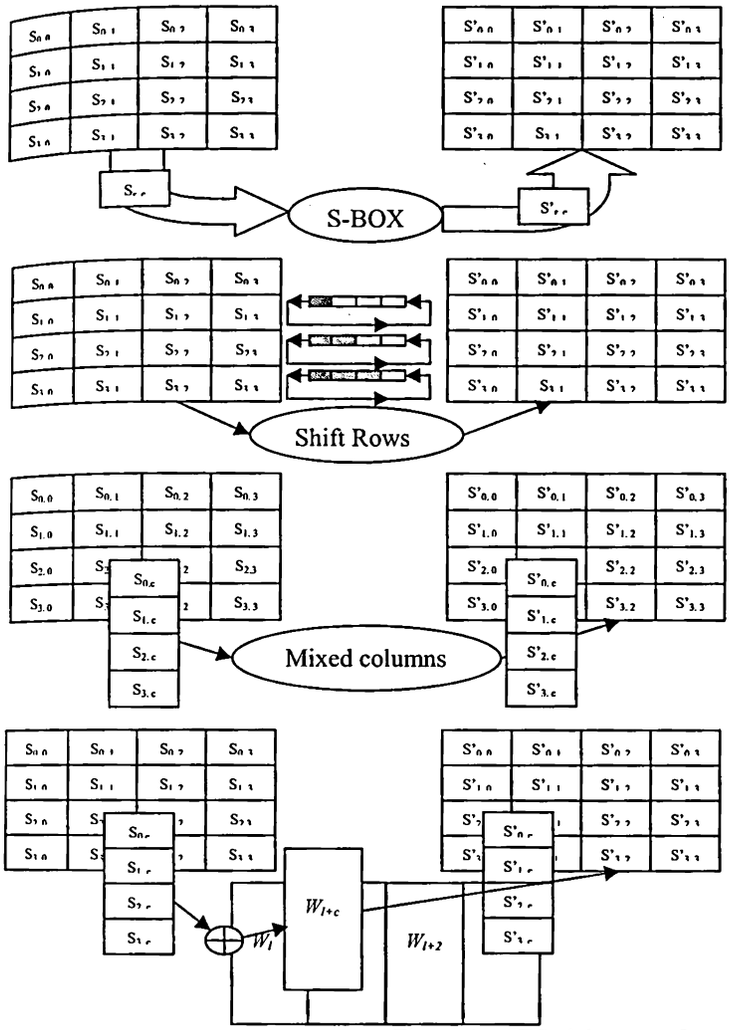


Figure 1 : AES cipher transformation

AES With CCM Mode

IEEE 802.15.4 uses CCM* mode which is composed of AES-CTR and CBC-MAC to provide message confidentiality and integrity. Two parameters (L and M) are important to run CCM mode in IEEE 802.15.4. They are coded as (L-1) and ((M-2)/2) respectively, where each one is stored as 3-bit. M (refers to the size of tag in byte unit) and L (refers to the number of bytes that needed to represent the size of message) where M $\in$ {4, 6, 8, 10, 12, 14, 16} and L $\in$ {2, 3, 4, 5, 6, 7, 8}. The length of: message, nonce and the tag are computed by (L and M) parameters. The message size (l (m)) is less than 2^{8*L} bytes, the nonce length is equal to (15-L) bytes, and the tag length is equal to (8*M) bits. The size of additional authentication data (l (a)) is less than 2^{64} bytes and it is independent of M and L parameters.

To perform data authentication a sequence of blocks B_0, B_1, B_2 ... B_n should be produced which is the input to AES-CBC-MAC algorithm. The first block (B_0) is structured as shown in figure 2(a). The first octet assigned for the flags, then (15- L) octets for nonce, then (L) octets assign to store the message length (l (m)). The flags octet includes (L) and (M) parameters in the first 6 bits (each parameter coded in 3-bit), then one bit is set to one when additional authentication data is enabled as shown in figure 2(b). The last bit is reserved for future use which is set to zero. The message is breaking to sequence of 128-bit blocks (B_1, B_2 ... B_n). Then a sequence of blocks (A_0, A_1 ...) is generated where each block is formatted as shown in figure 3. In the flag octet the first 3-bit assigned for L. The next 3-bit in addition to two reserved bits are set to zero. The (A_i) blocks are distinct from (B_i) blocks because the

value of 3-bit assigned to M will have none zero value in (B_i) blocks, but the same bits are set to zero in (A_i) blocks. For the octets from 16-L to 15 are assigned to counter and from 1 to 15-L are assigned to nonce. The CCM mode is implemented by running CTR and CBC-MAC together as shown in figure 4. The block (B_0) is encrypted (E) by AES and key (K) to compute (X_1). The authentication code is computed in Eq. 1. The ciphertext is produced by XOR plaintext blocks with a sequence of blocks (S_1, S_2 ...) as shown in figure 4(b). The sequence is computed in Eq.2. The block (A_0) is not used to cipher plaintext but it is XOR with (X_{n+1}) to compute message authentication code.

$$X_{i+1} = E_K (X_i \oplus B_i), \text{ where } i = 1 \text{ to } n \qquad (1)$$

$$S_i = E_K (A_i), \text{ where } i = 0... \qquad (2)$$

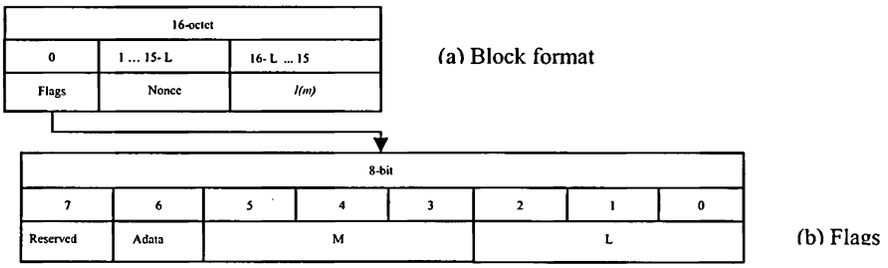


Figure 2 : Block (B_0) and flags format

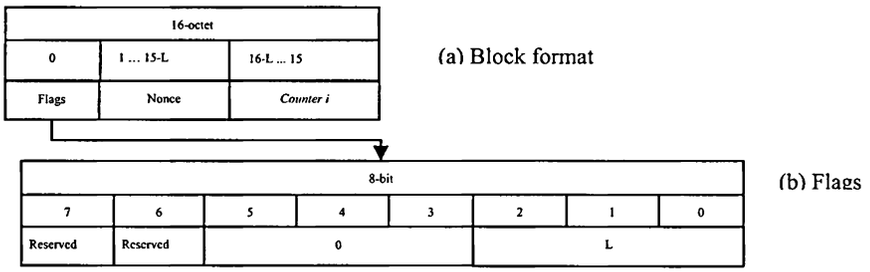
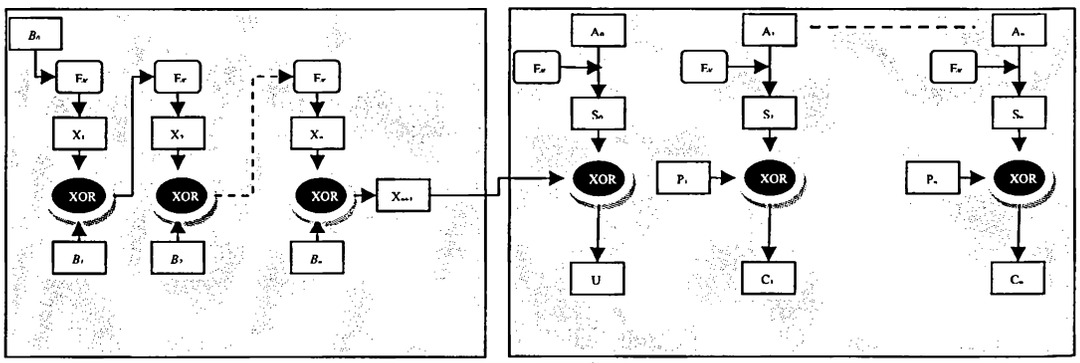


Figure 3 : Block (A_i) and flags format



(a)CBC-MAC (b)AES-CTR

Figure 4 : Message encryption and authentication by AES-CCM

Analysis of MKP-AES

MKP employs ECC to generate multiple keys to be used for ciphertext production. AES uses one secret key to cipher the plaintext message; however MKP uses (n) keys to do that. Moreover, the message is broken to (n) sub messages, where one key (K_i) is assigned to each sub message. The security level of the connection is computed by the number of generated keys. The secret key strength and cryptosystem system complexity is very important because it refers to robustness of security system. Brute force attack is trying to break the secret key by estimating the key based on its length. Secret key strength is limited to its length. The time complexity of secret key is computed by its length as notated in Eq.3, where (len) is the length of the key. For the IEEE 802.15.4 standard, 128-bit secret key is assigned for AES. The 128-bit key length time complexity is computed as O ($\log_2 64$), which is less secure than required. However, MKP provides (n) keys that mean the time complexity for key will be increased by (n) times as referred in Eq.4. In addition to confidentiality and authenticity, IEEE 802.15.4 has a protection against a replay attack. Nonce is used to distinguish among messages. The strength of nonce belongs to its length. The attacker should try 2^S times (S is the length of nonce) to break the nonce. The length of nonce (S) in IEEE 802.15.4 is computed by the counter length (L) as shown in Eq. 5. The MKP provide a single nonce for all sub messages. The length of nonce is computed by security level (n) and message size (m). The message is divided to (n) groups of sub messages; each sub message has (B) blocks as quoted in Eq.6. The number of bytes for counter representation (L) is computed by number of blocks per group (B) as referred in Eq.7. From Eq. 5, 6 and 7, it founded that MKP trades the length of nonce (S) to the message size and number of security level. The message size (m), which is measured by number of blocks, should be greater than the level of security (n). The perfect state is when the value of (L) is equaled to 1, where the maximum nonce length (S) is 14. By substitution in Eq. 6 and 7 it found that the maximum nonce length when the number of blocks per group (B) is 256.

$$\textit{Time complexity} = O(\log_2(len/2)) \quad (3)$$

$$\textit{MKP Time complexity} = O(n \log_2 64) \quad (4)$$

$$S = 15 - L \quad (5)$$

$$B = m/n \quad (\text{where } m > n) \quad (6)$$

$$L = (\log_2 B)/8 \quad (7)$$

Result

In this paper, we proposed nine different security levels (1 ... L_2^i, i=1 to 8), and 24 messages which have different size (2^j blocks, j=9 to 32 and block size is 16-byte), to compute the nonce length. The first level of security is considered as the original state with one group of blocks. Figure 5 shows the messages with size from 2^9 to 2^{16} had maximized their nonce length with security levels from L_2 to L_2^i (i = 2 to 8) respectively. The nonce length for messages with size from 2^{17} to 2^{24} blocks, had increased to become 13-byte, after grouping their blocks to 2^1 ... 2^i (i=2 to 8) groups respectively. The messages with the size from 2^{25} to 2^{32} blocks had increased their nonce length from 11to12 bytes. The computed result shows that for security level (n), the list of messages (G_1, G_2 ...) get nonce length incremental where the size of each message (m) is computed in eq.6.

$$\log_2(m) = 8 + \log_2(n) + 8*j, \; j = 0, 1 \ldots, n = 2, 4, 8, 16 \ldots \quad (8)$$

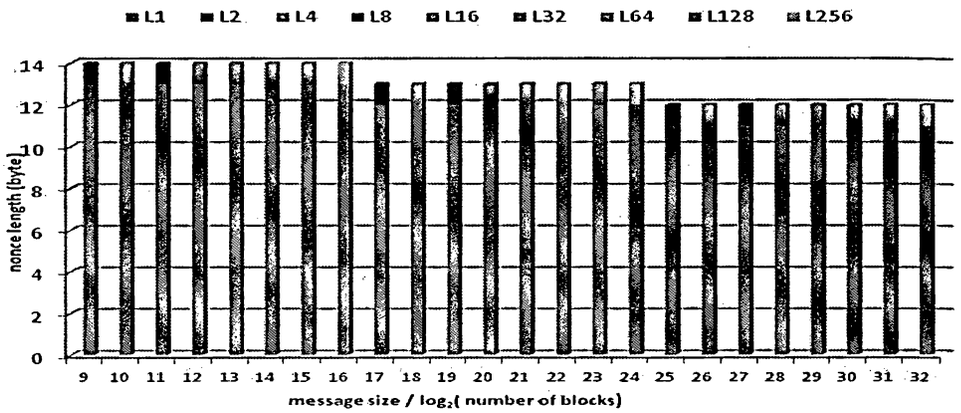


Figure 5 : Nonce length incremental over different security level

Conclusion

The analysis of MKP in this paper proves that the MKP increases the security strength of the system when using higher level of security. When the level of security is increased then the time complexity will be higher as computed to the previous level because the number of secret keys equals to the level of security. Also, the nonce length increases during higher level of security, where the sub messages have less size than original message that gives more byte for nonce in block fragment.

References:

LAN/MAN Standards Committee (2006). IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 15.4: Wireless MAC and PHY Specifications for Low-Rate WPANs, http://profsite.um.ac.ir/~hyaghmae/ACN/WSNMAC1.pdf.

Ahamed, S (2009). The role of zigbee technology in future data communication system. Journal of Theoretical and Applied Information Technology, 5, 129 - 135.

FIPS (2001). Announcing the advanced encryption standard (AES). Information Technology Laboratory, National Institute of Standards and Technology.

Dworkin, M (2004). Natl. Inst. Stand. Technol. Spec. Publ. 800-38C 25 pages (May 2004) CODEN: NSPUE2

Bernstein, D (2005). Understanding brute force, Workshop Record of ECRYPT STVL Workshop on Symmetric Key Encryption, eSTREAM report, 36.

Al-alak, S, Ahmed, Z, Abdullah, A, Subramiam, S (2011). AES and ECC Mixed for ZigBee Wireless Sensor Security. International Conference on Sensor Networks, Information, and Ubiquitous Computing (ICSNIUC'11). pp. 535-539. World Academy of Science, Engineering and Technology, Singapore.

Housley, R, Drive, S, Whiting, D, Ferguson, N. Counter with CBC-MAC (CCM) AES Mode of Operation Submission to NIST. http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ccm/ccm.pdf.

Rogaway, P (2011). Evaluation of Some Blockcipher Modes of Operation, Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan.

Daemen, J, Rijmen, V. AES Proposal: Rijndael, http://ftp.csci.csusb.edu/ykarant/courses/w2005/csci531/papers/Rijndael.pdf.

ANTI-SYNCHRONIZATION OF CHAOTIC SYSTEMS VIA ACTIVE SLIDING MODE CONTROL WITH APPLICATIONS TO CRYPTOGRAPHY

Wafaa Jawaada [1], M.S.M. Noorani [2] and M. Mossa Al-sawalha [3]
[1,2]*School of Mathematical Sciences, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia.*
[3] *Mathematics Department, Faculty of Science, University of Hail, Kingdom of Saudi Arabia.*
[1] *wafaibrahimj@gmail.com,* [2] *msn@ukm.my ,*[3]*sawalha_moh@yahoo.com*

Abstract:

In this paper, we present sliding mode anti-synchronization scheme to anti-synchronize two identical chaotic systems with different initial conditions. Analytical analysis will be done to prove the efficiency and robustness of this method alongside with numerical simulations. The anti-synchronization scheme is then used to design a methodology for text encryption. The encryption scheme will be secure and efficient since it is relaying on chaotic dynamical systems. And the efficiency of the encryption scheme will depend on the accuracy of the anti-synchronization method.

Keywords: Anti-synchronization, Active control, sliding mode control

Introduction

Since 1990, when Pecora and Carroll (Pecora and Carroll 1990) made history and introduced a method to synchronize two identical chaotic systems with different initial conditions. Several approaches are presently available to gain synchronization between two dynamical systems. (Yassen 2003,Zhang and Lu 2008,Yu and Cao 2007).

Chaos synchronization can be applied widely in the fields of physics and engineering systems, such as in power converters, chemical reactions, biological systems, information processing, and especially for secure communication (Feki 2003;Alasty and Shabani2006). These important applications and yet more are the reason of the so many researches and investigations which were done by scientists on this area. Causing revolution in the subject in a relatively short time.

Cryptography is the process of conversion of data into a secret code for transmission over a public network. Today, most cryptography is digital, and the original text ("plaintext") is turned into a coded equivalent called "ciphertext" via an encryption algorithm. The ciphertext is decrypted at the receiving end and turned back into plaintext.
The main importance of cryptography is the maintaining the confidentiality of data transmitted over a public channel. Nowadays, cryptography is widely used in many areas including data storage in disks, internet banking, shopping over the internet, protection of communications channels, etc.

The most recent approaches of cryptography uses chaotic process to generate the secrete key that hides the data (Schmitz 2001;Smaoui. and Kanso 2007), the researches in that area led directly to the use of synchronization of chaotic systems in the cryptography process. Since then many researchers (Banerjee and Chowdhury2009; Banerjee 2009; Chen 2010) have contributed in this field of research. This work aims to employ the technique developed by the authors in (Jawaada et. al. 2011) to design a scheme for text encryption.

Active sliding mode controller design

Consider a chaotic system described by the following nonlinear differential equation:

$$\dot{x} = A\,x + f(x) \qquad (1)$$

where $x(t) \in R^n$ denotes the system's n^{th}- dimensional state vector, $A \in R^{nxn}$ represents the Linear part of the system dynamics and $f : R^n \times R^n$ is the nonlinear part of the system.

Relation (1) represents the master system. The controller $u(t) \in R^n$ is added into the slave system, so it is given by:

$$\dot{y} = A\,y + f(y) + u(t) \qquad (2)$$

where $y(t) \in R^n$ is the slave system's n^{th} - dimensional state vector, $A \in R^{nxn}$ and $f: R^n \times R^n$ play similar roles as A and f for the master system.

The anti-synchronization problem is to design the controller $u(t) \in R^n$ which anti-synchronizes the states of the master and slave systems. The dynamics of the anti-synchronization errors can be expressed as

$$\dot{e} = A(y + x) + f(x) + f(y) + u(t) = Ae + F(x,y) + u(t) \qquad (3)$$

where $e = y + x$ and $F(x, y) = f(y) + f(x)$. Our goal is to design the controller $u(t) \in R^n$ such that

$$\lim_{t\to\infty} \|e\| = \lim_{t\to\infty} \|y(t, t_0) + x(t, t_0)\| = 0 \qquad (4)$$

Where $\|.\|$ is the Euclidian norm.
According to the active control design procedure, one uses the control input u(t) to eliminate the nonlinear part of the error dynamics. In other words, the input vector is considered as

$$u(t) = H(t) - F(x,y) \qquad (5)$$

The error system (3) is then rewritten as

$$\dot{e} = Ae + H(t) \qquad (6)$$

Eq. (6) describes the error dynamics with a newly defined control input H(t). There are many possible choices for the control H (t). Without loss of generality, we choose the sliding mode control law as follows:

$$H(t) = Kw(t) \qquad (7)$$

Where $K = [k_1, k2, k_3]^T$ is a constant gain vector and $w(t) \in R$ is the control input that satisfies:

$$w(t) = \begin{cases} w^+(t) & s(e) \geq 0 \\ w^-(t) & s(e) < 0 \end{cases}$$

and $s = s(e)$ is a switching surface which prescribes the desired dynamics. The resultant error dynamics is then

$$\dot{e} = Ae + Kw(t) \qquad (8)$$

In what follows, the appropriate sliding mode controller will be designed according to the sliding mode control theory.

Sliding Surface Design

The sliding surface can be defined as follows:

$$s(e) = Ce \qquad (9)$$

where $C = [c_1, c_2, c_3]$ is a constant vector. The equivalent control approach is found by the fact that $\dot{s}(e)=0$ is a necessary condition for the state trajectory to stay on the switching surface $s(e) = 0$. Hence, when in sliding mode, the controlled system satisfies the following conditions:

$$s(e) = 0 \quad and \quad \dot{s}(e) = 0 \qquad (10)$$

Now, using (8), (9) and (10), one can obtain:

$$\dot{s}(e) = \frac{\partial s(e)}{\partial e}\dot{e} = C\,[Ae - Kw(t)] \qquad (11)$$

Solving (11) for $w(t)$ results in the equivalent control $w_{eq}(t)$

$$weq(t) = -(CK)^{-1} CAe(t) \qquad (12)$$

where the existence of $(CK)^{-1}$ is a necessary condition. Replacing for $w(t)$ in (8) from $w_{eq}(t)$ of (12), the state equation in the sliding mode is determined as follows:

$$\dot{e} = [I - K(CK)^{-1}C]A \qquad (13)$$

As long as the system (9) has all eigenvalues with negative real parts, it is asymptotically stable.

Design of the Sliding Mode Controller

We assume that the constant plus proportional rate reaching law is applied. The reaching law can be chosen such that:

$$\dot{s} = -\frac{qs}{|s| + \gamma} - rs \qquad (14)$$

where$\gamma$is a positive real. The gains $q > 0$ and $r > 0$ are determined such that the sliding condition is satisfied and the sliding mode motion occurred. From (8) and (9), it can be found that

$$\dot{s} = C[Ae + Kw(t)] \qquad (15)$$

Now, from (14) and (15), the control input is determined as

$$w(t) = -(CK)^{-1}\left[C(rI + A)e(t) + rs + \frac{qs}{|s| + \gamma}\right] \qquad (16)$$

Stability Analysis

To check the stability of the controlled system, one can consider the following Lyapunov Candidate function:

$$V = \frac{1}{2}e^2 \qquad (17)$$

The time derivative of (17) is

$$\dot{V} = s\,\dot{s} = -\frac{qs^2}{|s| + \gamma} - rs^2$$

Since $qs^2 > 0$; $r > 0$ and $q > 0$ we have $\dot{V} = s\,\dot{s} < 0$, therefore $V(e)$ is negative definite. This property implies boundedness of the sliding surface s. The error dynamics can be obtained using (16) in (8).

$$\dot{e} = Ae - k\,(CK)^{-1}\left[C(rI + A)e(t) + rs + \frac{qs}{|s| + \gamma}\right] \qquad (18)$$

As a linear system with bounded input ($-K(CK)^{-1}q$ for s , 0 and $K(CK)^{-1}q$ for $s < 0$), the error system is asymptotically stable if and only if $[A - K(CK)^{-1}C(rI+A)]$ has negative eigenvalues. Because of the special structure for matrix A in the given chaotic systems, one of the eigenvalues is always r and therefore is stable. The two other eigenvalues are independent from r and determined by the other control parameters i.e. K and C. The latter two eigenvalues can be negative or positive depending on K and C values. By appropriate choices of r, K and C one is able not only to stabilize the error system but also to adjust the rate of the error convergence. The parameter q can be used to enhance the robust property expected from a sliding mode controller.

Active Sliding ModeCcontrolAanti-synchronization BetweenTwo Chen Systems with Different Initial Conditions.

To demonstrate the validity of our control input. We apply it to gain anti-synchronization Between two Chen systems with different initial conditions. The Chen system [11] is given by:

$$\begin{aligned} \dot{x} &= a(y - x) \\ \dot{y} &= (c - a)\,x - xz - cy \\ \dot{z} &= xy - b \end{aligned} \qquad (19)$$

Where x, y and z are state variables and a, b and c are positive parameters. Bifurcation studies shows that with the parameters $a = 35$ and $c = 28$, system (19) exhibits chaotic behavior when $b = 3$. So the drive and response systems are respectively given by:

$$\dot{x}_1 = a(y_1 - x_1)$$
$$\dot{y}_1 = (c - a)x_1 - x_1 z_1 - c y_1$$
$$\dot{z}_1 = x_1 y_1 - b z_1 \qquad (20)$$

And

$$\dot{x}_2 = a(y_2 - x_2) + u1$$
$$\dot{y}_2 = (c - a)x_2 - x_2 z_2 - c y_2 + u2$$
$$\dot{z}_2 = x_2 y_2 - b z_2 + u3 \qquad (21)$$

We add Eq. (20) to Eq. (21) to get:

$$\dot{e}_1 = a(e_2 - e_1) + u1$$
$$\dot{e}_2 = (c - a)e_1 - x_2 z_2 - x_1 z_1 - c e_2 + u2$$
$$\dot{e}_3 = x_2 y_2 + x_1 y_1 - b e_3 + u3 \qquad (22)$$

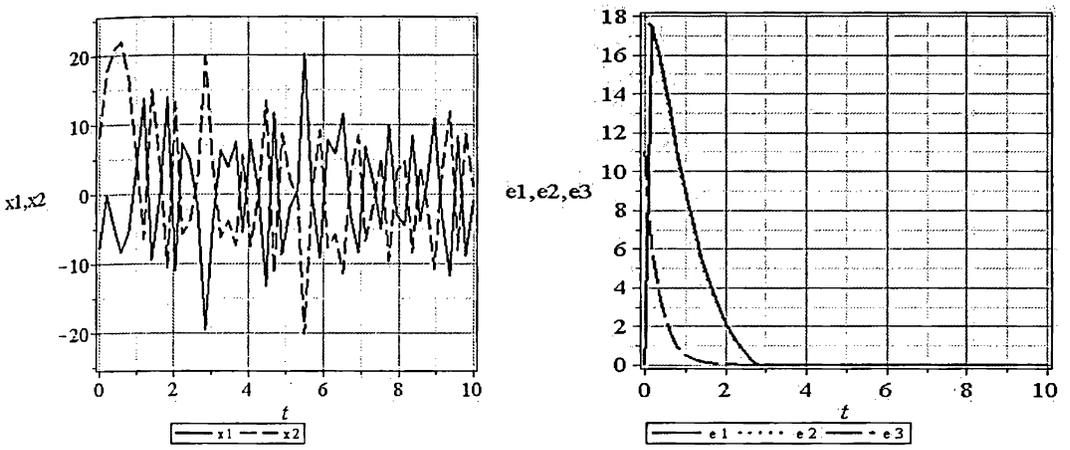
where $e_1 = x_2 + x_1$; $e_2 = y_2 + y_1$ and $e_3 = z_2 + z_1$ and u_i; $i = 1, 2, 3$ are the controllers to be designed according to section 2. The control parameters are chosen as $C = (0, 1, 1)$, $K = (0, 1, 0)^T$ and $q = 2$, $r = 1$ and $\gamma = 0.01$ then the switching surface

$$s(e) = e2 + e3 \quad \text{and} \quad w(t) = -[(c - a)e_1 + c e_2 - b e_3 + s + \frac{2s}{|s| + 0.01}] \qquad (23)$$

Inserting (23) into (22) yields an error system which is stable. Then response system Eq. (21) can anti-synchronize drive system Eq. (21) asymptotically.

Numerical Simulations

In this section, to verify and demonstrate the effectiveness of the proposed method, we discuss the simulation result for the active sliding mode anti-synchronization between two Chen system with different initial conditions. In the numerical simulations, the fourth-order Runge-Kutta method is used to solve the systems with time step size 0.001. For this numerical simulation, we assumed that the initial conditions, $(x_1(0), y_1(0), z_1(0)) = (-8, 8, 32)$ and $(x_2(0), y_2(0), z_2(0)) = (-6, 10, 20)$. Hence the error system has the initial values $e_1(0) = -14$, $e_2(0) = 18$ and $e_3(0) = 52$. The systems parameters are chosen as $a = 35$, $b = 3$, $c = 28$ in the simulations such that both systems exhibit chaotic behavior. Anti-synchronization of the systems Eqs. (21) and (20) via active sliding mode control laws in Eq. (24) are shown in Figure 1. Figure's 1(a)display the x state trajectories of drive system (20) and response system (21). Figure 1(b) display the error signals e_1, e_2, e_3 of two Chen systems with different initial conditions under the controller Eq. (24). And table (1) includes some values of the states x1 and x2 of master and slave systems after time t =10.



Designing of Anti-synchronization Based Encryption Scheme

Let us assume the actual message is in plaintext and denoted: p, Encrypted Message or cipher text is denoted c. The plaintext (p) and the corresponding cipher text (c) can be divided into message units, see table (1) (Banerjee 2009).

Table 1 : Representation of plaintext

0	1	2	3	4	5	6	7	8	9	10	11	12	...	37
0	1	2	3	4	5	6	7	8	9	- (space)	.	A	...	Z

Corresponds to every message unit we use one message key, which are randomly Generated. For a complete message the secret keys are a series of numbers $\{k_1, k_2 \ldots k_n\}$. Where kj hide and secure pj .
Consider the sliding mode anti-synchronization scheme, let the anti-synchronization occurs after $t = t_0$ Therefore we have
$y(t) = - x(t)$ at. $t \geq t_0$ (Anti-synchronisation).
Sender choose $\rightarrow$ xi (t)
Receiver choose $\rightarrow$ yi (t) at $t=t_1, t_2, t_3 \ldots$ respectively, after t_0.

To encrypt the message we do the following:

- First: Arrange the plaintext into sequence of real numbers

p1, p2, p3, p4, p5, p6, p7 . . .

- Then: The sender and receiver choose

$k_s = f(xi)$ And $k_r = f(-yi)$
Respectively from their corresponding time series at $t = t_1$, ($> t_0$) for the first key, where f is any suitable function of the state variables of the master and slave systems. At theanti-synchronized state ks= kr=k (say).

- Finally: the formula for the cipher text and recovered plaintext are

ci = pi + ki and pi = ci − ki respectively for i =1,2,3,...
Again they choose the value of k from the corresponding data series at $t = t_2 (> t_1)$ for the next key and continue the process. The flowchart in figure (2) describes this scheme

Concluding Remark

In this paper, we have applied an anti-synchronization scheme to two identical Chen systems with different initial conditions via active sliding mode control. We have proposed a novel active sliding mode control scheme for asymptotic anti-synchronization .Numerical simulations are provided to show the effectiveness of our method. Finally, the scheme is used to design an encryption scheme that is very robust.

Acknowledgement

This work is financially supported by Universiti Kebangsaan Malaysia Grant: UKM–DLP–2011–016.

References:

Alasty, A. and Shabani, R. (2006).Chaotic motions and fractal basin boundaries in springpendulum system.*Nonlinear Analysis: Real World Applications.* 7(1):81-95.
Banerjee,S. Chowdhury,A. (2009). Lyapunov function, parameter estimation, synchronization and chaotic cryptography. *Commun Nonlinear Sci Numer Simulat.*14: 2248–2254.

Banerjee,S.(2009). Synchronization of time-delayed systems with chaotic modulation and cryptography.*Chaos, Solitons and Fractals*42: 745–750 2.

Chen, J.et.al. (2010). Projective synchronization with different scale factors in a driven response complex network and its application in image encryption.*Nonlinear Analysis: Real World Applications*11: 3045_3058.

Feki M. (2003). An adaptive chaos synchronization scheme applied to secure communication. *Chaos, Solitons and Fractals* 18: 141-148.

Pecora,L.M.and Carroll, T.L. (1990). Synchronization in chaotic systems, *Phys. Rev. Lett.* 64: 821-824.

Schmitz, R. (2001). Use of chaotic dynamical systems in cryptography. *Journal of the Franklin Institute*338:429–441.

Smaoui, N., Kanso A. (2009). Cryptography with chaos and shadowing. *Chaos, Solitonsand Fractals*42: 2312–2321.

Jawaada, W.Noorani M.S.M. Al-sawalha M. (2012).Active Sliding Mode Control Anti-synchronization of Chaotic Systems with Uncertainties and External Disturbances,*Journal of Applied Math*ematics.doi:10.1155/2012/293709.

Yassen MT. (2005).Chaos synchronization between two different chaotic systems using active control. *Chaos Solitons Fractals.*23:131-40.

Yu, W.and Cao, J. (2007).Adaptive synchronization and lag synchronization of uncertaindynamical system with time delay based on parameter identification.*Physica A.* 375:467-482.

Zhang, Q.and Lu, J. (2008). Chaos synchronization of a new chaotic system via nonlinear control. *Chaos Solitons Fractals* 37:175-9.

BIVARIATE POLYNOMIALS AND ITS APPLICATION IN A PUBLIC KEY ENCRYPTION SCHEME

[1]Ruma Kareem Ajeena, [1]Hailiza Kamarulhaili and [2]Sattar B. Almaliky
[1]*School of Mathematical Sciences, Universiti Sains Malaysia,11800, Minden, Penang Malaysia*
[2]*Computer Sciences School, Babylon University, Iraq.*
ruma_kareem@yahoo.com, hailiza@cs.usm.my, Sattar-Almaliky@yahoo.com

Abstract:

The Polynomial Reconstruction is one of the important problems in cryptography. There are several public key cryptographic systems constructed based on this problem.This paper provides an analytical study on a public key cryptosystem (PKC) that was based on bivariate polynomial Reconstruction Problem (BPRP) and takes into considerations the developments performed on the (PKC). A modification was proposed using bivariate polynomial instead of univariate polynomial which is used in the original Augot's system to enhance its security. The analysis concerned mainly the mathematical backgrounds related to bivariate polynomials and the operation, valid generally for these polynomials, especially in the finite fields GF(q). The coding problem is included in the public key cryptosystem that considers the (BPRP). The Reed-Solomon Code is used in such type of (PKC) based on (BPRP).

Introduction

Cryptography is one of the oldest fields of technical study. The records went back at least 4000 years. Only 3 systems in widespread use remain hard enough to break to be of real value. One of them takes too much space for most practical uses, another is too slow for most practical uses, and the third is widely believed to contain serious weaknesses. [1].

The Cryptography is a term which refers to the design of cryptosystems and cryptanalysis. This science Cryptology is divided into three parts; the cryptosystem designing part which is specialized in designing and constructing cryptosystems, the cryptanalysis part which is specialized in finding techniques and methods of transforming the cipher text to plain text, and the evaluation of the algorithms part which is specialized in calculating the complexities of these algorithms [2]. We consider a special class of Bose, Chaudhuri and Hocquenghem (BCH) codes and several important techniques available to enhance error correction capabilities. In particular the well known Reed-Solomon Codes, is very widely used in mass storage systems to correct the burst errors associated with media defects. Reed Solomon error correction is a coding scheme which works by first constructing a polynomial from the data symbols to be transmitted and then sending an over-sampled plot of the polynomial instead of the original symbols themselves. Because of the redundant information contained in the over-sampled data, it is possible to reconstruct the original polynomial and thus the data symbols even in the face of transmission errors, up to a certain degree of error [3].

Electronic commerce requires at least the following fundamental cryptological primitives: one digital signature, one public-key encryption or key exchange scheme, and symmetric cipher. Currently deployed PKCs most involve the integer factoring problem or BPRP. We aim to introduce a new public-key encryption scheme that may be used for this problem. This is one of many schemes based on the difficulty of solving a system of bivariate polynomial equations. PKCs of this class are usually described as Bivariate (multivariate) or polynomial – based schemes [4].

Mathematical Background

Definition 2.1 : [5] A polynomial in two variables (that is a bivariate polynomial) with constant coefficients is given by

$$a_{n\,m}\,x^{n}\,y^{m}+\ldots+a_{22}\,x^{2}\,y^{2}+a_{21}\,x^{2}\,y+a_{12}\,x\,y^{2}+a_{11}\,x\,y+a_{10}\,x+a_{01}\,y+a_{00}. \qquad (1)$$

Definition 2.2 : [5] The sum of two polynomials is obtained by adding together the coefficients sharing the same powers of variables (i.e., the same terms).

For example, $(a_2 x^2 + a_1 x + a_0) + (b_1 x + b_0) = a_2 x^2 + (a_1 + b_1) x + (a_0 + b_0)$. (2)

This polynomial has order less than (in the case of cancellation of leading terms) or equal to the maximum order of the original two polynomials. Similarly, the product of two polynomials is obtained by multiplying term by term and combining the results, for example

$$\begin{aligned}(a_2 x^2 + a_1 x + a_0)(b_1 x + b_0) &= a_2 x^2 (b_1 x + b_0) + a_1 x (b_1 x + b_0) + a_0 (b_1 x + b_0) \\ &= a_2 b_1 x^3 + (a_2 b_0 + a_1 b_1) x^2 + (a_1 b_0 + a_0 b_1) x + a_0 b_0, \end{aligned} \quad (3)$$

and has order equal to the sum of the orders of the two original polynomial [5].

Definition 2.3: The ***Reed- Solomon Code*** ([*n*, *k*] RS_k code) of dimension *k* and length *n* over F_q is the following set of *n* - tuples (codeword):

$$RS_k = \{ev(f(x,y)) : f \in F_q[x,y], \deg(f) < k\}, \quad (4)$$

where F_q $[x,y]$ is the set of bivariate polynomials with coefficients in F_q. The set $(x_i, y_j) i, j \in \{1,2,\ldots..,\ n\}$ is called the Support of RS_k.

Example 2.1: Suppose we have *4* 2D points (0, 1), (2, 5), (4, 3), and (6, 7) and we have values for each of these points, e.g., ((0, 1), 13), ((2, 5), 17), ((4, 3), 15), and ((6, 7), 18) and we want to fit a bivariate polynomial through these points .

From the Vander monde method, it would make sense that we could find an interpolated bivariate polynomial with four terms, for example:

$$p(x, y) = c_1 xy + c_2 x + c_3 y + c_4 \quad (5)$$

Thus, if we were to simply evaluate $p(x, y)$ at these four points, we get four equations:

$$\begin{aligned} p(0, 1) &= c_1 0 + c_2 0 + c_3 1 + c_4 = 13 \\ p(2, 5) &= c_1 10 + c_2 2 + c_3 5 + c_4 = 17 \\ p(4, 3) &= c_1 12 + c_2 4 + c_3 3 + c_4 = 15 \\ p(6, 7) &= c_1 42 + c_2 6 + c_3 7 + c_4 = 19 \end{aligned}$$

This defines a system of linear equations which we may solve. In this case, the Vander monde matrix is the rather simple

$$\begin{bmatrix} 0 & 0 & 1 & 1 \\ 10 & 2 & 5 & 1 \\ 12 & 4 & 3 & 1 \\ 42 & 6 & 7 & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} = \begin{bmatrix} 13 \\ 17 \\ 15 \\ 19 \end{bmatrix}$$

How to find an interpolating polynomial which passes through *n* points $((x_1, y_1), z_1), \ldots, ((x_n, y_n), z_n)$.

Assuming the (x, y) pairs of values are unique. Since there are n points, the degree of the interpolating polynomial must have n terms. Thus, the form of the interpolating polynomial may be various, for example, given four points in a square, (0, 0), (0, 1), (1, 0), (1, 1), the logical choice is:

$$p(x, y) = c_1 xy + c_2 x + c_3 y + c_4.$$

Given nine points in a square, we could use,

$$p(x, y) = c_1 x^2y^2 + c_2 x^2y + c_3 xy^2 + c_4 x^2 + c_5 y^2 + c_6 xy + c_7 x + c_8 y + c_9.$$

We define the $n \times n$ Vander monde matrix V by evaluating the n terms on each of the n points. We can generalize the Vandermonde method to interpolate multivariate real-valued functions. We will focus on bivariate polynomials, and the generalization is obvious.

Definition 2.4(Bivariate Interpolation)[6]: Let $f(x, y)$ be a function defined for a surface. Given points $((x_1, y_1), z_1)$, $((x_2, y_2), z_2)$, ..., $((x_n, y_n), z_n)$. To find an interpolating polynomial, we simply substitute the points into the bivariate polynomial, and obtained naturally a system of linear equations in the coefficients which may then be solved using Gaussian elimination or LU decomposition.

Example 2.2: Find the polynomial which interpolates the points ((3, 3), -1), ((3, 4), 2), ((5, 3), 1). Because there are three points, the interpolating polynomial could be of the form $p(x, y) = c_1x + c_2y + c_3$. Thus, we define the Vander monde matrix

$$\begin{bmatrix} 3 & 3 & 1 \\ 3 & 4 & 1 \\ 5 & 3 & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} -1 \\ 2 \\ 1 \end{bmatrix}$$

and solve the system Vc = Z, where Z = $(-1, 2, 1)^T$. This gives the result c = $(1, 3, -13)^T$, and therefore the interpolating polynomial is $p(x, y) = x + 3y - 13$.

Example 2.3: Find the polynomial which interpolates the points ((3, 3), 5), ((3, 4), 6), ((4, 3), 7), ((4, 4), 9). Because there are four points, the interpolating polynomial could reasonably be of the form $p(x) = c_1xy + c_2x + c_3y + c_4$. Thus, we define the Vander monde matrix

$$\begin{bmatrix} 9 & 3 & 3 & 1 \\ 12 & 3 & 4 & 1 \\ 12 & 3 & 4 & 1 \\ 16 & 4 & 4 & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} = \begin{bmatrix} 5 \\ 6 \\ 7 \\ 9 \end{bmatrix}$$

and solve the system Vc = Z where Z = $(5, 6, 7, 9)^T$. This gives the result c = $(1, -1, -2, 5)^T$, and therefore the interpolating polynomial is $p(x, y) = xy - x - 2y + 5$.

Cryptographic System Based on BPRP

At Euro crypt 2003 **Augot** and **Finiasz** in 2003 [5] proposed a first public key encryption scheme based on the (PRP). This section will present discussion of the performances and state the parameters that are required to reach the desired security level from such scheme. Let us consider the following **parameters:**

- F_q is a finite field, q is the size of F_q.

- n is the length of the Reed –Solomon code used by this scheme.
- k its dimension.
- W is the weight of a large error E, so that the PRP for n, k, W is believed to be hard, or it must have $W > (n-k)/2$ which need to be verified.
- w is the weight of a small error e, such that $w \leq (n-k)/2$

Key Generation Process

Let us consider that we have two parties A and B. Then want to have their communication using modified cryptosystem based on the bivariate polynomial.
A secretly do the followings:

- Choose the sets x and y.
- Generates a monic (unitary) bivariate polynomial $p(x, y)$ of degree equal to k -1, with respect x and y.
- Generates an error vector E of dimension n with the weight W, where W is exactly non zero coordinates.
- Computes the codeword $C = ev(p(X, Y)) = p(x_i, y_j)$ of RS_k, $\exists$ $x_i = i$ and $y_j = j$ for $i = 1,2,\ldots\ldots,n$ and $j = 1,2,\ldots\ldots,n$.
- Computes

$$Pk = C+E, \qquad (6)$$

where Pk is the public-key, while C and E are kept secret or the secret- key is (C, E).

Example 3.1: Let us have Modified Augot's Cryptosystem, $n = 8$, $k = 3$, and $F_q = F_{11}$. Then it is required to generate the public-key. Let $x = (2,3,3,4,5,6,7,8)$, $y = (4,3,6,2,1,5,7,8)$.

- Generate a monic bivariate polynomial $p(x, y) = x^2y + xy^2 + 3xy + 5$.
- Generate a random 8 - dimension vector E of weight $W = 3$, is exactly non zero coordinates, $E = (0,0,0,10,0,7,3,0)$, since $W > \lfloor (n-k)/2 \rfloor = 2$. That is, $W = 3$.
- Compute the codeword $C = ev(p(X, Y))$ of RS_k. That is, $C = p(x_i, y_j) \bmod q$, $\exists$ $x_i = i$ and $y_j = j$ for $i = 1,2,\ldots\ldots,n$ and $j = 1,2,\ldots\ldots,n$.
  $p(2, 4) = 0, p(3, 3) = 9, p(3, 6) = 1, p(4, 2) = 0, p(5, 1) = 6, p(6, 5) = 7, p(7, 7) = 2,$
  $p(8, 8) = 0$. Then $C = (0,9,1,0,6,7,2,0)$.

The public-key is $Pk = C+E = (0,9,1,10,6,3,5,0)$.

Encryption Process

Let us consider that B wishes to send a message to A. The message m_0 of length $k+1$ over the alphabet F_q. The following steps will be performed :

- Generates the m_0 bivariate polynomial of length $k+1$, where $m_0 = m_{0,0}, \ldots\ldots, m_{0,k+1}$ is seen as the polynomial :

$$m_0(X, Y) = m_{0,0} + m_{0,1} Y + m_{0,2} X + \ldots\ldots\ldots + m_{0,k-2} X^{k-2} Y^{k-2} \qquad (7)$$

- The message is firstly encoded using (Reed-Solomon Code) into a codeword m in RS_{k-1}.
- Randomly generates a primitive element $\alpha \in F_q$.
- Randomly generates an error pattern vector e of dimension n with the weight w, where w is exactly non zero coordinates.
- Compute the cipher text

$$CT = m + \alpha \times Pk + e. \qquad (8)$$

- Transmits CT to A.

Example 3.2: Let us have Modified Augot's Cryptosystem, $n = 8$, $k = 3$, and $F_q = F_{11}$ and $Pk = (0,9,1,10,6,3,5,0)$. Then it is required to compute the encrypted message. The encryption of the message can be computed as follows :
Let $m_0(X, Y) = xy + 2x + 4y + 3$, that length $k+1 = 4$, deg $(m_0) = 1$ with respect x and y,
and the coefficients 2, 4 and 3 $\in F_{11}$.
Compute m_s for s = 1, 2, ..., 8.
$m_1 = m_0(2, 4) = 9$, $m_2 = m_0(3, 3) = 8$, $m_3 = m_0(3, 6) = 7$, $m_4 = m_0(4, 2) = 5$, $m_5 = m_0(5, 1) = 0$, $m_6 = m_0(6, 5) = 10$, $m_7 = m_0(7, 7) = 6$, $m_8 = m_0(8, 8) = 5$.
That is $m = (9, 8, 7, 5, 0, 10, 6, 5)$, let $\alpha = 3 \in F_{11}$ and since $w \le \lfloor (n-k)/2 \rfloor = 2$, let $w = 1$, then $e = (0, 0, 0, 0, 0, 7, 0, 0)$, where e has exactly $w = 1$ non zero coordinates.

The cipher text is $CT = m + \alpha \times Pk + e$, that is CT_s for $s = 1,2,.....,8$.

$CT_1 = m_1 + \alpha \times Pk_1 + e_1 = 9$, $CT_2 = 2$, $CT_3 = 10$, $CT_4 = 2$, $CT_5 = 7$, $CT_6 = 4$, $CT_7 = 10$,
$CT_8 = 5$. then $CT = (9, 2, 10, 2, 7, 4, 10, 5)$.

Decryption Process

We proposed a modification to this system by using Vander monde interpolation Method instead of Berlekamp-Welch Interpolation that was used in the original Augot system. Hence we will describe the steps of the proposed decryption process.

Upon receipt of $CT = m + \alpha \times Pk + e$. **A** will perform the following steps:

- Considers only the positions where $E_i = 0$.
- Considers the shortened code of length n-W which is also a Reed Solomon Code of dimension k, $(\overline{RS_k})$.
- Solve the equation $\overline{m} + \alpha \times \overline{C} + \overline{e} = \overline{CT}$, where $\overline{m}$, $\overline{C}$, $\overline{e}$ correspond to the shortened versions of m, C, e. And E has disappeared, $\overline{m} + \alpha \times \overline{C} \in \overline{RS_k}$.
- Computes by using Vander monde interpolation Method, the unique polynomial $q(X, Y)$ of degree k -1 such that $ev(q(X, Y)) = \overline{m} + \alpha \times \overline{C}$.
- Computes $q(X, Y) - \alpha\, p(X, Y) = m_0(X, Y)$, where α leading coefficient of $q(X, Y)$, $\overline{C} = ev(p(X, Y))$ and $p(x, y)$ has degree k -1, deg $(m_0) \le k$ -2.

Example 3.3: Let us have Modified Augot's Cryptosystem based on bivariate polynomial, $n = 8$, $k = 3$, and $F_q = F_{11}$, $Pk = (0,9,1,10,6,3,5,0)$ and $CT = (9, 2, 10, 2, 7, 4, 10, 5)$. Then it is required to apply the decryption process and recover the message.

The decryption of the cipher text and recover the message can compute by the steps:
Firstly, compute n-$W = 5$. That is, $E_1 = E_2 = E_3 = E_5 = E_8 = 0$, and
$\overline{CT} = (CT_1, CT_2, CT_3, CT_5, CT_8) = (9, 2, 10, 7, 1)$. By using Vander monde interpolation Method, we can compute the unique bivariate polynomial $q(X, Y)$ of degree k -1= 2 with respect x and y such that $ev(q(X, Y)) = \overline{m} + \alpha \times \overline{C}$. Since $\overline{CT} = \overline{m} + \alpha \times \overline{C} + \overline{e}$, where $\overline{m} + \alpha \times \overline{C} \in \overline{RS_k}$, and $\overline{e} < \overline{w} \le (n\text{-}W\text{-}k)/2$. Then $\overline{CT} = ev(q(X, Y)) = \overline{m} + \alpha \times \overline{C}$, that is,
$CT_1 = q(2, 4) = 9$, $CT_2 = q(3, 3) = 2$, $CT_3 = q(3, 6) = 10$, $CT_5 = q(5, 1) = 7$,
$CT_8 = q(8, 8) = 5$. Now, applying the Vander monde interpolation method to find a bivariate polynomial $q(X, Y)$.
Since x = 2, 3, 3, 4, 5, 6, 7, 8 and y= 4, 3, 6, 2,1, 5, 7, 8,
then we get five shadows: CT_1, CT_2, CT_3, CT_5, CT_8, we can construct $q(X, Y)$ from four of the shadows: CT_1, CT_2, CT_3, CT_8.
Let $q(X, Y) = q_1 x^2y + q_2xy^2 + q_3xy + q_4x + q_5y + q_6$,
we have,

$9 = q_1 (16) + q_2(32) + q_3(8) + q_4(2) + q_5(4) + q_6$
$2 = q_1 (27) + q_2(27) + q_3(9) + q_4(3) + q_5(3) + q_6$
$10 = q_1 (54) + q_2(108) + q_3(18) + q_4(3) + q_5(6) + q_6$
$5 = q_1 (512) + q_2(512) + q_3(64) + q_4(8) + q_5(8) + q_6$

$$\begin{bmatrix} 5 & 10 & 8 & 2 & 4 & 1 \\ 5 & 5 & 9 & 3 & 3 & 1 \\ 10 & 9 & 7 & 3 & 6 & 1 \\ 6 & 6 & 9 & 8 & 8 & 1 \end{bmatrix} \begin{bmatrix} q_1 \\ q_2 \\ q_3 \\ q_4 \\ q_5 \\ q_6 \end{bmatrix} = \begin{bmatrix} 9 \\ 2 \\ 10 \\ 5 \end{bmatrix}$$

By using Gaussian Elimination we can find the coefficients $q_1 = 3$, $q_2 = 3$, $q_3 = 10$, $q_4 = 2$, $q_5 = 4$, $q_6 = 7$.Then

$$q(X, Y) = 3x^2y + 3xy^2 + 10xy + 2x + 4y + 7.$$

The leading coefficient of $q(X, Y) = 3 = \alpha$. Then the message is

$m_0(X, Y) = q(X, Y) - \alpha\, p(X, Y)$.

$= 3x^2y + 3xy^2 + 10xy + 2x + 4y + 7 - 3(x^2y + xy^2 + 3xy + 5)$

$= (xy + 2x + 4y - 8) \bmod 11$

$= xy + 2x + 4y + 3$.

Security Implications

In our modified scheme based on bivariate polynomial, we have managed to apply the scheme on key generation process, encryption and decryption processes of the cryptosystem. This improvement has increased the security level compared with the original cryptosystem which was based on a univarate polynomial. The adversaries will have to solve for two variables equation systems instead of just a single variable in the univariate version. This in return will give more running time to attack the bivariate polynomial cryptosystem based.

Conclusions

Giving the public-key and cipher text, we can recover the corresponding plaintext in bivariate polynomial. The proposed modified Cryptosystem based on BPRP and using Vander monde interpolation method is comparable with the original system. The use of polynomials with two variables instead of polynomials with one variable, help us to increase security level and resistance against many attacks. This work can be further extended to multivariate polynomials, where we can generalize the modified cryptosystem by using multivariate polynomials.

References:

Wikipedia , " History of Cryptography " , the free encyclopedia en.wikipedia.org/wiki / History_ of_cryptography.

W. Diffie And M. E. Hellman ,"New Directions in Cryptography", IEEE trans. Inform. Theory ,Vol. IT-22

L-C. Wang, B-Y. Yang Y-H Hu, and F. Lai, " A Medium-Field Multivariate Public key encryption scheme

D. Augot and M. Finiasz, "A public key encryption scheme bases on the Polynomial Reconstruction Problem" , Proceedings of Euro crypt2003.

Bivariate Polynomials – Wikipedia, the free encyclopedia, en.wikipedia.org/wiki/Polynomial_function

Douglas Wilhelm Harder, " Vandermonde Method (HOWTO)", University Avenue West Waterlo against many of the attackso,Ontario, Canada N2L 3G1, ece.uwaterloo.ca/~ece204/TheBook/.../vandermonde/

KARATSUBA MULTIPLICATION ALGORITHM BASED ON THE BIG-DIGITS AND ITS APPLICATION IN CRYPTOGRAPHY

Shahram Jahani and Azman Samsudin
School of Computer Sciences, Universiti Sains Malaysia, 11800 Penang, Malaysia
Jahani2001@yahoo.com, azman@cs.usm.my

Abstract:

The efficiency of number theory based cryptosystems correlatesdirectly to the efficiency of large integer multiplication operation.In this paper, we propose a hybrid of Karatsuba-Classical multiplication algorithm that is based on a Look-up table of "Big-Digits" representation. The Big-Digits representation is a more compact representation compared to the binary representation.Therefore,by using the Big-Digits representation, the number of sub-multiplication operations in a multiplication algorithm will reducesignificantly. The results of this study show that the proposed multiplication algorithm, which is based on the Big-Digits representation, is faster than the classical, Karatsuba and the hybrid of Karatsuba-Classical multiplication algorithms in range of the public-key cryptography implementation.

Keywords: Public-key cryptography, Big-integer calculation, and Karatsuba multiplication algorithm.

Introduction

Number theory based public-key algorithms use multiplication extensively in their operations. Subsequently, many mathematicians and computer scientists have devoted their time in devising efficient multiplying algorithms for large numbers. The best known algorithmsfor multiplying big numbers in order of complexity are: Schoolbook or classical multiplication algorithm (Knuth 1997), Karatsuba multiplication algorithm (Karatsuba and Ofman 1963), Toom-Cook multiplication algorithm (Cook May 1966), Shönang-Strassenmultiplication algorithm (Schönhage and Strassen 1971), and Fürer(Fürer 2007) multiplication algorithm.Related work on big integer multiplication algorithms can also be found in the following literatures (Jedwab and Mitchell 1989; Montgomery 2005; Bodrato 2007; Hars 2007).

Classical Multiplication Algorithm

The usual method of multiplying two numbers in positional numeral system is recognized as classical multiplication algorithm (Knuth 1997)which can be stated as follows (see Algorithm 1):

Algorithm 1: Classical Multiplication CL (A,B)

Input: $A = (a_p \dots a_0)_b$

$$B = (b_q \dots b_0)_b$$

Output: $C = (C_{p+q} \dots, C_1 C_0)_b$

1. **for** $(i = 0; i \leq q; i{+}{+})$
2. **if** $(i \neq 0)$ do
3. **for** $(j = 0; j \leq p; j{+}{+})$
4. $TMP = C_{i+j} + (a_i \times b_j) + CRY$
5. $CRY = \lfloor TMP/b \rfloor$, $C_{i+j} = TMP \bmod b$
6. **return** C

There are two nested loops as shown in Steps 1 and 3 of Algorithm 1 to scan all q digits of the multipliers and p digits of the multiplicands. The value of TMP in Step 4,is computed by adding the value of $C_{i+j}$with the value of$CRY$and the result of multiplying the non-zero digit of the multipliers, a_i, (Step 2) with digitb_j from the multiplicand. The values of quotient and reminderareextracted from TMPafter divided by b, in Step 5 and are saved in c_{i+j} and CRY respectively. In this way, all the output digits from the least to the most significant are consecutively computed. The complexity of this algorithm is$O(n^2)$, which is slow for applications such as cryptography.

Karatsuba Multiplication Algorithm

Karatsuba multiplication algorithm (Karatsuba and Ofman 1962) with complexity $O(n^{1.58})$ is a suitable algorithm for multiplying numbers larger than few hundred digits long (Xianjin and Longshu 2007). This algorithm is performing based on two mechanisms; divide and conquer (Cormen, Leiserson et al. 2000; Levitin 2002; Mainzer 2007) and binary splitting (Brent 1976).

Equations 1 and 2 describe the multiplication operations, which the classical algorithm and Karatsuba algorithm are based on, respectively. The number of partial products in each iteration of the Karatsuba algorithm is three while the classical algorithmhas four, which gives Karatsuba algorithm the extra advantage in its calculation.

$$a \times b = (a_L \times b_L)r^{2n} + (a_R \times b_L + a_L \times b_R)r^n + (a_R \times b_R) \quad (1)$$

$$a \times b = (a_L \times b_L)r^{2n} + \{(a_R + a_L) \times (b_L + b_R) - (a_L \times b_L) - (a_R \times b_R)\}r^n + (a_R \times b_R) \quad (2)$$

Algorithm 2 shows the recursive Karatsuba multiplication algorithm in detail. When the length of the numbers that are being multiplied is1, the multiplication proses is a simple digit by digit multiplication (see Step 2). For numbers larger than 1 digit, the numbers are divided into a lower (a_R) and an upper half (a_L) as shown by Equation 3 before the algorithm is being call again recursively.The algorithm ends after $log_2 n$steps.

$$a = a_L \times r^{n/2} + a_R\,,\; b = b_L \times r^{n/2} + b_R \quad (3)$$

Algorithm 2: Karatsuba Multiplication C=KA (A,B)

Input: $A = (a_{n-1} \dots a_0)_r$
$B = (b_{n-1} \dots b_0)_r$

Output: KA (A,B)

1. **If** $n = 1$
2. **return** $A \times B$
3. **else**
4. $a_L = \left\lfloor \frac{a}{r^{n/2}} \right\rfloor$ *and* $a_R = a \bmod r^{n/2}$ // dividing a into two halves
   $b_L = \left\lfloor \frac{b}{r^{n/2}} \right\rfloor$ *and* $b_R = b \bmod r^{n/2}$ // dividing b into two halves
5. $k_0 = KA(a_L, b_L)$
6. $k_1 = KA(a_R, b_R)$
7. $k_2 = KA(a_R + a_L\,,\; b_R + a_L)$
8. **return** $k_0 \times r^n + (k_2 - k_1 - k_0) \times r^{n/2} + k_1$

Since Karatsuba multiplication algorithm run slower for numbers shorter than few hundred digits, some researchers (J. Von 2002)had proposed a hybrid approach where Karasubaalgorithm is combined with other multiplication methods. Another approach to improvethe performance of Karasubaalgorithm, is by splitting the numbers into more than 2 segments per iteration. Dan Zurasdescribed 3-way and 4-way variationsof the Karatsuba algorithm (Zura August 1994), and these studies was later extended by M. Sadiq and A. Jawed (Sadiq and Ahmed 2006) by splitting the numbers into 2-to-ten parts.Related work on Karatsuba algorithm can be found in these literatures (Montgomery 2005; Haining and Hasan 2007; Bernstein 2009).

Big-Digits Representation

ZOT representation (Jahani 2009) is a new representation for integers, which was derived from the binary numbering system. Symbols used in this representation are known as Big-Digits or in short "BD". The different patterns of "0" and "1" symbolsare the foundation of ZOT. These patterns are described as follows:

- Big-Zero: Asequence of symbol "0" is identified as Big-Zero or BZ. We represent a BZwith length of $n$as Z_n. For example, Z_3 = "000".

- Big-One: Asequence of symbol "1" is identified as Big-One or BO. We represent a BO with length of $n$asO_n. For example, O_7 = "1111111". The numerical value of each Big-One could be obtainedby $O_n = \sum_0^{n-1} 2^i$.
- Big-Two: A sequence of symbols "10" with extra symbol "1" at the right side of the sequence is called Big-Two or BT. We represent a BT with length of n as T_n. For example, T_5 = "10101". It is clear from the definition that the length of BT is always odd and its numerical value can be obtained from $T_n = \sum_0^{(n-1)/2} 4^i$.

Big-Digits is not a unique representation. For example, the binary number of "11111" could be represented by O_5, $O_4\,O_1$, $O_1\,O_4$or $O_3\,O_2$. ZOT representationlimits these varieties to only one representation. To convert a binary number to the ZOT representation the following rules must be considered.

- The direction of scanning a binary number to search for a new BD does not matter;however right-to-left is preferred.
- A valid BD in ZOT representation is a BD, which cannot be extendedwith any symbols, either tothe left or to the right of the BD. There is one exception; when a Big-One and a Big-Two are next to each other. In this situation the common "1" must belongs to BO.For example, the valid representation for "1111010101" is $O_4\,Z_1\,T_5$, not $O_3\,T_7$. More detail on ZOT representation can be found in (Jahani 2009).

For coding purposes ZOTis represented as shown by the following example:

$$\underbrace{11111}_{O_5}\,000\,\underbrace{1010101}_{T_7}\,000\,\underbrace{11111}_{O_5} = O_{(5,18)}\,T_{(7,8)}\,O_{(5,0)}$$

In above example, we can see all BZs disappeared and every non-zero BDs in the representation carry extra one more parameter. The parameters are the length and position of BD in its original binary form. In above example, $T_{(7,8)}$ means there is a BT with length 7 at position 8. This representation will prevent from double scanning of zeros while doing multiplication in ZOT representation.

Implementing Look-Up Table (LUT) in multiplication algorithm has its advantages(Hasan 2000; Mahboob and Ikram 2005; Wen-Ching, Jun-Hong et al. 2008).To benefit from this technique the ZOT representation is modified to form another variant of ZOT known as ZOT_x, where$x$ is the upper limit forthe maximum size of non-zero BDs in the representation. In this case, the size of the multiplication LUT will be limited to x^2.The procedure for obtaining ZOT_x representation is similar tothe process of obtaining the ZOT representation, except that the maximum length of BDs must belimited to $x$bits.The following exampleclarifies this concept. Let$x$=5, thenZOT_5 of "1111111000010101000111111"will be

$$ZOT_5(1111111000010101000111111) = O_{(2,23)}O_{(5,18)}\,T_{(5,9)}\,O_{(1,5)}O_{(5,0)}$$

Karatsuba Multiplication Algorithm withZOT_xRepresentation

TheZOT_xhas less non-zero digitsin its representation compared to its original binary representation.Hence, to multiply twoZOT_x numbers, less sub-multiplication operations is required. Classical multiplication algorithm, with some modification, can support the ZOT_x representation; as demonstrated by Algorithm 3.

The first modification is the conversion step, converting binary numbers a and$b$ toZOT_x representation a^* and b^* (see Steps 1 and 2). In these steps, all BDs such as a_n^*,will be denoted by three additional parameters; type denoted bya_{nt}^*, lengthdenoted by a_{nl}^*, and position of BD denoted bya_{np}^*.Theseconversions are actually the first overhead of the algorithm. The second modification is in Step 5.In this step, the function $BigDigitMultiplication(a_i^*, b_j^*)$fetches the result of binary multiplication of two Big-Digits a_i^*andb_j^* from a pre-calculated LUT. This value will be added todigit$c_{a_{ip}^*+b_{jp}^*}$,where$a_{ip}^* + b_{jp}^*$addresses theposition of thedigit. Note that, there is no "carry" from the previous calculation being calculated in Step 5. Therefore, the pre-defined memory for each digit of the output must be big enough to support the summation value in Step 5. The third modification is related to the format of the output. Based on to the memory specified for each digit, the base of the output can be defined. For example if we consider n bytes for each digits. The base of the output is2^n.

Algorithm 3: Classical ZOT_x Multiplication Algorithm

Input: $A = (a_{p-1} \ldots, a_1, a_0)_2$

$B = (b_{q-1} \ldots, b_1, b_0)_2$

Output: $C = CL - ZOT_x(A, B) = (c_{p+q} \ldots, c_2, c_1, c_0)_2$

1. $ZOT_x(A) = a^* = a^*_{p-1} \ldots, a^*_1, a^*_0$;where $a^*_n = (a^*_{nt}, a^*_{nl}, a^*_{np})$
2. $ZOT_x(B) = b^* = b^*_{q-1} \ldots, b^*_1, b^*_0$;where $b^*_n = (b^*_{nt}, b^*_{nl}, b^*_{np})$
3. **for** ($i = 0; i \leq p; i{+}{+}$)
4. **for** ($j = 0; j \leq q; j{+}{+}$)
5. $c_{a^*_{ip}+b^*_{jp}} = c_{a^*_{ip}+b^*_{jp}} + BigDigitMultiplication(a^*_i, b^*_j)$;
6. **return** C

Algorithm 4 shows the hybridof the Karatsuba algorithm with the Classical-ZOT_xmultiplication algorithm. The only difference between Algorithms 2 and 4 is in Step 1.In this step, when the sizes of the numbers reach the cut-off point value, theClassical-ZOT_xmultiplication algorithm will be used for the calculation.

Algorithm 4: Mixture of Karatsuba and Classical-ZOT_x Multiplication Algorithm

Input: $A = (a_{n-1} \ldots a_0)_r$

$B = (b_{n-1} \ldots b_0)_r$

Output: $KA - ZOT_x(A, B)$

1. **If**$n \leq$ cut_off point
2. **return**$(A \times B)_{Classical\_ZOTx}$
3. **else**
4. $a_L = \left\lfloor \frac{a}{r^{n/2}} \right\rfloor$ *and* $a_R = a \bmod r^{n/2}$ // dividing b into two halves

   $b_L = \left\lfloor \frac{b}{r^{n/2}} \right\rfloor$ *and* $b_R = b \bmod r^{n/2}$// dividing b into two halves
5. $k_0 = KA(a_L, b_L)$
6. $k_1 = KA(a_R, b_R)$
7. $k_2 = KA(a_R + a_L\,,\, b_R + a_R)$
8. **return** $k_0 \times r^n + (k_2 - k_1 - k_0) \times r^{n/2} + k_1$

In the following section,we compare the efficiency of the proposed multiplication algorithm with the existingclassical (CL), Karatsuba (KA) and hybrid of Karatsuba-Classical (KA-CL)multiplication algorithms in range of the public-key cryptography algorithms.

Results

According to (Jahani 2009), the Hamming weight for 32 bits to 32 Kbitsrandom numbers (Matsumoto and Nishimura 1998) is about 20% while the Hamming weight for binary number is 50%. Therefore, theoretically the execution time for classical and Classical-ZOT_x multiplication algorithm will be about$0.25n^2$and$0.04n^2$,respectively. Subsequently, the classical-ZOT_x multiplication algorithm should be about 6.25 times faster than the classicalmultiplication algorithm. Because of the overhead in converting the binary numbers to the ZOT_x representation andthe call to the function*BigDigitMultiplication*,the actual speed-up ratio is less than what is being speculated above. This paper investigates the effectiveness of combining the Karatsuba algorithm with the Classical-ZOT_x multiplication algorithm. Table 1 shows the measured execution time for each algorithm (CL, KA, KA-CL and KA-ZOT_x)within the range of 32 bits to 8 Kbits. The number of random numbers used for each test is 50 and the cut-off points were determined by experimenting with the KA-CL algorithm. The proposed algorithm was tested under the same conditionsas other algorithms with the same cut-off points. The machine specification used in the experiment is as follows: AMD Phenom (TM) 9950 Quad-core CPU 2.6 GHz, 3.25GB RAM, Windows XP Professional version 2002 (Service Pack 3) OS and Dev-C++ version 4.9.9.2 compiler.

Table 1 : Execution time (msec) of multiplication algorithms

Algorithm	Length of numbers (bits)								
	32	64	128	256	512	1024	2048	4096	8192
CL	0.007	0.023	0.083	0.344	1.27	4.9	19.2	76.9	308.5
KA	0.021	0.064	0.193	0.592	1.77	5.4	15.9	48.3	142.9
KA-CL	0.008	0.024	0.078	0.267	0.82	2.5	7.6	23.3	71.4
Proposed	0.005	0.010	0.020	0.094	0.28	1.4	4.1	13	33.3
Cut-off point	*16*	*32*	*64*	*32*	*32*	*16*	*16*	*16*	*16*

Table 1shows that thehybrids algorithms have a different cut-off points depending on the length of the number. The cut-off point value increases continuously againstthe length of numbers within the range of 32 to 128 bits.For numbers in the range of 1Kbits up to 8 Kbits, the cut-off point stable at 16 bits.

The results show that the performance of KA-ZOT_xmultiplication algorithm is better than CL, KA and KA-CL. The speed of KA-$ZOT_x$is about1.4 times faster than CL and increases to 9.2 times faster for 8 Kbits numbers. Comparing the execution speed between KA-$ZOT_x$and KA, tells us that KA-$ZOT_x$is about 4.2 times faster for 32 bits number and increases to about 4.3 times faster for 8 Kbits numbers,with some fluctuation in between. Figure 1 also indicates that KA-ZOT_x is relatively faster than KA-CL. KA-$ZOT_x$is about 1.6 times faster to 2.9 times faster for multiplying numbers in the range of 32 bits to 8Kbits.

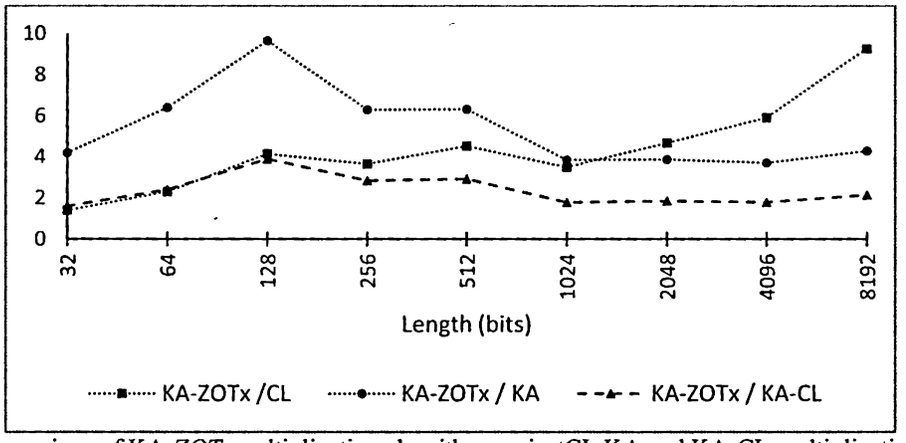


Figure 1 : Comparison of KA-ZOT_x multiplication algorithm againstCL,KA and KA-CL multiplication algorithms

Conclusion

In this paper, we proposed a new hybrid multiplication algorithm, combining the Karatsuba multiplication algorithmwith theZOT_x multiplication algorithm.The proposedKaratsuba-ZOT_xout-performs all other tested algorithms. The result indicated that Karatsuba-ZOT_x algorithm is about 1.6 (for 32 bits numbers) to 2.9 times faster (for 8192 bits numbers) against the best existing Karatsuba-Classical algorithm. The finding from this paper indicates that the proposed algorithm is currently the most suitable multiplication algorithm for the use in existing public-key cryptosystems.

Acknowledgement

The researchers would like to thank the Universiti Sains Malaysia for supporting this research (Project grant: 1001/PKOMP/817059).

References:

Bernstein, D. J. (2009). Batch Binary Edwards. Advances in Cryptology - Crypto 2009. *S. Halevi*. Berlin, Springer-Verlag Berlin. 5677: 317-336.

Bodrato, M. (2007). Towards Optimal Toom-Cook Multiplication for Univariate and Multivariate Polynomials in Characteristic 2 and 0. Proceedings of the 1st international workshop on Arithmetic of Finite Fields. Madrid, Spain, Springer-Verlag.

Cook, S. A. (May 1966). On the Minimum Computation Time of Functions. Mathematics, Harvard University. Ph.D. Thesis, Department of Mathematics.

Fürer, M. (2007). Faster integer multiplication. Proceedings of the thirty-ninth annual ACM symposium on Theory of computing. San Diego, California, USA, ACM.

Haining, F. and A. Hasan (2007). "Comments on "Five, Six, and Seven-Term Karatsuba-Like Formulae'." *Computers, IEEE Transactions on* 56(5): 716-717.

Hars, L. (2007). "Applications of fast truncated multiplication in cryptography." *EURASIP J. Embedded Syst.* 2007(1): 3-3.

Hasan, M. A. (2000). "Look-up table-based large finite field multiplication in memory constrained cryptosystems." *Computers, IEEE Transactions on* 49(7): 749-758.

J. Von, J. S. (2002). Fast Arithmetic for Polynomials Over F2 in Hardware. In Proc. IEEE Information Theory Workshop.

Jahani, S. (2009). ZOT-M_K: A New Algorithm for Big Integer Multiplication. Department of Computer Science. Penang, Universiti Sains Malaysia. Msc. Thesis.

Jedwab, J. and C. J. Mitchell (1989). "Minimum weight modified signed-digit representations and fast exponentiation." *Electronics Letters* 25(17): 1171-1172.

Karatsuba, A. and Y. Ofman (1962). Multiplication of Many-Digital Numbers by Automatic Computers. Proceedings of the USSR Academy of Sciences. 145: 293-294.

Karatsuba, A. and Y. Ofman (1963). "Multiplication of Multidigit Numbers on Automata." *Soviet Physics Doklady (English translation)* 7(7): 595-596.

Knuth, E. (1997). The Art of Computer Programming, Addison-Wesley.

Mahboob, A. and N. Ikram (2005). "Lookup table based multiplication technique for GF(2(m)) with cryptographic significance." *IEE Proceedings-Communications* 152(6): 965-974.

Montgomery, P. L. (2005). "Five, six, and seven-term Karatsuba-like formulae." *Computers, IEEE Transactions on* 54(3): 362-369.

Sadiq, M. and J. Ahmed (2006). "Complexity Analysis of Multiplication of Long Integers." *Asian Jurnal of Information Technology* 5(2).

Schönhage, A. and V. Strassen (1971). "Schnelle Multiplikation großer Zahlen." *Computing in Science & Engineering* 7 139-144.

Wen-Ching, L., C. Jun-Hong, et al. (2008). A new look-up table-based multiplier/squarer design for cryptosystems over GF(2^m). *Circuits and Systems, 2008. ISCAS 2008. IEEE International Symposium on.*

Xianjin, F. and L. Longshu (2007). On Karatsuba Multiplication Algorithm. *Data, Privacy, and E-Commerce, 2007. ISDPE 2007. The First International Symposium on.*

NEW METHOD FOR SPEEDING UP THE CHEBYSHEV POLYNOMIAL CALCULATION FOR CRYPTOGRAPHIC PURPOSES

Mohammed Benasser Algehawi, AzmanSamsudin and Shahram Jahani
School of Computer Sciences, Universiti Sains Malaysia, 11800 Penang, Malaysia
malgehawi@yahoo.com, azman@cs.usm.my, jahani2001@yahoo.com

Abstract:

It has been recommended that the safe size of the key space for any cryptosystem based on Chebyshev polynomial extended over the finite field $\mathbb{Z}_p$ must be chosen such that $p \geq 2^{256}$. For this big size of p, the calculation of Chebyshev polynomial will be very slow and impractical. Thus, there is a need to find solutions for this issue so thatChebyshev based algorithmsare secure and at the same time practical. In this paper, we worked with two types of algorithms: the Matrix algorithm and the Characteristic polynomial algorithm. We have proposed new ideas in order to improve the Chebyshev polynomial calculations by enhancing these algorithms. Our results show some improvement compared to the original algorithms. The performance comparison was done on the original algorithms for calculating Chebyshev polynomial by Fee & M. B. Monagan, the improved versions by Li et al. and our proposed algorithms. Results show indications that the proposed method is a reliable alternative for implementing Chebyshev polynomial calculation.

Keywords: Public-key cryptography, Chebyshev polynomial, and Chaos cryptography.

Introduction

Many cryptosystems have been proposed based on Chebyshev polynomial(Algehawi & Samsudin 2010; Wang & Zhao 2010; Xiao et al. 2007; Yoon & Yoo 2008). The common issue among these cryptosystems is the security against attacks, such as brute force attack and period distribution attack. Consider the extended Chebyshev polynomial over the finite field $\mathbb{Z}_p$ as follows:

$$T_n(x) = (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x^1 + a_0)\ (mod p) \qquad (1)$$

To avoid attacks on cryptosystems based on Chebyshev polynomial extended over the finite field $\mathbb{Z}_p$, the value of p must be chosen very large such that p is considered as strong prime, or what is called a safe prime. At the same time the value of n should be large enough such that large period can be obtained. As claimed by many researchers (Liao et al. 2010; Li et al. 2011; Fee & Monagan 2004), a strong prime $p$means that both $p+1$ and $p-1$ have a large factors e.g., greater that 2^{256}.For this big size of p, the calculation of Chebyshev polynomial will be very slow and impractical. Thus, there is a need to find solutions for this issue so thatcryptosystems based on this polynomialare secure and at the same time practical.There are numerous solutions that have been proposed in many places in order to enhance the computational speed of the Chebyshev polynomial extended over the finite field $\mathbb{Z}_p$.

In this paper, we worked with two types of algorithms; the Matrix algorithm (MA) and the Characteristic polynomial algorithm (CPA)(Fee & Monagan 2004). These two algorithms have been improved by Li et al. in 2011 and they named the improved versions of the algorithm as the Modified Matrix algorithm (MMA) and the Modified Characteristic polynomial algorithm (MCPA). In the following sections, a brief explanation of MA, MMA, CPA, and MCPA algorithms are given.

Matrix Algorithm (MA) (Fee & Monagan 2004)

The first matrix algorithm to calculate the Chebyshev polynomial $T_n(x)$ was proposed by Fee and M. B. Monagan (2004). By considering Equation 1, this algorithm can be explained as follows(Li et al. 2011):

Input: n, A, I
$If\ n = 0\ \ then\ \ return\ 1$
$Else\ \ if\ \ n > 0$
$C \leftarrow I, S \leftarrow A$// C represents the immediate result in the process
$For\ i = 0\ up\ to\ r-1\ by\ 1$// S element holds the result of squaring the matrix A
$If\ b_i = 1\ then\ C \leftarrow C \times S$ // C_{11} and C_{12} are elements of$C$.
$S \leftarrow S \times S$

Output: $C_{11} + xC_{12}$

Inmatrix algorithm (MA), the users used the square and multiply method to calculate $C = A^n$. At each step i of the loop, the exponent$n = \sum_{j=0}^{r-1} b_j 2^j$, $S = A^{2(i+1)}$. At the end of the same loop $S = A^{2r}$. First, the exponent n, matrix A, and the matrix I will be inputted. If the value of n is 0 then the program will return 1 as a result, else C will be initialized with the identity matrix I and S will be initialized with the matrix A such that at each step of the loop if $b_j = 1$ then C is calculated as $C = C \times S$.

Assume m representing the number of the 1's in the binary representation of the exponent n of the matrix A. Then, the squaring $(S \times S)$ is performed in each loop step while the multiplication $(C \times S)$ is performed only $m + 1$ times with the first multiplication $A \times I$ where its running time is negligible. The binary digits of the exponent $n$are checked one by one in right to left order.To calculate the running cost of the MA, the following matrix operations should be considered:

Matrix	Running Cost
$C \times S = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix}\begin{pmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{pmatrix} = \begin{pmatrix} C_{11}S_{11} + C_{12}S_{21} & C_{11}S_{12} + C_{12}S_{22} \\ C_{21}S_{11} + C_{22}S_{21} & C_{21}S_{12} + C_{22}S_{22} \end{pmatrix}$	$8t_m + 4t_a$
$C \times C = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix}\begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix} = \begin{pmatrix} {C_{11}}^2 + C_{12}C_{21} & C_{12}(C_{11} + C_{22}) \\ C_{21}(C_{11} + C_{22}) & C_{21}C_{12} + {C_{22}}^2 \end{pmatrix}$	$3t_m + 2t_s + 3t_a$
$A \times C = C \times A = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 2x \end{pmatrix} = \begin{pmatrix} -C_{12} & C_{11} + 2xC_{12} \\ -C_{22} & C_{21} + 2xC_{22} \end{pmatrix}$	$2t_m + 2t_a$

Accordingly, the computation time of MA can be illustrated as the follows:

$$T_{MA} = (r-1)(3t_m + 2t_s + 3t_a) + m(8t_m + 4t_a) + 3(t_m + t_a) \quad (2)$$

From Equation 2, r is the number of all the bits in the exponent n, t_m is the multiplication time, t_s is the squaring time,t_a is the summation time, and m is the number of 1's in the exponent n.

Characteristic Polynomial Algorithm (CPA)(Fee & Monagan 2004)

The first Characteristic Polynomial Algorithm (CPA) to calculate the Chebyshev polynomial $T_n(x)$ was presented by Fee and M. B. Monagan (2004). Based on Cayley-Hamilton theory, the matrix satisfies its own characteristic polynomial, i.e. if the characteristic polynomial of a square matrix A is $f(\lambda) = det\ (\lambda I - A)$ then $f(A) = 0$ where det is the determinant operation and I is the identity matrix. More precisely, since that the entries of the matrix are (constant) polynomials in λ, the determinant is also a polynomial in λ. The Cayley–Hamilton theorem states that substituting the matrix A for λ in this polynomial result in the zero $f(A) = 0$. Thus, instead of calculating A^n we just calculate λ^n modulo the characteristic polynomial using the square and multiply method. The characteristic polynomial is a quadratic polynomial and can be expressed as, $f(\lambda) = a_1\lambda + a_0$ where the nth power of the matrix A have the form $a_1A + a_0$ such that $T_n(x)$ can be expressed as (Li et al. 2011):

$$T_n(x) mod\ p = A^n \begin{pmatrix} T_0(x) \\ T_1(x) \end{pmatrix} mod\ p = (a_1A + a_0)\begin{pmatrix} 1 \\ x \end{pmatrix} mod\ p = (a_1x + a_0)\ mod p \quad (3)$$

By using Equation 3, $T_n(x)$can be calculated as follows:

Input: n, A, I
$If\ n = 0\ \ then\ \ return\ 1$
$Else\ \ if\ \ n > 0$
$a_1\lambda + a_0 \leftarrow I, s_1\lambda + s_0 \leftarrow A$
$For\ i = 0\ up\ to\ r - 1\ by\ 1$
  $If\ b_i = 1\ then$
$$a_1\lambda + a_0 \leftarrow (a_1\lambda + a_0) \times (s_1\lambda + s_0)$$

$s_1\lambda + s_0 \leftarrow (s_1\lambda + s_0) \times (s_1\lambda + s_0)//(s_1\lambda + s_0) \times (s_1\lambda + s_0)$ uses squaring operation
$a_1\lambda + a_0 \leftarrow (a_1\lambda + a_0) \times (s_1\lambda + s_0)//(a_1\lambda + a_0) \times (s_1\lambda + s_0)$usesmultiplication operation
Output: $a_1x + a_0$

To calculate the running cost of the CPA, the following basic operations should be considered:

CPA Equation	Running Cost
$(a_1\lambda + a_0) \times (s_1\lambda + s_0) = (2xs_1a_0 + s_1a_0 + s_0a_1)\lambda + (s_0a_0 - s_1a_1)$	$5t_m + 3t_a$
$(s_1\lambda + s_0) \times (s_1\lambda + s_0) = (2xs_1{}^2 + 2s_1s_0)\lambda + (s_0{}^2 + s_1{}^2)$	$2t_m + 2t_s + 3t_a$
$\lambda(s_1\lambda + s_0) = (2xs_1 + s_0)\lambda - s_1$	$t_m + t_a$

Accordingly, from the CPA above, the running time of the CPA can be calculated as the follows:

$$T_{CPA} = (r-1)(2t_m + 2t_s + 3t_a) + (m-1)(5t_m + 3t_a) + 2(t_m + t_a) \quad (4)$$

The Running Time of the Modified Matrix Algorithm (MMA) and the Modified Characteristic Polynomial Algorithm (MCPA)(Li et al. 2011)

The running time of the Modified Matrix algorithm MMA can be calculated as the follows:

$$T_{MMA} = (r-1)(3t_m + 2t_s + 3t_a) + m(2t_m + 2t_a) + (t_m + t_a) \quad (5)$$

The running time of the Modified Characteristic Polynomial algorithm MCPA can be calculated as the follows:

$$\begin{aligned} T_{MCPA} &= (r-1)(2t_m + 2t_s + 3t_a) + (m-1)(t_m + t_a) + (t_m + t_a) \\ &= (r-1)(2t_m + 2t_s + 3t_a) + m(t_m + t_a) \end{aligned} \quad (6)$$

The New Matrix Algorithm Based on Look-up Table (LMA)

Following is our proposed method, which utilizes look-up table while executing the MA. The bits representing the exponent n is checked in reverse order (right-to-left) with step of b bits. The flag will be set to false to avoid the squaring $C \leftarrow C \times C$ at the start of the algorithm. Consequently, after setting the flag to true there will be b squaring in each loop. In each loop, the result of the look-up table will be multiplied with the previous result which stored previous value in C such that $C \leftarrow C \times LUT$. The look-up table LUT contains the result of the different operations according to binary digits of the current three bits of the exponent n. More precisely, the look-up table contains the operations done on the matrix A according to the binary representation of its power such that the power of the matrix $A$is divided into b bits. Suppose that size of b is 3 bits, then the look-up table will be made for the numbers from 0 to 7. The whole LMA algorithm with the construction of the look-up table can be described as follows:

//Look-up table creation
$a[b_0]$: Do nothing, $a[b_1]$: Return A, $a[b_2]$: Return $A^2 = A \times A$,
$a[b_3]$: Return $A^3 = A^2 \times A$, $a[b_4]$: Return $A^4 = A^3 \times A$, $a[b_5]$: Return $A^5 = A^4 \times A$,
$a[b_6]$: Return $A^6 = A^5 \times A$, $a[b_7]$: Return $A^7 = A^6 \times A$,
Input:$n, A, I, b = 3$
$Flag = false$
$C \leftarrow I$
$For\ i = r\ up\ to\ 0\ by - 3$
  $If\ flag = true\ then$
    $For\ j = 0\ up\ to\ 3 - 1\ by + 1$ // (Shift three bits)
$C \leftarrow C \times C$
$Flag = true$
$C \leftarrow C \times a[b_k]$ //(multiplying the results with returned value //from the Look-up table //$a[b_k]$ where k from 0-to-7)

Output:$xC_{11} + C_{12}$

The overall running time of LMA can be calculated as follows:

$$T_{LMA} = (r-1)(2t_m + 2t_s + 3t_a) + \frac{r-1}{b}(8t_m + 4t_a) + (t_m + t_a) + T_{LUT} \quad (7)$$

The New Characteristic Polynomial Algorithm Based on Look-up Table (LCPA)

The proposed LCPA drew the results of each loop computation from a pre calculated look-up table. The bits representation of the exponent $n$is checked in reverse order (left-to-right) with step of b bits. First, consider the following LPCA pseudocode:

//Look-up table creation
$a[b_0]$: Do nothing, $a[b_1]$: Return $(S_1\lambda + S_0)$, $a[b_2]$: Return $(S_1\lambda + S_0) \times \lambda$,
$a[b_3]$: Return $(S_1\lambda^2 + S_0) \times \lambda$, $a[b_4]$: Return $(S_1\lambda^3 + S_0) \times \lambda$, $a[b_5]$: Return $(S_1\lambda^4 + S_0) \times \lambda$,
$a[b_6]$: Return $(S_1\lambda^5 + S_0) \times \lambda$, $a[b_7]$: Return $(S_1\lambda^6 + S_0) \times \lambda$
Input:n, A, I, b
$Flag = false$
$S_1\lambda + S_0 \leftarrow I$
$For\ i = r\ up\ to\ 0\ by - b$
$If\ flag = true\ then$
$For\ j = 0\ up\ to\ b - 1\ by + 1$
$S_1\lambda + S_0 \leftarrow (S_1\lambda + S_0) \times (S_1\lambda + S_0)$
$Flag = true$
$S_1\lambda + S_0 \leftarrow (S_1\lambda + S_0) \times a[b_k]$ //(multiplying the results with returned value from the //Look-up table $a[b_k]$ where k from 0-to-7)
Output:$xS_1 + S_0$

The look-up table accessing time is relatively small and therefore can be neglected. Thus, with such assumption the running time of the LCPA can be calculated as follows:

$$T_{LCPA} = (r-1)(2t_m + 2t_s + 3t_a) + \frac{r-1}{b}(5t_m + 3t_a) + T_{LUT} \quad (8)$$

Analysis of the Proposed Algorithms

Recall Equation 2, Equation 5, and Equation 7, the new LMA can be compared to the MA theoretically as the following:

$$\begin{aligned} T_{MA} - T_{LMA} &= \left((r-1)(3t_m + 2t_s + 3t_a) + m(8t_m + 4t_a) + 3(t_m + t_a)\right) \\ &\quad - \left((r-1)(3t_m + 2t_s + 3t_a) + \frac{r-1}{b}(8t_m + 4t_a) \right. \\ &\quad \left. + (t_m + t_a) + T_{LUT}\right) \\ &= \left(m(8t_m + 4t_a) + 3(t_m + t_a)\right) \\ &\quad - \left(\tfrac{r-1}{b}(8t_m + 4t_a) + (t_m + t_a) + 2^b(2t_m + 2t_a)\right). \end{aligned}$$

Similarly, in the case of the MMA and LMA, the comparison is as follows:

$$\begin{aligned} T_{LMA} - T_{MMA} &= \left((r-1)(3t_m + 2t_s + 3t_a) + \frac{r-1}{b}(8t_m + 4t_a) + \right. \\ &\quad \left. (t_m + t_a) + 2^b(2t_m + 2t_a)\right) \\ &\quad -\left((r-1)(3t_m + 2t_s + 3t_a) + m(2t_m + 2t_a) + (t_m + t_a)\right) \end{aligned}$$

$$= \left(\frac{r-1}{b}(8t_m + 4t_a) + (t_m + t_a) + 2^b(2t_m + 2t_a)\right) - \left(m(2t_m + 2t_a) + (t_m + t_a)\right)$$

Figure 1, shows a theoretical comparison among LMA, MA, and MMA considering that the number of 1's in the exponent is always 50%. LMA is tested with $b = 7$. The comparison has shown that LMA has the less number of operations compared to the MA and very close to MMA with preference for MMA on LMA.

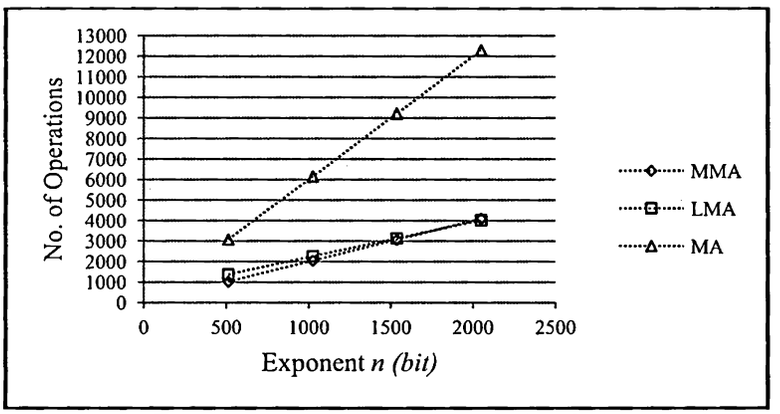


Figure 1 : Theoretical comparison between MA, MMA, and LMA

From Equation 4, Equation 6, and Equation 8, the different in the cost between CPA, MCPA, and LCPA can explained as the following. In the case of the CPA against LCPA, the theoretical comparison is as follows:

$$T_{CPA} - T_{LCPA} = \left((r-1)(2t_m + 2t_s + 3t_a) + (m)(5t_m + 3t_a) + 2(t_m + t_a)\right) - \left(\begin{matrix}(r-1)(2t_m + 2t_s + 3t_a) + \\ \frac{r-1}{b}(5t_m + 3t_a) + (t_m + t_a) + T_{LUT}\end{matrix}\right)$$
$$= \left((m-1)(5t_m + 3t_a) + 2(t_m + t_a)\right) - \left(\frac{r-1}{b}(5t_m + 3t_a) + (t_m + t_a) + 2^b(t_m + t_a)\right)$$

Similarly, in the case of the MCPA and LCPA, the theoretical comparison is as follows:

$$T_{LCPA} - T_{MCPA} = \left(\begin{matrix}(r-1)(2t_m + 2t_s + 3t_a) + \frac{r-1}{b}(5t_m + 3t_a) \\ +(t_m + t_a) + T_{LUT}\end{matrix}\right) - \left((r-1)(2t_m + 2t_s + 3t_a) + (m-1)(t_m + t_a) + (t_m + t_a)\right)$$
$$= \left(\frac{r-1}{b}(5t_m + 3t_a) + 2^b(t_m + t_a)\right) - \left((m-1)(t_m + t_a)\right)$$

Thus, the LCPA is costing extra 541 multiplications and 135 additions than the MCPA.

Figure 2, shows a theoretical comparison among LCPA, CPA, and MCPA considering that the number of 1's in the exponent is always 50%. LCPA is tested with $b = 7$. The comparison showed that LCPA has less number of operations compared to the CPA and very close to MCPA with preference for MCPA over LCPA.

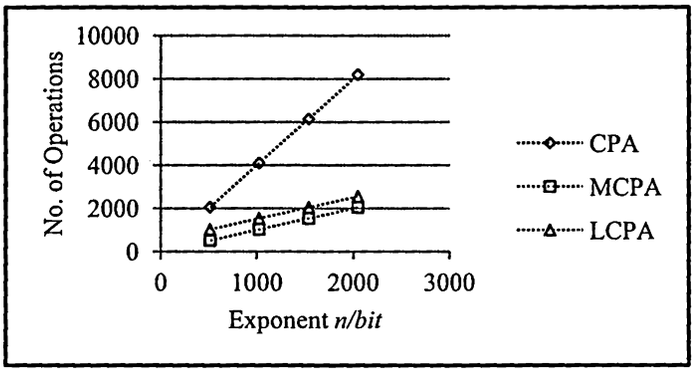


Figure 2 : Theoretical comparison between CPA, MCPA, and LCPA

Conclusion

In this paper, we have presented the most common algorithms that have been used for the calculation of the extended Chebyshev polynomial over the finite fields. These algorithms are the MA, MMA, CPA, and MCPA. Also, we have proposed new improvement on the MA and CPA by using the look-up tables. The results have shown good improvement over the MA and CPA but not over the MMA and MCPA.

References:

Algehawi, M.B. & Samsudin, A., 2010. A new Identity Based Encryption (IBE) Scheme using Extended Chebyshev Polynomial Over the Finite Fields Zp. Physics Letters A, 374, p.4670-4674.

Fee, G.J. &Monagan, M.B., 2004. Cryptography using Chebyshev Polynomials. In Proceedings of the Maple Summer Workshop MSW'04. Burnaby, Canada, pp. 1-15.

Li, Z.-hui, Cui, Y.-dong & Xu, H.-min, 2011. Fast Algorithms of Public Key Cryptosystem Based on Chebyshev Polynomials Over Finite Field. The Journal of China Universities of Posts and Telecommunications, 18(2), p.86-93. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1005888510600490 [Accessed October 12, 2011].

Liao, X., Chen, F. & Wong, K.-wo, 2010. On the Security of Public-Key Algorithms Based on Chebyshev Polynomials over the Finite Field Z_N. IEEE Transactions on Computers, 59(10), p.1392-1401. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5487511.

Wang, X. & Zhao, J., 2010. An Improved Key Agreement Protocol Based on Chaos. Communications in Nonlinear Science and Numerical Simulation, 15, p.4052-4057.

Xiao, D., Liao, X. & Deng, S., 2007. A novel Key Agreement Protocol Based on Chaotic Maps. Information Sciences, 177, p.1136-1142.

Yoon, E.-jun & Yoo, K.-young, 2008. A New Key Agreement Protocol Based on Chaotic Maps. In Agent and Multi-Agent Systems: Technologies and Applications - KESAMSTA. Berlin, Heidelberg: Springer-Verlag, pp. 897-906.

POINT COUNTING ALGORITHMS FOR GENUS 2 HYPERELLIPTIC CURVES

Liew Khang Jie and Hailiza Kamarulhaili
School of Mathematical Sciences, Universiti Sains Malaysia
kenji_liewkj@yahoo.com.my, hailiza@cs.usm.my

Abstract:

Hyperelliptic curves were proposed by Neal Koblitz in 1989 as an alternative for the elliptic curves. As for elliptic curves, it is another discrete logarithm based cryptosystem and therefore one can say that the hyperelliptic curve cryptosystem is the generalization of elliptic curve cryptosystem. For cryptographic purposes, lower genus curves are considered secure compared with higher genus curves. In order to implement, the order of the Jacobian of the hyperelliptic curve and its twisted curve must be prime or almost prime. So, in this paper, we are going to discuss the elementary arithmetic and the group laws of hyperelliptic curve or specifically the imaginary hyperelliptic curve. In addition, we also carry outsome surveys on the developmentand enhancement of Gaudry-Harleypoint counting algorithm of genus 2 hyperelliptic curves over prime fields.

Introduction

Victor Miller (Miller, 1986) and Neal Koblitz (Koblitz, 1987) had independently proposed the elliptic curve cryptosystem in 1985. Four years later, Koblitz (Koblitz, 1989) proposed another cryptosystem namely hyperelliptic curve cryptosystem which is a generalization of the elliptic curve cryptosystem. Koblitz investigated the Jacobian of hyperelliptic curve defined over finite field. Abelian group is said to be the most suitable for cryptographic purposes. For implementation, one consider only for hyperelliptic curve which has genus, g less than four(Pelzl, Wollinger, Guajardo, & Paar, 2003). As for curve with genus larger than four, it may potentially insecure. The hyperelliptic curve with lower genus is efficient due to its group laws and arithmetic are well known and also the absence of sub exponential-time algorithms such as index-calculus method(Jacobson Jr, Menezes, & Stein, 2004). Therefore, elliptic curve and hyperelliptic curve of genus two receive most attention from cryptographers and researchers. Furthermore, genus 2 hyperelliptic curves now can compete with the elliptic curve cryptosystem in terms of speed. Besides having their application in public key cryptosystem, it also used in algorithm of primality proving, designing of error-correcting code and integer factorization algorithm(Menezes, Zuccherato, & Wu, 1996).In addition, the hyperelliptic curve can be divided into two types, namely imaginary and real form. In this paper, we focus on the model that proposed by Koblitz which was imaginary hyperelliptic curve.

Besides, to ensure the security of the implementation, the group order must have large prime order or almost prime (Gaudry & Schost, 2004). This is because to avoid being attacked by Pohlig Hellman method or make this attack takes an unrealistic time (Menezes, et al., 1996).To get a good compromise between security and efficiency, the base field should be large enough with order 2^{80} which is barely adequate security and 2^{128} is considered safe. An example on prime field, $F_p$is $p = 2^{127} - 1$ with $\#J_C(F_p) = 2^{254}$ elements and the prime p is the Mersenne prime so that reduction modulo p can be done very fast compared with generic prime of the same size.

Based on these conditions, the interest curves can be constructed using point counting algorithm or complex multiplication method. For complex multiplication method, the curve is constructed based on the desired Jacobian order. Due to the efficiency considerations, point counting method is preferable. The hyperellipticcurves are randomly generated and theirgroup orders are computed. The curves which are not prime order are eliminated using early abort strategy.In this paper, we survey and describe the developments of the practical pointing counting of genus 2 that is Gaudry - Harley algorithm besides the elementary arithmetic of genus 2 imaginary hyperelliptic curve.

Hyperelliptic Curves

Definition 1: Let K be a field and let $\overline{K}$ be the algebraic closure of K. The equation of a non-singular imaginary quadratic hyperelliptic curve, C of genus, g such that $g \geq 2$ over K is in the form (Menezes, et al., 1996):

$$C: v^2 + h(u)v = f(u)$$

where $h(u)$ and $f(u) \in K[u]$ with degree of $h(u)$, $\deg(h(u)) \leq g$ and $f(u)$ is a monic polynomial with degree, $\deg(f(u)) = 2g+1$. There are no solutions $(u,v) \in \overline{K} \times \overline{K}$ simultaneously satisfied the equation $v^2 + h(u)v = f(u)$

and also both of the partial derivative equations $2v+h(u)=0$ and $h'(u)v-f'(u)=0$ to ensure no singular points exist.

Definition 2: The set of $\bar{K}$ - Weiestrass points on C is denoted as

$$C(\bar{K}) = \{(x,y) \in \bar{K} \times \bar{K} \mid y^2 + h(x)y = f(x)\} \cup \{\infty\}$$

The point ∞ is called point at infinity that satisfies the homogenized equation. For $P = (x, y) \in C(\bar{K})$, the opposite of P is $\tilde{P} = (x, -y - h(x)) \in C(\bar{K})$, also $\tilde{\infty} = \infty$. In (Blake, Seroussi, & Smart, 2005) the opposite of P is called the hyperelliptic involution, denoted as ι. The points other than ∞ are called finite points. If $P = \tilde{P}$, then the point is special, else it is ordinary.

Lemma 1: Let C be a hyperelliptic curve over K defined above(Menezes, et al., 1996).

(i) If $h(u) = 0$, thencharacteristic K, char $(K) \neq 2$.

(ii) For char $(K) \neq 2$, the transformation of variables $u \rightarrow u$, $v \rightarrow (v - h(u)/2)$ to the form of $v^2 = f(u)$, deg $f = 2g + 1$

(iii) If char $(K) \neq 2$, $h(u) = 0$, then C is a hyperelliptic curve if and only if $f(u)$ has distinct roots in $\bar{K}$.

We are going to show graphical representation on several examples of hyperelliptic curve of genus two defined over real field, $\mathbb{R}$.

Example 1*:* A hyperelliptic curve with genus 2 defined over real field with equation

$$v^2 + u^2v + 5uv + 2v = u^5 + 4u^4 + 2u^3 + 8u^2 + 3u + 20$$

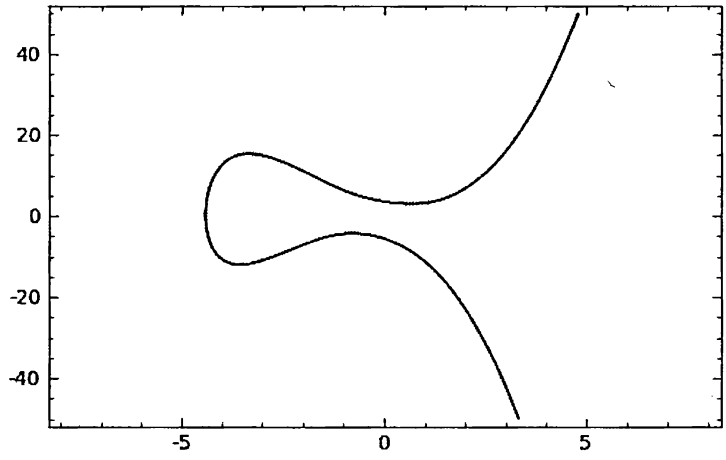


Figure 1 : C: $v^2 + (u^2 + 5u + 2)\, v = u^5 + 4u^4 + 2u^3 + 8u^{2+} 3u + 20$ over $\mathbb{R}$

Example 2:A hyperelliptic curve with genus 2 defined over real field,$\mathbb{R}$ with equation

$$v^2 = u^5 - 11u^3 + 15u$$

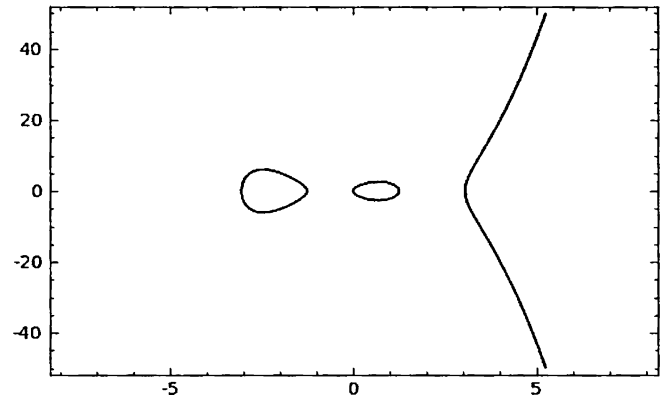


Figure 2 : C: $v^2 = u^5 - 11u^3 + 15u$ over $\mathbb{R}$

Group Law for Hyperelliptic Curves

For hyperelliptic curves of genus greater or equal to 2, there is no natural group law on $C(\bar{K})$ like elliptic curves.For genus greater than 1, we no longer can use the chord and tangent method from elliptic curves as a line intersects in five instead of three points. Therefore, the group actually is the quotient group of finite sums of points on the curve by all sums of points that lie on a function (Cohen et al., 2006).A group law of hyperelliptic curve is defined such is known as the Jacobian of C over K which is a finite Abelian group.It isgeneralization of the group points on an elliptic curve.

To understand the concept of Jacobian, J_C, we need to know the following definition which based on (Menezes, et al., 1996). Again, let Cbe an imaginary quadratic non-singular hyperelliptic curve.

Definition 5: Coordinate ring of C over $\bar{K}$, denoted $\bar{K}[C]$, is the quotient ring

$$\bar{K}[C] = \bar{K}[u, v] / (v^2 + h(u)v - f(u))$$

where $v^2 + h(u)v - f(u)$ denotes the ideal in $\bar{K}[u,v]$ generated by the polynomial $v^2 + h(u)v - f(u)$. An element of $\bar{K}[C]$ is called a polynomial function on C.

Lemma 2: The polynomial $r(u, v) = v^2 + h(u)v - f(u)$ is irreducible over $\bar{K}$ and hence $\bar{K}[C]$ is an integral domain.

Definition 3: The function field $\bar{K}(C)$ over $\bar{K}$ is the field of fractions of $\bar{K}[C]$. The elements in $\bar{K}(C)$ are called rational functions on C. Note that $\bar{K}$ [C] is the subring of $\bar{K}(C)$ that is every polynomial function is also a rational function.

Definition 4: Let $R \in \bar{K}(C)$ and let $P \in C$, $P \neq \infty$. Then R is said to be defined at P if there exist polynomial functions $G, H \in \bar{K}[C]$ such that $R = G/H$ and $H(P) \neq 0$; if no such $G, H \in \bar{K}[C]$ exist, then R is not defined at P. If R is defined at P, the value of R at P is defined to be $R(P) = G(P) / H(P)$.

Definition 5: A divisor D is a formal sum of points in C

$$D = \sum_{P \in C} m_P P, \; m_p \in \mathbb{Z}$$

where only a finite number of the m_P are non-zero.

Definition 6: The degree (or weight) of D, denoted as deg D is the integer $\sum_{P \in C} m_P$.

The order of D at P is the integer m_P, written as $\text{ord}_P(D) = m_P$. The set of all divisors denotes as D, forms an additive group under the addition rule:

$$D = \sum_{P \in C} m_P P + \sum_{P \in C} n_P P = \sum_{P \in C} (m_P + n_P) P$$

The set of all divisors of degree 0, denoted D^0, is a subgroup of D.

Definition 7: Let $D_1 = \sum_{P \in C} m_P P$ and $D_2 = \sum_{P \in C} n_P P$ be two divisors, the greatest common divisor of D_1 and D_2 is defined to begcd$(D_1, D_2) = \sum_{P \in C} \min(m_P, n_P)P - \left(\sum_{P \in C} \min(m_P, n_P)\right)\infty$. Note thatgcd$(D_1, D_2) \in D^0$.

Definition 8: Let $R \in \bar{K}(C)^*$. The divisor of R is $div(R) = \sum (ord_P R)P$. The divisor of rational function is indeed a finite formal sum and has degree of 0.

Definition 9: A divisor $D \in D^0$ is called a principal divisor if D = div(R) for some rational function $R \in \bar{K}(C)^*$. The set of all principal divisors denoted as *Princ* is a subgroup of D^0.

Definition 10: Jacobian of the curve C is the quotient group denoted as $J_C = D^0 / Princ$. If $D_1, D_2 \in D^0$, then $D_1 \sim D_2$ if $D_1 - D_2 \in Princ$; $D_1$and $D_2$are said to be equivalent divisors.

Definition 11: Let $D = \sum_{P \in C} m_P P$ be a divisor. The support of D is the set supp $(D) = \{P \in C \mid m_P \neq 0\}$.

Definition 12: A divisor D is said to be defined over K if $D^\sigma = \sum_{P \in C} m_P P^\sigma = D$ for all automorphisms σ of $\bar{K}$ over K where $P^\sigma = (\sigma(x), \sigma(y))$ if $P = (x, y)$ and $\infty^\sigma = \infty$. Note that $P_i^\sigma = P_i$ does not imply they are the same, σ may permute the points.

Definition 13: A semi-reduced divisor is a divisor of the form $D = \sum m_i P_i - (\sum m_i)\infty$, where each $m_i \geq 0$ and the P_i's are the finite points such that when $P_i \in$ supp(D) then $\tilde{P}_i \notin$ supp (D), unless $P_i = \tilde{P}_i$, in which case $m_i = 1$.

Definition 14: Let $D = \sum m_i P_i - (\sum m_i)\infty$ be a semi-reduced divisor. If $\sum m_i \leq g$, then D is called a reduced divisor.

Every element of J_C is represented by exactly one reduced divisor in D^o. So, to represent the elements of Jacobian, Mumford representation is used. A semi-reduced divisor $D = \sum m_i P_i - (\sum m_i)\infty$ in Mumford representation is a pair gcd (div ($a(u)$), div($b(u)$ - v)) and can be simplified into div(a, b) where $a(u)$ is a monic polynomial such that $a(u) = \prod (u - x_i)^{m_i}$ and $b(u_i) = y_i, \forall\ i$ for which $m_i \neq 0$. Also, $a(u) \mid b(u)^2 + b(u)h(u) - f(u)$ and deg $b(u)$ < deg $a(u)$.

The following is the brief description of the group law which is given in terms of the Mumford polynomial representation (Taylor, 2007):

- Given divisor classes, $D_1, D_2 \in J_C$ take rational reduced representatives D_1, D_2.
- Form a new rational, semi-divisor $D_1 + D_2$ by combining the points D_1, D_2 in D^o.
- Reduce modulo *Princ* to some rational D of degree at most g.
- Define $D_1 \oplus D_2$ to be the equivalence class of D in J_C.

Cantor's Algorithm

In 1987, David G. Cantor (Cantor, 1987) was presented the Cantor's algorithm to compute the group law of Jacobian, $J_C$for any field K, where C is an imaginary hyperelliptic curve. Cantor's algorithm is general and can work in any field and genus (Cohen, et al., 2006). Let D_1 = div(u_1,v_1) and D_2= (u_2, v_2) be two reduced divisor defined over K. The aim is to find the unique reduced divisor equivalent to $D_1 + D_2$. In his algorithm, performance steps can be divided into two steps namely composition and reduction. Let the hyperelliptic curve equation defined over K such that $C : v^2 + h(u)v = f(u)$.

Input : D_1 = div(u_1, v_1) and D_2= (u_2, v_2), both defined over K

Output: A reduced divisor D = div(u', v') defined over K such that $D \sim D_1 + D_2$

(A) Composition

1. Using extended Euclidean algorithm, find $d_1 = \gcd(u_1, u_2) = e_1 u_1 + e_2 u_2$
2. Using extended Euclidean algorithm, find
   $d = \gcd(d_1, v_1 + v_2 + h) = c_1 d_1 + c_2(v_1 + v_2 + h)$
3. $s_1 = c_1 e_1$; $s_2 = c_1 e_2$; $s_3 = c_2$

4. $u = \frac{u_1 u_2}{d^2}$; $\quad v = \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \pmod{u}$

The divisor D = div (u, v) in step 4 is known as semi-reduced divisor.

(B) Reduction

5. $u' = \frac{f - vh - v^2}{u}$ $v' = (-h - v) \bmod u'$
6. If $\deg(u') > g$, then $u = u'$, $v = v'$ go to 5.
7. Make u' monic by dividing by its leading coefficient.
   The divisor D = div (u', v') in step 7 is known as reduced divisor.

Example 1: We here will present an example of computing the addition of two divisors in imaginary genus two hyperelliptic curve defined over prime field, F_{31} using Cantor's algorithm. Given$C$: $y^2 = x^5 + 7x^4 + 6x^3 + 2x^2 + 8x + 2$ over F_{31}.

Solution:

Let $P = (2,1)$, $Q = (8,3)$ and $R = (10,4)$. We have $D_1 = P + Q - 2\infty$ and $D_2 = P + R - 2\infty$

$u_1 = (x-2)(x-8) = x^2 - 10x + 16 \equiv x^2 + 21x + 16 \pmod{31}$, $v_1 = \frac{1}{3}[x+1] \equiv 21x + 21 \pmod{31}$

$\rightarrow D_1 = \text{div}(x^2 + 21x + 16, 21x + 21)$

$u_2 = (x-2)(x-10) = x^2 - 12x + 20 \equiv x^2 + 19x + 20 \pmod{31}$, $v_2 = \frac{3}{8}x + \frac{1}{4} \equiv 12x + 8 \pmod{31}$

$\rightarrow D_2 = \text{div}(x^2 + 19x + 20,\ 12x + 8)$

Now, we can compute the sum by using Cantor's Algorithm.

1. Using extended Euclidean algorithm, find $d_1 = \gcd(u_1, u_2) = e_1 u_1 + e_2 u_2$

$x + 29 = 16(x^2 + 21x + 16) + 15(x^2 + 19x + 20)$

$d_1 = x + 29$; $\quad e_1 = 16$; $\quad e_2 = 15$

2. Using extended Euclidean algorithm, find

$d = \gcd(d_1, v_1 + v_2 + h) = c_1 d_1 + c_2(v_1 + v_2 + h)$

$h = 0$; $v_1 + v_2 = 21x + 21 + 12x + 8 \equiv 2x + 29 \pmod{31}$

$1 = 30(x + 29) + 16(2x + 29)$,

$d = 1$; $\quad c_1 = 30$; $\quad c_2 = 16$

3. $s_1 = c_1 e_1 = 30 \times 16 = 480 \equiv 15 \pmod{31}$, $s_2 = c_1 e_2 = 30 \times 15 = 450 \equiv 16 \pmod{31}$, $s_3 = c_2 = 16$

4. $u = \frac{u_1 u_2}{d^2} = \frac{(x^2 + 21x + 16)(x^2 + 19x + 20)}{1^2} = \frac{x^4 + 9x^3 + x^2 + 11x + 10}{1} \equiv x^4 + 9x^3 + x^2 + 11x + 10 \pmod{31}$

$s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f) =$

$15(x^2 + 21x + 16)(12x + 8) + 16(x^2 + 19x + 20)(21x + 21) + 16((21x + 21)(12x + 8) + x^5 + 7x^4 + 6x^3 + 2x^2 + 8x + 2)$

$\equiv 16x^5 + 19x^4 + 23x^3 + 21x^2 + 25x + 14 \pmod{31}$

$v = \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \pmod{u}$

$= 16x^5 + 19x^4 + 23x^3 + 21x^2 + 25x + 14 \pmod{x^4 + 9x^3 + x^2 + 11x + 10} \equiv 16x^3 + x^2 + 24 \pmod{31}$

5. $u' = \frac{f - vh - v^2}{u} = \frac{(x^5 + 7x^4 + 6x^3 + 2x^2 + 8x + 2) - (16x^3 + x^2 + 24)^2}{x^4 + 9x^3 + x^2 + 11x + 10}$

$\equiv \frac{23x^6 + 6x^4 + 13x^3 + 16x^2 + 8x + 15}{x^4 + 9x^3 + x^2 + 11x + 10}$

$$= 23x^2 - 207x + 1846 + \frac{(-16647x^3 + 217x^2 - 18228x - 18445)}{x^4 + 9x^3 + x^2 + 11x + 10}$$

$$\equiv 23x^2 + 10x + 17 + (\frac{0}{x^4 + 9x^3 + x^2 + 11x + 10})(\text{mod } 31)$$

$$\equiv 23x^2 + 10x + 17(\text{mod } 31)$$

$$v' = (-h - v) \bmod u'$$

$$= -(16x^3 + x^2 + 24)(\text{mod } 23x^2 + 10x + 17) \equiv 25x + 5$$

6. Make u' monic by dividing its leading coefficient

$$u' = 23x^2 + 10x + 17 \equiv x^2 + 22x + 25(\text{mod } 31)$$

$\therefore$ A reduced divisor, $D_1 + D_2 \sim D = \text{div}(u', v') = \text{div}\ (x^2 + 22x + 25,\ 25x + 5)$

Hyperelliptic Curve Discrete Logarithm Problem (HCDLP): The HCDLP on $J_C(F_p)$ can be defined such that two divisors, D_1 and D_2, $D_2 \in \langle D_1 \rangle$ defined over F_p, one needs to determine $l \in \mathbb{Z}$ such that $D_2 \sim lD_1$ if l exists (Koblitz, 1989).

Isogenies: Although the curves are not isomorphic, the Jacobian of the curves may share common properties. An isogeny is the exist of morphism such that $\psi : J_C \to J_{C'}$ which maps the neutral element div (1, 0) to the neutral element of J_C. For every isogeny, there exists dual isogeny such that $\hat{\psi} : J_{C'} \to J_C$. Two curves are isogenous if the Jacobian varieties of both curves are isogenous.

Torsion elements: The kernel of $[n]$ on J_C is denoted as $J_C[n]$. An element $\bar{D} \in J_C[n]$ is called an element of n-torsion.

Frobenius endomorphism: The isogeny $\phi_p : (x_1, y_1) \mapsto (x_1^p, y_1^p)$ induces an endomorphism, ϕ_p which called as Frobenius endomorphism. Frobenius endomorphism related with a characteristic polynomial of degree $2g$.

For genus 2 hyperelliptic curve, its characteristic polynomial has the form such that:

$$\chi(T) = T^4 - a_1T^3 + a_2T^2 - a_1pT + p^2$$

For the Frobenius endomorphism map $\chi(\phi)$ on Jacobian, J_C, $\forall P \in J_C(F_{p^n})$ we have

$$\phi^4(P) - [a_1]\phi^3(P) + [a_2]\phi^2(P) - [a_1p]\phi(P) + [p^2]P = \infty$$

where $|a_1| \leq 4\sqrt{p}$ and $|a_2| \leq 6p$. So, if $T = 1$, then we have $\chi(1) = \#J_C(F_p) = 1 - a_1 + a_2 - pa_1 + p^2$

Order of Jacobian: As for elliptic curve, there is an interval on the number of points over a finite field. To find the order of Jacobian, $\#Jc(F_p)$, we have the following theorem:

Hasse-Weil Interval: Let C be a hyperelliptic curve with genus g defined over F_p, then the order of Jacobian, $\#J_C(F_p)$ will fall in the interval as shown below:

$$(\sqrt{p} - 1)^{2g} \leq \#J_C(F_p) \leq (\sqrt{p} + 1)^{2g}$$

Development on Point Counting Algorithm of Genus 2 Hyperelliptic Curves

In (Cohen, et al., 2006), Pilla was described the generalization of Schoof's algorithm of genus 1 that enable one to compute the characteristic polynomial of Frobenius endomorphism on an arbitrary Abelian variety over finite field in1990. As we know the elliptic curve is the Abelian variety of dimension 1 whereas the hyperelliptic curve genus 2 is the Abelian variety of dimension 2. However, this algorithm seem to be impractical as it required the input a system of polynomial equations to describe the Abelian variety and the group law was expressed in rational functions.

The algorithm was for the genus 2 hyperelliptic curve with odd characteristic only. Gaudry and Harley had conjectured that it was possible to reduce the degree from $O(l^4)$ to $O(l^5)$ by constructing the modular equations for Siegel modular forms to increase the performance of the algorithm. In the paper (Matsuo, Chao, & Tsujii, 2002),

they mentioned that Gaudry - Harley algorithm still cannot compute the orders in sizes for cryptography because when the search was performed on ten Alpha workstations working in parallel and calculated 5 x 10^{11} operations in the Jacobian, it took close to 50 days for the computation on a single 500 MHz workstation. In (Matsuo, et al., 2002) , they were improving the square root algorithm that was baby-steps and giant-steps algorithm. They improved the last step of the Gaudry- Harley algorithm and implemented their improvement on Alpha 21264/667MHz by calculating 135 bits order and it took 16 hours for the computation of $\#J_C(F_q)$. They suggested improving the Schoof- like algorithm. This because the Gaudry-Harley's Schoof like algorithm was time consuming in calculating the order of general curve.

Due to the several limitations in Gaudry-Harley (Gaudry & Harley, 2000), Pierrick Gaudry and Eric Schost (Gaudry & Schost, 2004) presented their several improvements and combined with the works from (Matsuo, et al., 2002) to make the previous algorithm to be effective and perfect for practical purpose in cryptography. They implemented the improved algorithm and result was the improved algorithm managed to count the point of Jacobian of the size 164 bits within one week on a 2.36 GHz Pentium IV computer using NTL and Magma program. Besides the improvement of algorithm, another purpose was to search the hyperelliptic curve which had prime order where early abort strategy was implemented. This strategy was to eliminate the Jacobian order for the curve of genus 2 or its twisted curve which was non-prime. They proposed a faster halving algorithm using better representation instead of Grobner basic computations. However the lifting technique in 3- torsion was harder than in 2- torsion due to the computation difficulty.

In (Scholten & Vercauteren, 2008), Jacobian with associated with hyperelliptic curve genus 2, there exist a generalization of the Schoof-Elkies-Atkin (SEA) algorithm to count the number of elements in by the paper of Gaudry and Schost in 2004 but it is quite slow for implementation. So, they recommended hyperelliptic curve complex multiplication method to construct the desire curves. From (Pelzl, et al., 2003), the theoretical comparison between elliptic (ECC) and hyperelliptic curve cryptosystem (HECC) defined over characteristic 2, their result showed that the performance was almost the same. In addition, HECC genus 3 with $h(x) = 1$ is faster than HECC genus 2.

In (Gaudry & Schost, 2011), to determine the order of Jacobian of genus 2 over a large prime field, the best approach is to extend the Schoof's algorithm of genus 1 curve. They are searching for curve and its quadratic twisted curve which has Jocobian whose order is 16 times a prime. To obtain cryptographic-secured curve, point counting and complex multiplication method can be used. In order to compute the cardinality of the Jacobian of curve genus 2, the main idea is to computer the characteristic polynomial of the Frobenius endomorphism modulo several small prime l and reconstruct by the Chinese Remainder Theorem using Weil's bounds or it is equivalently to find a_1 and a_2. However, the tedious part in genus 2 is the explicit computation of torsion subgroup. They also mentioned that the extension of SEA algorithm in genus 2 did not work well because there was unknown algorithm for computing part of the l- torsion faster than the whole torsion. They improved their previous work in (Gaudry & Harley, 2000) and (Gaudry & Schost, 2004) and the maximum they achieved was $l = 31$ compared with the previous work that was $l = 13$. They also explain the method to compute the torsion divisors of index l^k for $l = 2, 3, 5, 7$ which is different from p.

In the following, we give the practical point counting algorithm forgenus 2 hyperelliptic curve namely Gaudry-Harley algorithm.

Gaudry-Harley algorithm in Genus 2

Input : Hyperelliptic curve, C defined over F_p

Output: $\#J_C(F_p)$

1. Compute $\#J_C(F_p) \bmod 2^k$ by the halving algorithm.
2. For prime number $l = 3, 5, \ldots, l_{max}$, ($l_{max} = 31$,(Gaudry & Schost, 2011)) do
3. Compute $\chi_p(T) \bmod l$ by a Schoof-like algorithm by involving Cantor's division polynomial.

Below are the Schoof-like algorithm:

- For sufficiently many small primes l: Set $L=\{(a_1, a_2); a_1, a_2 \in [0, l-1]\}$. While $\#L > 1$ do:
- Construct l-torsion divisor D.
- Eliminate elements of L such that $\phi^4(D)-[a_1]\phi^3(D)+[a_2]\phi^2(D)-[a_1 p \bmod l]\phi(D)+[p^2 \bmod l]D \neq 0$
- Deduce $\chi(T) \bmod l$ from the final pair a_1, a_2.

4. Compute $\#J_C(F_p) \bmod l$ from $\chi_p(T) \bmod l$.

End for

5. Compute $\chi_p(T) \bmod p$ by using Cartier-Manin operator (Hasse- Witt matrix).
6. Compute $\#J_C(F_p) \bmod p$ from $\chi_p(T) \bmod p$.
7. Compute $\#J_C(F_p) \bmod m$ for $m = 2^e \cdot 3 \cdots l_{\max} \cdot p$ by Chinese Remainder Theorem.
8. Compute $\#J_C(F_p)$ by a square root algorithm (improved baby-steps and giant-steps (Matsuo, et al., 2002)) using $\#J_C(F_p) \bmod m$.

Conclusion

We have given the brief introduction on the arithmetic of imaginary hyperelliptic curves. Besides rely on the hyperelliptic curve discrete logarithm problem, the order of the Jacobian of the curve also is the major concern. The Gaudry-Harley algorithm that we have described becomes the practical algorithm for counting the order of the Jacobian for any randomly chosen genus 2 hyperelliptic curve. Therefore, this significantly contributes to the implementation of the hyperelliptic curve cryptosystem in the real world applications. With the advancement in computational technologies and the further enhancement in point counting algorithm, the genus 2 hyperelliptic curve cryptosystem can compete with the performance of elliptic curve cryptosystem in the future.

Acknowledgment

The authors would like to take this opportunity to thank Universiti Sains Malaysia, School of Mathematical Sciences and USM short term grant for supporting this research. Liew Khang Jie would like to thank Institute of Postgraduate Studies for the financial support under the USM Fellowship scheme.

References:

Blake, I. F., Seroussi, G., & Smart, N. P. (2005). *Advances in Elliptic Curve Cryptography*. New York: Cambridge University Press.

Cantor, D. (1987). Computing in the Jacobian of a hyperelliptic curve. *Mathematics of Computation, 48*(177), 95-101.

Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Kim, N., et al. (2006). *Handbook of Elliptic Curve and Hyperelliptic Curve Cryptography*. USA: Taylor & Francis Group, LLC.

Gaudry, P., & Harley, R. (2000). Counting points on hyperelliptic curves over finite fields. *Algorithmic number theory*, 313-332.

Gaudry, P., & Schost, É. (2004). Construction of secure random curves of genus 2 over prime fields. 239-256.

Gaudry, P., & Schost, É. (2011). Genus 2 point counting over prime fields. *Journal of Symbolic Computation*.

Jacobson Jr, M., Menezes, A., & Stein, A. (2004). Hyperelliptic curves and cryptography. *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, 41*, 255.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation, 48*(177), 203-209.

Koblitz, N. (1989). Hyperelliptic cryptosystems. *Journal of cryptology, 1*(3), 139-150.

Matsuo, K., Chao, J., & Tsujii, S. (2002). An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields. *Algorithmic number theory*, 461-474.

Menezes, A., Zuccherato, R., & Wu, Y. (1996). *An elementary introduction to hyperelliptic curves*: Faculty of Mathematics, University of Waterloo.

Miller, V.(1986). Use of Elliptic Curves in Cryptography, Advances in Cryptology — CRYPTO '85 Proceedings, Hugh C. Williams, 417-426, Springer Berlin / Heidelberg, New York.

Pelzl, J., Wollinger, T., Guajardo, J., & Paar, C. (2003). Hyperelliptic curve cryptosystems: Closing the performance gap to elliptic curves. *Cryptographic Hardware and Embedded Systems-CHES 2003*, 351-365.

Scholten, J., & Vercauteren, F. (2008). An Introduction to Elliptic and Hyperelliptic Curve Cryptography and the NTRU.

Taylor, G. (2007). *The Point Counting Problem for Curves over Finite Fields.* (First-Year Report): University of Edinburgh.

SECURITY UPGRADE FOR A K-RESILIENT IDENTITY-BASED IDENTIFICATION SCHEME IN THE STANDARD MODEL

[1]Ji-Jian Chin and [2]Swee-Huay Heng
[1]*Faculty of Engineering, Multimedia University, Cyberjaya, Malaysia*
[2]*Faculty of Information Science and Technology, Multimedia University, Melaka, Malaysia*
jjchin@mmu.edu.my, shheng@mmu.edu.my

Abstract:

In 2010, Heng and Chin [10] proposed an identity-based identification (IBI) scheme in the standard model which was resilient to a coalition of attackers conspiring together to break the scheme. They argued that the scheme was desirable due to its proof in the standard model, which is still rare in existing literature. Also desirable was that the proposed scheme was designed without bilinear pairings, which costs greatly in terms of operation costs, thereby allowing the scheme to run more efficiently. However, the proof of security for the proposed scheme was only against impersonation under passive attacks, where the adversary is only allowed to eavesdrop on conversations between honest parties during the identification protocol. In this paper, we upgrade the security proof to prove that the scheme is also secure against impersonation under active and concurrent attacks, showing that the scheme is still secure even if the adversary is to interact with honest parties during the attack.

Introduction

An identification scheme allows an entity to prove its identity (prover) to another entity (verifier) in order to gain access to certain resources. In traditional public key cryptography, an identification scheme required the use of certificates in order to bind a user's identity to his random public key. This gave rise to the certificate management problem as managing certificates can prove to be a daunting task in a system with a large amount of users.

Shamir [17] proposed the idea of identity-based cryptography, utilizing a user's identity-string to generate his public/private key pairs instead, therefore doing away with certificates. While the problem of key escrow still existed because the Private Key Generator (PKG) who generates the public/private key pairs knew all the secrets involved, the idea still is a desirable one because it solved the certificate management problem.

However, identity-based identification (IBI) schemes were only introduced and had their security rigorously mathematically defined in 2004 by Neven et al.[1] and Kurosawa and Heng [13] independently. The former proposed transformations that would transform traditional public key identification schemes into IBI schemes while the latter proposed a transformation from traditional signature schemes into IBI schemes. Both papers utilized security proofs assuming the existence of random oracles.

Bellare and Rogaway [4] introduced the idealistic model where random oracles exist to model security proofs where there are no practical functions to provide sufficient mathematical properties that satisfy the proof of security. A random oracle produces a bitstring of infinite length that can be truncated to a desired length, and is open to access by all parties, honest and malicious alike.

Canetti et al. [5] however shown that given certain conditions, a scheme proven secure in the random oracle model may not be secure once these random oracles are replaced by real-life hash functions. Therefore, while all cryptographic schemes should have at least a basic proof of security in the random oracle model, it would be better if the proof of security was given in the standard model.

Recent Developments in IBI

The first IBI schemes in the standard model was introduced by Kurosawa and Heng in [14], followed by a an IBI scheme secure against man-in-the-middle attack by the same authors in [15, 16]. Yang et al. [19] provided a frame work for IBI construction in the random oracle model, with security for standard model schemes provided in the selective-ID model, a weaker setting where the attacker must first identify the target to be attacked before commencing with the training phase of the simulation.

Meanwhile, Chin et al. [7] proposed an IBI scheme based on direct proof of security, instead of transformations from conventional identification and signature schemes as previously proposed in [1] and [11]. The same authors also formalized the security model for hierarchical IBI (HIBI) schemes in [8] and proposed the first concrete HIBI scheme in the random oracle model. Subsequently, Thorncharoensri et al. [18] proposed the first non-stateless IBI scheme secure against concurrent reset attacks, achieving the highest level of security so far, but relying on a new variant of the q-Strong Diffie-Hellman (q-SDH) assumption, the 2-SDH assumption. In the area of code-based cryptography, [6] and [9] have proposed code-based IBI schemes instead of number-theoretical ones.

Our Contribution

In [10], the authors proposed a k-resilient IBI scheme based on [11], [12]'s k-resilient identity-based encryption scheme. However, they only achieved security against passive attacks for up to k-malicious users using the Discrete Logarithm problem in the standard model.

The k-resilient IBI scheme is a desirable scheme because it has a natural proof of security in the standard model, and also offers competitive runtime efficiency due to the fact that it does not rely on bilinear pairings, as all other IBI schemes provably secure in the standard model currently available in literature do. Bilinear pairings are the costliest of all operational expenses, and doing without pairings improves the speed of the identification protocol.

However, [10] left the open question of whether the same scheme is secure against active and concurrent attackers. In this paper, we show that the answer to that question is a positive one.

Preliminaries

In this section, we introduce some descriptions of preliminaries that are used in our k-resilient IBI construction and proof.

The One-More Discrete Logarithm Problem (OMDLP)

The OMDLP was first introduced in [2] and [3]. Let G be a finite cyclic group of order q and let g be a generator of G. An adversary is given a challenge oracle, CHALL, that produces a random group element $W_i \in G$ when queried and a discrete logarithm oracle, DLOG, which provides the discrete logarithm $w_i \in Z_q$ corresponding to the query $W_i$where$g^{w_i} = W_i$. The adversary wins if after making i queries to the challenge oracle, the adversary is able to output solutions to all i challenges with only $i - 1$ queries to the discrete logarithm oracle, meaning it has to solve at least one instance of the discrete logarithm problem without relying on the discrete log oracle..

Formal Definition of IBI

An IBI scheme consists of four probabilistic polynomial time algorithms (Setup S, Extract E, Prove P and Verify V)

1. ***Setup(S).*** *S on input of the security parameter 1^k, publishes the master public key mpk and keeps the master secret key msk to itself.*
2. ***Extract(E).*** *E on input of the public identityID and msk, returns the corresponding user private key usk.*
3. ***Identification Protocol(canonical interaction between P and V).*** *P receives mpk, ID and usk as input while V receives mpk and ID. The two will then run a canonical 3-step interactive protocol which upon completion V will decide to accept or reject P. The interactive protocol consists of the following steps:*
   a. ***Commitment.*** *P sends a commitment CMT to V.*
   b. ***Challenge.*** *V sends a randomly chosen challenge CHA.*
   c. ***Response.*** *P returns a response RSP which V will evaluate and then choose to accept or reject.*

Security Model for IBI

The goal of an impersonator towards an IBI scheme is impersonation. An impersonator succeeds if after interacting with the verifier with public identity ID and is accepted with non-negligible probability.
We describe three types of adversaries for IBI schemes:

1) **Passive Attacker.** The passive adversary eavesdrops on conversations between an honest prover and verifier to extract information.
2) **Active Attacker.** The active adversary interacts with honest provers sequentially as a cheating verifier several times to extract information before attempting impersonation.
3) **Concurrent Attacker.** This is a special type of active adversary where it can interact with multiple provers at the same time.

The difference between IBI security and that of conventional identification schemes is that 1) instead of a random public key, an impersonator can freely choose a public identity ID to impersonate and 2) we assume the impersonator has compromised and therefore already possessed the private keys of several honest users. This allows the impersonator to obtain private keys of any honest users of his choice (thereby corrupting them) besides the one being attacked. The impersonation attack between an impersonator and the challenger is described as a two-phased game as follows:

1) **Setup.** The challenger takes in the security parameter and runs *setup*. The resulting system parameters are given to the impersonator while the master secret is kept to itself.
2) **Phase 1.** In this phase, the impersonator can issue Extract queries to the challenger. The challenger responds by running the Extract algorithm to generate and returns the private key to the impersonator. The queries may be asked adaptively. The capabilities of the impersonator differ in terms of passive attacks, where only conversation transcript queries are allowed, and active and concurrent attacks where it can request to interact with the challenger as a cheating verifier instead.
3) **Phase 2.** Finally, the impersonator outputs a challenge identity which it wishes to impersonate. The challenge identity must have not been queried before in Phase 1. The impersonator now acts as a cheating prover to convince the verifier based on information gathered in Phase 1 and wins the game if it is successful.

We say an IBI scheme is (t, q_I, ε) -secure under passive/ active/concurrent attacks if for any passive/active/concurrent impersonator I who runs in time, Pr $[I\ can\ impersonate] < \varepsilon$, where I can make at mostq_I extract queries.

Review of the k-Resilient IBI Scheme

Construction

1. **Setup**: Define a group G of order q such that $p = 2q + 1$ and p is prime. Pick a random generator $g \epsilon G$ and a random k-degree polynomial $f(x) = \sum_{t=0}^{k} d_t \cdot x^t$ chosen over Z_q. The system parameters are publicized as $\langle g, D_0 = g^{d_0}, \ldots, D_k = g^{d_k} \rangle$. The master secret $f(x)$is kept as secret.
2. **Extract**. Given a public identity $ID \in Z_q$ (can be hashed using a hash function to desired length), compute $f_0 = f(ID)$ from the master key.
3. **Identification Protocol**: P and V do the following:
   a) P chooses a random $r \in Z_q$, computes $x = g^r$and sends x to V.
   b) V picks a random challenge $c \in Z_q$and sends to P.
   c) P calculates $y = r + cf(ID)$and sends y as a response to V.
   d) V accepts if $g^y = x \cdot \left(\prod_{t=0}^{k} D_t^{ID^t}\right)^c$

To verify the correctness of the identification protocol, wehave:

$$g^y = g^{r+cf(ID)} = g^r\left(g^{f(ID)}\right)^c = g^r(g^{\sum_{t=0}^{k} d_t ID^t})^c = x.(\prod_{t=0}^{k} D_t^{ID^t})^c \quad (1)$$

Current Security

We obtain the current security for the k-resilient IBI scheme from Theorem 1 from [10]:

Theorem 1: The k-resilient IBI scheme is (t, q_I, ε)-secure against impersonation under passive attacks (imp-pa) assuming the discrete log problem is (t', ε')-hard where :$\varepsilon \leq \sqrt{\frac{\varepsilon' n}{n-k}} + \frac{1}{q}$

The Security Upgrade

In this section, we provide the new proof of security for the above k-resilient IBI scheme against impersonation under concurrent/active attack (imp-aa/ca):

Theorem 2: The k-resilient IBI scheme is (t, q_I, ε)-secure against impersonation under active and concurrent attacks (imp-aa/ca) assuming the one-more discrete log problem is $(t", q_I, \varepsilon")$-hard where :$\varepsilon \leq \sqrt{\frac{\varepsilon" n}{n-k}} + \frac{1}{q}$

Proof. Assume there exists an impersonator I who (t, q_I, ε)-breaks the k-resilient IBI scheme. Then we show that there is an algorithm M who $(t", q_I, \varepsilon")$-solves the OMDLP with the help of I. Mwill be given a group G , a generator $g \in G$, and access to oracles CHALL andDLog. Mwill then attempt to simulate a challenger for I as:

1) *Setup:* M begins Phase 1 by querying CHALL for the initial challenge, upon which M will be given $W_0 = g^{w_0} = g^{d_0}$. Mfirst chooses k private keys $f_1, \dots, f_k$at random to perform the following calculations for the system parameters $g^{d_1}, \dots, g^{d_k}$. We have the following matrix equation:

$$\begin{bmatrix} f_1 \\ \vdots \\ f_k \end{bmatrix} = \begin{bmatrix} d_0 \\ \vdots \\ d_0 \end{bmatrix} + \begin{bmatrix} ID_1 & \cdots & ID_1^k \\ \vdots & \ddots & \vdots \\ ID_k & \cdots & ID_k^k \end{bmatrix} \begin{bmatrix} d_1 \\ \vdots \\ d_k \end{bmatrix} \quad (2)$$

with$V = \begin{bmatrix} ID_1 & \cdots & ID_1^k \\ \vdots & \ddots & \vdots \\ ID_k & \cdots & ID_k^k \end{bmatrix}$as a non-singular Vandermonde matrix with distinct elements $(ID_1, \dots, ID_k)$. We then have $(d_1, \dots, d_k)^T = V^{-1}(f_1 - d_0, \dots, f_k - d_0)^T$.

Let $(b_{t_1}, \dots, b_{t_k})$ be the t^{th} row of V^{-1}, then we obtain $d_t = b_{t_1}(f_1 - d_0) + \cdots + b_{t_k}(f_k - d_0) = b_{t_1} f_1 + \cdots b_{t_k} f_k - (b_{t_1} + b_{t_k}) d_0$. Upon which, we can then calculate

$$D_t = g^{d_t} = \frac{g^{b_{t_1} f_1 + \cdots + b_{t_k} f_k}}{W_0^{b_{t_1} + \cdots + b_{t_k}}} : t = 1,2, \dots, k \quad (3)$$

Let $f'(x) = \sum_{t=1}^{k} f_t \lambda_t(x)$ and $f(x) = f'(x) + d_0 \lambda_0(x)$where $\lambda_t(x)$, the Lagrange coefficients, are computed from $ID_0 = 0$ and $ID_1, \dots, ID_k$. Mdoes not know $w_0 = f_0$. Mthen passes the k private keys $f_1, \dots, f_k$and the system parameters $\langle g, W_0, D_0, \dots, D_k \rangle$ to I.

2) *Identification Queries:* In this phase, I plays the role of a cheating verifier requesting M to prove itself with ID_j . We can assume without a loss to generality that $ID_j \notin \{ID_1, \dots, ID_k\}$.

a. Commitment: M queries CHALL for a random challenge W_m, sets $x = W_m$and sends it to I.

b. Challenge: I selects a random challenge $c_m \in Z_q$ and sends it to M.

c. Response: M queries DLog with $W_m W_0^{c_m} \left(\prod_{t=0}^{k} D_t^{ID_j^t} \right)^{c_m}$ and sends the result $y_m = log\ [W_m W_0^{c_m} \left(\prod_{t=1}^{k} D_t^{ID_j^t} \right)^{c_m}]$ to I. M increases m by 1.

3) *Impersonation Phase:* After some time, I outputs the challenge identity$ID^* \notin \{ID_1, \dots, ID_k\}$ that it wishes to impersonate, thus ending Phase 1. In Phase 2, I will now assume the role of the cheating prover trying to convince M to accept. $M$is then able to obtain two valid transcripts (x, c_1, y_1) and $(x, c_2, y_2)$by resetting I to the commitment phase after sending x. Based on the Reset Lemma proposed by [3], M can then extract two conversation transcripts with probability more than $(\varepsilon - \frac{1}{q})^2$. M extracts the secret w_0 by calculating $f(ID^*) = \frac{y_2 - y_1}{c_2 - c_1}$ and outputs the solution to the initial challenge by calculating

$$\frac{f(ID^*) - f'(ID^*)}{\lambda_0(ID^*)} = \frac{\sum_{t=0}^{k} f_t \lambda_t(ID^*) - \sum_{t=0}^{k} f_t \lambda_t(ID^*)}{\lambda_0(ID^*)} = \frac{d_0 \lambda_0(ID^*)}{\lambda_0(ID^*)} = d_0 = w_0 \quad (4)$$

Mthen proceeds to calculate the solutions for the other challenges as

$$w_m = y_m - c_m (w_0 + \sum_{t=1}^{k} d_t ID_j^t) \quad (5)$$

where$j$ corresponds to the identification queries for ID_j. This way, M solves all $m + 1$ challenges by making only m queries to the DLog oracle. This completes the description of the simulation.

4) *Probability Study:* We analyze the probability of M winning the game and solving the OMDLP with strictly less queries to DLog than CHALL. Firstly, we have $\Pr[M \text{ computes } w_0 | \neg abort] \geq (\varepsilon - \frac{1}{q})^2$ by the Reset Lemma, accounting for the probability that M can extract $f(ID^*)$ from two valid transcripts. Therefore, the probability of M solving the OMDLP is given by

$$\Pr[M \text{ wins } OMDLP] = \Pr[M \text{ computes } w_0 \wedge \neg abort] = \Pr[M \text{ computes } w_0 | \neg abort] \Pr[\neg abort] \quad (6)$$

$$\varepsilon'' \geq (\varepsilon - \frac{1}{q})^2 \Pr[\neg abort] \quad (7)$$

Finally, we calculate $\Pr[\neg abort]$. Mwill not abort in Phase 1 since there are no adaptive extract queries. In Phase 2, the probability of M not aborting is if I outputs the challenge identity ID^* which it has not queried before. This is given by the probability $\frac{n-k}{n}$ where n is the total number of users. Putting them together, we have:

$$\varepsilon'' \geq (\varepsilon - \frac{1}{q})^2 (\frac{n-k}{n}) \quad (8)$$

$$\frac{\varepsilon'' n}{n-k} \geq (\varepsilon - \frac{1}{q})^2 \quad (9)$$

$$\varepsilon \leq \sqrt{\frac{\varepsilon'' n}{n-k}} + \frac{1}{q} \quad (10)$$

Efficiency Analysis

In this section, we review the efficiency analysis of the k-resilient IBI scheme and compare it against other IBI schemes currently in literature. It is to our discovery that some values can be pre-computed and thereby we revise the complexity costs based on this discovery. The efficiency of the k-resilient IBI scheme is given as in Table 1. We compare the efficiency of the k-resilient IBI scheme against other IBI schemes in the standard model in Table 2.

Table 1 : Complexity cost for each algorithm in the proposed k-resilient IBI.

	Addition	Multiplication	Exponentiation
Setup	*0*	*0*	*k*
Extract	*0*	*k*	*k*
Prove	*1*	*1*	*1*
Verify	*0*	*k+1*	*2k+2*

Table 2 : A Comparison with other IBI schemes in the standard model.

	Efficiency	Imp-pa	Imp-aa/ca	Reset Attacks
HKIBI05a[14]	6G,6E,4P	q-SDH	unknown	Insecure
HKIBI05b[14]	12G,12E,6P	q-SDH	q-SDH	Insecure
HKIBI06[15]	9G,11E,3P,1SOTSS	q-SDH	q-SDH	Insecure
CHG08[7]	(n+4)G,5E,3P	CDH	OMCDH	Insecure
TSY09[18]	16G,20E,2P	q-SDH	2-SDH	2-SDH
k-resilient IBI	(k+2)G,(2k+3)E	DLP	OMDLP	insecure

Legend: G:Group Operations, E:Exponentiations, P:Pairings, SOTSS: Strong One-Time Signature Scheme, imp-pa:passive attack, imp-aa/ca:active/concurrent attack, CDH:computationalDiffie-Hellman assumption, OMCDH: one-more computational Diffie-Hellman assumption, q-SDH: q-strong Diffie-Hellman assumption, 2-SDH: 2-strong Diffie-Hellman assumption.

Conclusion

In this paper, we have provided an upgrade of security for the *k*-resilient IBI scheme. We showed that while the scheme is secure against impersonation under passive attacks previously, it is also provably secure against impersonation attacks under active and concurrent attacks. It is also the first IBI scheme without bilinear pairings.

However while the scheme is now secure against passive, active and concurrent attackers, we have yet to prove it secure against adaptive attackers who can query any identity of its choice. We pose an open problem to construct a k-resilient identity based identification scheme secure against attackers who can query user secrets adaptively.

Acknowledgment

The authors would like to thank the Fundamental Research Grant Scheme EP20100429004 and the Exploratory Research Grant Scheme EP20110815001 for sponsoring this research.

References:

Bellare, M., Namprempre, C. and Neven, G. 2004. SecurityProofs for Identity-Based Identification and SignatureSchemes. In Christian Cachin and Jan Camenisch (Eds.),Advances in Cryptology - ASIACRYPT 2004, Springer-Verlag:Lecture Notes in Computer Science (LNCS), 3027: 268-286.

Bellare, M., Namprempre, C., Pointcheval, D. and Semanko,M. The One-More-RSA-Inversion Problems and the Securityof Chaums Blind Signature Scheme, Journal of Cryptology, 16(2003), pp. 185-215.

Bellare, M. and Palacio, A. 2002. GQ and Schnorr IdentificationSchemes: Proofs of Security against Impersonation underActive and Concurrent Attacks. In Moti Yung (Ed.), Advancesin Cryptology CRYPTO 2002, Springer-Verlag: Lecture Notesin Computer Science (LNCS), 2642: 167-177.

Bellare, M. and Rogaway, P. 1993. Random Oracles are Practical:Paradigm for Designing Efficient Protocols. Proceedingsof the 1st ACM Conference on Computer and CommunicationsSecurity CCS 1993, USA: 6273.

Canetti,R., Goldreich, O, and Halevi, S. The random oraclemodel, revisited. 30th ACM Symposium on Theory of ComputingSTOC 1998, pp. 209-218. ACM Press, 1998.

Cayrel, P.-L., Gaborit, P.,Galindo, D., and Girault, M. 2009.Improved Identity-based Identification using Correcting Codes.Computing Research Repository, Vol(abs/0903.0069).

Chin, J.-J., Heng, S.-H. andGoi, B.-M. 2008. An Efficientand Provable Secure Identity-Based Identification Scheme inthe Standard Model. In S.F. Mjlsnes, S. Mauw, and S.K. Katsikas(Eds.), EuroPKI 2008,. Springer-Verlag: Lecture Notesin Computer Science (LNCS), 5057: 60-73.

Chin, J.-J., Heng, S.-H. andGoi, B.-M. 2009. HIBI: An Efficientand Provable Secure Hierarchical Identity-Based IdentificationScheme. In DominikSlezak, Tai-Hoon Kim, Wai-Chi Fang, and Kirk. P. Arnett (Eds.), Security TechnologySECTECH 2009, Springer- Verlag: Communications in Computerand Information Science (CCIS), 58: 93-99.

El YousfiAlaoui,M., Cayrel,P.-L. andMeziani,M. ImprovedIdentity-based Identification and Signature Schemes usingQuasi-Dyadic GoppaCodes.Proceedings of ISA 2011 (to appearin LNCS).

Heng, S.-H., Chin, J.-J. 2010. An k-Resilient Identity-BasedIdentification Scheme in the Standard Model. InternationalJournal of Cryptology Research, Vol2(1): 15-25.

Heng, S.-H. and Kurosawa, K. 2004. k-Resilient Identity-Based Encryption Scheme in the Standard Model. In TatsuakiOkamoto (Eds.), Topics in Cryptology CT-RSA 2004,Springer-Verlag: Lecture Notes in Computer Science (LNCS),2964: 6780.

Heng, S.-H. and Kurosawa, K. 2006. k-Resilient Identity-Based Encryption Scheme in the Standard Model. IEICETransactions on Fundamentals, E89-A(1): 39-46.

Kurosawa, K. and Heng, S.-H. 2004. From Digital Signatureto ID-based Identification/Signature. In FengBao, Robert H.Deng, and Jianying Zhou (Eds.), Public Key CryptographyPKC 2004, Springer- Verlag: Lecture Notes in ComputerScience (LNCS), 2947: 248261.

Kurosawa, K. and Heng, S.-H. 2005. Identity-Based Identificationwithout Random Oracles. In Osvaldo Gervasi, MarinaL. Gavrilova, Vipin Kumar, Antonio Lagan'a, HeowPueh Lee,YoungsongMun, David Taniar, and ChihJeng Kenneth Tan (Eds.), Computational Science and Its Applications ICCSA2005, Springer-Verlag: Lecture Notes in Computer Science(LNCS), 3481: 603613

Kurosawa, K. and Heng, S.-H. 2006. The Power of IdentificationSchemes. In Moti Yung, YevgeniyDodis, AggelosKiayias, and Tal Malkin (Eds.), Public Key Cryptography PKC2006, Springer-Verlag: Lecture Notes in Computer Science(LNCS), 3958: 364377.

Kurosawa, K. and Heng, S.-H. 2008. The Power of IdentificationSchemes. International Journal of Applied Cryptography(IJACT), 1(1): 6069.

Shamir, A. 1984. Identity Based Cryptosystems and SignatureScheme. In G. R. Blakley, and David Chaum (Eds.),Advances in Cryptology - CRYPTO 1984, Springer-Verlag:Lecture Notes in Computer Science (LNCS), 196: 4753.

Thorncharoensri, P., Susilo, W. and Yi, M. 2009. Identity- Based Identification Scheme Secure against CR Attacks without RO. In HeongYoulYoum and Moti Yung (Eds.), The 11th Workshop on Information Security Applications WISA 2009, Springer-Verlag: Lecture Notes in Computer Science (LNCS), 5932: 94108.

Yang, G., Chen, J., Wong, D.S.,Deng, X. and Wang, D. 2007. A More Natural Way to Construct ID-Based Identification Schemes. In Jonathan Katz, Moti Yung (Eds.), Applied Cryptography and Network Security - ACNS 2007, Springer-Verlag: Lecture Notes in Computer Science (LNCS), 4521: 30732.

MUTUAL REMOTE ATTESTATION IN IPSEC BASED VPN

Norazah Abd Aziz[1,2], Sharipah Setapa [2] and Nur Izura Udzir[1]
[1]*Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor Darul Ehsan, Malaysia*
[2]*MIMOS Berhad, Technology Park Malaysia, 57000 Kuala Lumpur*
azahaa@mimos.my, sharipah@mimos.m, izura@fsktm.upm.edu.my

Abstract:

Secure communication between computer systems is normally established using secure tunnel technologies such as Internet Protocol Security (IPSec). IPSec protocol guarantees authenticity of communication and secure the data at each gateway but it does not provide any assurance on the entity authentication. So, it is important to make sure the trustworthiness of the remote party that already has a faithful system. Trusted Computing Group (TCG) has introduced a platform to solve this issue into the mainstream computer industry through their main approach called Trusted Platform Module (TPM). TPM is a security module which has been designed to store information of system events securely as well as the key component in the attestation realization. Trusted Computing Platform (TCP) provides a mechanism to supports attestation by its Platform Configuration Registers (PCR) which has become the integrity measurement of a platform. Attestation is a mechanism to provide remote assurance of the state of the hardware component running on a computing device. This paper, proposes an extension to the IPSec key exchange protocol by establishing properties-based attestation using key management service. An embedded attestation extension is provided in VPN communication such as IPSec protocol by establishing mutual properties based attestation using key management service (KeyMS) measurement value as properties. Hence, the proposed approach will protect both sender's and receiver's platforms integrity at their respective gateways.

Introduction

Virtual Private Networks (VPN) is secure network approaches that are widely used for public network infrastructures. It offers the easy way to handle complex networks as well as maintaining sure data transfer between two network hosts. However, the VPN mechanism acquires severe managerial restriction in order to provide the better perimeter security for all VPN endpoints. Hence, it affects the VPN secure capabilities to protect the network from attacker. Although, there are many proprietary security software solution such as anti-virus moving towards solving this issue but it still cannot prevent unexpected attacks. Furthermore, the complexities of the solution may reduce the interoperability of the mechanism with other software. This issue was addressed by Trusted Computing Group (TCG) with attestation approach [1].

Attestation is a mechanism to provide remote assurance of the state of the hardware component running on a computing device [standard]. It provides the trust foundation for computing platform by achieving the integrity of properties and/or configuration of the platform [2]. Remote attestation is a process by which a TCG compliant platform embedded with TPM authenticates its platform to a remote platform by sending its hashes of the properties or configuration platform component via digital signature. Then, the remote platform will verify the trustworthiness of the platform with standard or enhanced attestation protocol accordingly. Through remote attestation protocol, the requestor or client can access the remote platform without revealing its identity while allowing the requestor to verify the integrity of hardware and software of the running remote platform. So, the requestor can decide whether or not to trust the remote platform's configuration. In order to achieve the goals, the Trusted Platform Module (TPM) is implemented as the key component in the remote attestation realization. TPM provides the essential safe memory and cryptographic operation ability for the protocol. It provides a mechanism that supports the attestation by its Platform Configuration Registers (PCR) which has become the integrity measurement of a platform. The PCR are meant to store the integrity measurement safely.

Normally, we have to setup configuration before any communication is established. The configuration means any authorization mechanism such as username and password at the host. Since everyone can use the host, they can trace the username and password; hence change the configuration without notice by the owner of the host. Due to that, hosts lack the capability to remotely verify the hardware, operating system, or other software running. This leads to host vulnerabilities in operating system. TPM by using attestation approach, attempts to solve this deficiency using secure hardware and public-private key-pair as well as the module responsible in verifying the trustworthiness of the system.

IPSec is one of the famous VPN communication mechanisms. Due to limitation of VPN mechanism as discuss earlier, this paper proposes IPSec key exchange protocol extension. The extension is embedding the attestation mechanism in IPSec protocol and explains further in next part.

Related work

The TCG has started Trusted Network Connect (TNC) project to utilize remote attestation in existing secure communication protocol. The TNC framework is discussed in [3] involving data exchanges between Agents [4][5] through network endpoints using attestation approach. In [6], the extended works of TNC method [4] that integrates with Extensible Authentication Protocol (EAP) framework was proposed. EAP is a protocol that enables multiple authentication mechanisms. However, this approach has a few issues which were discussed detail in [7].

The issue of compromised remote tunnel endpoints has been discussed in [8], but they focus on SSL implementation. They also proposed mechanism that links specific properties of a remote endpoint to gain TPM-based attestation. The approach focuses on virtualization environment implementation and aims to avoid certificate complexity. In [9], the author discuss about remote tunnel access tunnel involving VPN server. The paper focuses in depth of policy enforcement in order to verify the integrity of client properties. They introduced the method of track the changes of remote client's security properties by utilizing Linux prototype and attestation mechanism. However, they focus more on policy rather than embedded the attestation into IPSec architecture.

Our method takes a similar approach as [7] which provides an embedded attestation extension in IPSec protocol. Their approach proposed new payload in IKEv2 which called as Attestation Data Payload (ADP) in IKE version 2 but our approach just using the existing payload in ESP header and support both IKE version 1 and version 2. Our approach using Key management service (KeySMS) as one of properties-based-attestation [10] value as well as is implement remote attestation protocol.

IPSec and Remote Attestation

Typically, users utilize a Virtual Private Network (VPN) to secure their network communication to their organization intranet from home, cybercafé and other places. The VPN offer security mechanism using cryptographic protocols in order to provide data confidentiality, entity authentication and data integrity. One of the security mechanisms is IPSec which developed by Internet Engineering Task Force (IETF). IPSec [8] is a protocol to provide end-to-end security in the Internet Protocol (IP) to secure and authenticate transmission of each IP packet of a communication session. IPSec consist of two main operations, namely Authentication Header (AH) and Encapsulating Security Payloads (ESP). AH is to protect against replay attack by offering data integrity and data origin authentication for IP datagram. ESP is also providing data origin authentication as well as data confidentiality and connectionless integrity. IPSec offers channel and transport encryption modes. The channel mode encrypt header and data payload but transport mode only encrypt the payload. IPSec also provides Security Association (SA) function in order to make use the AH and ESP. The SA is a bundle of algorithms to run AH and/or ESP operations such as Internet Security Association and Key Management Protocol (ISAKMP) framework. The ISAKMP framework consists of key exchange authentication that comes with pre-shared key such as Internet Key Exchange (IKE) and Kerberized Internet Negotiation of Keys (KINK). Figure 1 describes a relation between IKE and IPSEC.

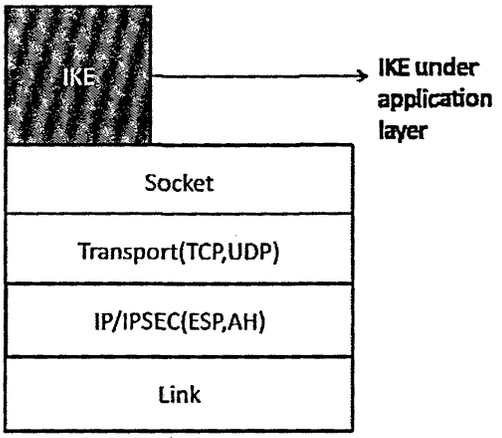


Figure 1 : IPSec layer and relation with IKE

Through the IKE, algorithm and other parameters are negotiated. So, IPSec manage to secure Internet Protocol (IP) communications by encrypting each IP packet of a communication session. However, the IPSec only protects application traffic across IP network but not the integrity of the connection endpoints. Since this issue is not being addressed in IPSec, this paper proposes to extend IPSec with the attestation mechanisms. In our method, the properties based attestation is embedded in IPSec protocol to establish mutual remote attestation between end to end point VPN networks. Our framework containing the IPSec router with the embedded attestation illustrated in Figure 2. In the framework, each endpoint has built-in TPM capabilities in order to establish integrity measurement architecture and providing mutual remote attestation.

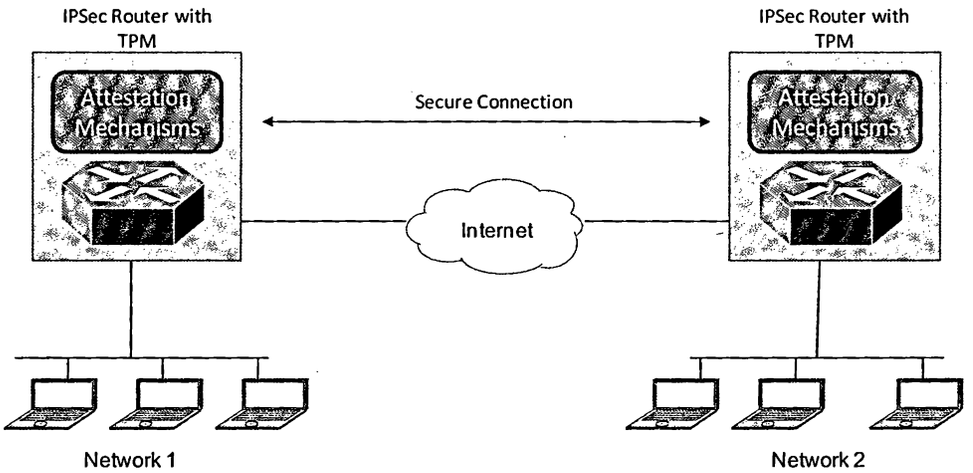


Figure 2 : Mutual attestation between two network endpoints

Basically, our method consists of three main processes: initial configuration process, remote attestation process and verification process. The initial configuration process is to generate the core properties based attestation hash value based on core policy and VPN configuration setup which has been agreed by each VPN endpoint. Remote attestation process as we know is involving authentication and negotiation process between each VPN endpoint. The last step is verification of encrypted data packet process.

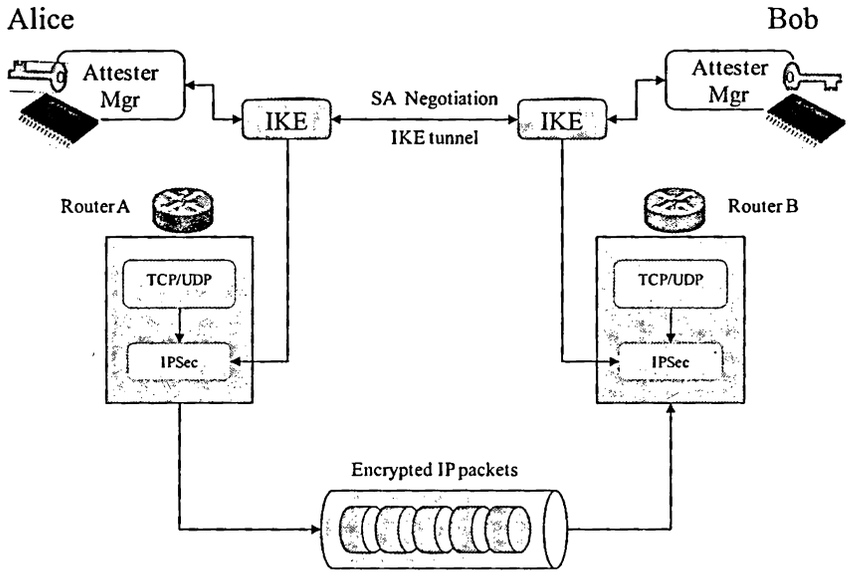


Figure 3 : Detail proposed framework

Before remote attestation via IPSec is established, a core policy based on VPN tunnel configuration that at least uses the IKE management service is generated. A core policy is generated based on system environment and requirement of each platform. The following steps show the process of obtaining the core integrity measurement value:

1. Generate a policy which has been agreed by each of the host and is aligned with key management services, and update into security policy database. The copy of policy is stored at secure storage handled by Privacy CA. Each host has the same configuration value based on IPSec policy.
2. Generate a properties-based attestation as core integrity measurement based on the policy, and key management service ID and append with specific host ID such as MAC address and store it into the PCR. The PCR will encrypt this data at least with the specified TPM key or IPSec key.
3. Each host encrypts the core policy and then stores it at secure storage.

If there are requests for attestation by both gateways, the communication process begins by generating the property based attestation hash values. The process is as follows.

1. First, Alice runs the attestation process to produce the integrity measurement value and TPM key. The key is then sent to the Privacy CA to obtain the TPM certificate. Next, Alice sends the IKE management service request to Bob including a bundle of data containing the ID of network host, properties hash value encrypted with Alice's TPM key, and Alice's TPM certificate.
2. When Bob receives the request, he sends Alice's TPM certificate and network host ID to the Privacy CA for verification. If the returned status is valid, then Bob computes the hash value on Alice's extended PCR values and compares the value to Alice's properties hash values. If the verification is successful, Bob requests for his TPM certificate from the Privacy CA and also generates his properties hash value based on the core policy. Then Bob sends the IKE management service request to Alice.
3. When Alice receives the request, she sends Bob's TPM certificate and network host ID to the Privacy CA for verification. If the verification is successful, Alice continues to verify Bob's extended PCR values. Finally, if the values are valid, Alice begins the IPSec communication for data transmission.

The following is the last step of the IPSec establishment process.

1. After the successful attestation process, Alice and Bob communicates through IPSec using the TPM key which is embedded in the ESP header and the AH header.
2. Every time the data arrives, the recipient will first verify the TPM certificate of the sender.
3. The finger print of payload is signed with TPM key to generate signature as shown below:

$$\text{sign}(\text{hash}(\text{payload}), \text{TPM}_{\text{key}})$$

Conclusion

IPSec protocol provides a method for secure transmission of data and the authenticity of the communication. However, it does not assure the integrity of the involved endpoints platforms which can be solved by remote. We have proposed a protocol that utilizes the IKE negotiation of IPSec and attestation mechanism. The IKE management service is one of properties value in order to realize properties-based attestation mechanism in our extended IPSec. During the IKE negotiation, the remote attestation properties-based is established to measure the state of the end-to-end endpoint. Hence, through this protocol, besides protecting confidentiality, data integrity and origin authentication, it also guarantee the endpoint's integrity and privacy.

References:

TPM Main: Part 1 Design Principles. 1.2 revision 85 edition, 2005.

Trusted Computing Group. Retrieved from http://trustedcomputinggroup.org.

Trusted Computing Group: TNC Architecture for Interoperability, v1.3. (2008)

Trusted Computing Group: TNC TNC IF-IMC Speci_cation, v1.2. (2007)

Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H.: Extensible Authentication Protocol (EAP). RFC 3748 (2004) Updated by RFC 5247.

Trusted Computing Group: TNC IF-T: Protocol Bindings for Tunneled EAP Methods, v1.1. (2007)

Ahmad-Reza Sadeghi, Steffen Schulz, Extending IPSec for Efficient Remote Attestation, Proceeding, FC'10 Proceedings of the 14th international conference on Financial cryptography and data security, ISBN:3-642-14991-X 978-3-642-14.

Goldman, Kenneth and Perez, Ronald and Sailer, Reiner, Linking remote attestation to secure tunnel endpoints, Proceedings of the first ACM workshop on Scalable trusted computing, ISBN: 1-59593-548-7, ACM

Reiner Sailer, Trent Jaeger, Xiaolan Zhang, Leendert van Doorn, Attestation-based Policy Enforcement for Remote Access, Proceedings of the 11th ACM conference on Computer and communications security, ISBN: 1-58113-961-, ACM.

Ahmad-Reza Sadeghi and Christian Stuble, Property-based attestation for computing platforms: caring about properties, not mechanisms, Proceedings of the 2004 workshop on New security paradigms, ISBN:1-59593-076-0, ACM.

THE ANALYSIS OF ELLIPTIC CURVES CRYPTOSYSTEMS ACCORDING TO THE MATHEMATICAL COMPLEXITY AND THE TIME IMPLEMENTATION

Najlae F. Hameed Al-Saffar[1] and Mohamad Rushdan Md Said[2]
Institute for Mathematical Research,
Universiti Putra Malaysia,
43400 UPM Serdang
Malaysia
[1] *najlae_falah@yahoo.com,* [2] *rushdan@math.upm.edu.my*

Abstract:

The group of the elliptic curve points forms an abelian group, which is considered as a suitable choice for constructing a problem similar to the Discrete Logarithm Problem. This creates and opens a new door for treatments of the special group and new operations. In 2005, Al-Saffar (2005) proposed two new methods for elliptic curve cryptosystems using the keys from the algorithm of Diffie–Hellman Key Exchange. In addition, she introduced a variant of the ElGamal scheme. Also, three propositions were introduced to develop the Menezes-Vanstone Elliptic Curves Cryptosystem (MVECC). In this paper, we will discuss all of these propositions and will compare them with the original schemes (ElGamal and MVECC) according to the complexity and the time which they took to implement each scheme.

Introduction

Elliptic curve is a set of solution to binary equations. Elliptic curve cryptography preferably implemented using non-supersingular because of its better security. The group Elliptic Curve systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz (1987) from the University of Washington, and Victor Miller (1986). The elliptic curve cryptosystem was thus created. Since then, numerous researchers and developers have spent years researching the strength of ECC and improving the techniques for its implementation. Today, the scientific efforts are looking for a smaller and faster public key cryptosystem, a practical and secure technology, even for the most constrained environments (see Henkerson and Menezes (2003). For any cryptographic system based on the discrete logarithm problem, there is an analogue for Elliptic Curve (Meng, 2001). One of these systems is Diffie – Helman key exchange system.

Discrete logarithm cryptosystems have been first described in the setting of the multiplicative group of the integers modulo a prime p. Such systems can be modified to work in the group of points on an elliptic curve. For example, the Diffie–Hellman key exchange can be adapted for elliptic curves as follows: Firstly, note that a random point on an elliptic curve E can serve as a key, since Ali and Benin can agree in advance on a method to convert it to an integer. So suppose that E is an elliptic curve over F_p, and P is a publicly known point on this curve. Ali secretly chooses a random integer kA and computes the point kAP, which he sends to Benin. Now, Benin secretly chooses a random kB, computes kBP, and sends it to Ali. Therefore the common key is $Q = kAkBP$. Ali computes Q by multiplying the point he received from Benin by his secret kA, and Benin computes Q by multiplying the point she received from Ali by her secret kB. An eavesdropper who wanted to spy on Ali and Benin would have to determine $Q = kAkBP$ knowing P, kAP, and kBP, but not kA or kB.

This paper, firstly will discuss ElGamal and MVECC which were considered as the original schemes in ECC. Secondly, we will discuss all propositions which have been introduced in Al-Saffar (2005). Finally, we will compare them with the original schemes according to the complexity and the time which they took to implement each scheme.

ElGamal Elliptic Curve Cryptosystem (ElGamal ECC)

ElGamal elliptic curve cryptosystem is a popular and important cryptosystem because of its safety, efficiency and low complexity.

Let $E(F_p)$ be an elliptic curve group and let B be a point on E. The user Benin first selects a private key d and generate a public key $Q = dB$. Second, Ali to encrypt and send a message P_m to Benin, he chooses a random positive integer e and produce the ciphertext C_m, such that: $C_m = \{C, eB\}$, where $C = P_m + eQ$.

To decrypt the ciphertext, Benin computes the following:

$$\begin{aligned} C - d(eB) &= P_m + eQ - d(eB) \\ &= P_m + e(dB) - d(eB) \\ &= P_m. \end{aligned}$$

Example

Let E be an elliptic curve define over F_{11317} with parameters $a = 9817, b = 47$ where $(4a^3 + 27b^2) \bmod p = 7090 \neq 0$. And $\#E = 11489$. Since $\#E$ is prime number then, every point on E is base point (Al-Saffar, 2005), so let $B = (11117, 3663)$. If Ali wishes to send the message $M = (10498, 1304)$ to Benin using ElGamal elliptic curve cryptosystem, what should they do?

Solution

Benin chooses a random integer d as a secret key, let $d = 7391$, and computes her public key $dB = 7391 * (11117, 3663) = (8916, 7552)$.

Ali chooses a random integer e as a secret key, let $e = 6693$ and computes $e(dB) = 6693 * (8916, 7552) = (2094, 6145)$,

$eB = 6693 * (11117, 3663) = (326, 2417)$,

$C = M + e(dB)$.

$= (10498, 1304) + (2094, 6145)$

$= (3038, 367)$,

and sends $\{(3038, 367), (326, 2417)\}$ to Benin.

Benin to decrypt the ciphertext,

she computes $d(eB) = 7391 * (326, 2417) = (2094, 6145)$,

and computes $C - d(eB) = (3038, 367) - (2094, 6145)$

$= (3038, 367) + (2094, -6145)$

$= (10498, 1304)$

$= M$.

Menezes–Vanstone Elliptic Curve Cryptosystem (MVECC)

This is a cryptosystem that has no analogue for discrete logarithm problem (i.e. this cryptosystem does not depend on discrete logarithm problem as the above cryptosystems). In this variation, the elliptic curves is used for "masking", and plaintexts and ciphertexts are allowed to be arbitrary ordered pairs of (nonzero) elements (i.e., they are not required to be points on E) (see Sagheer (2004) and Pietiläinen (2000)).

Algorithm for MVECC

If Ali wants to encrypt and send Benin the message M , then they do the following setup:

Setup:

- Ali and Benin agree upon an elliptic curve $E(F_p)$ and a base point B .
- Benin first selects a private key d and generates a public key $Q = dB$.

- Ali wishes to encrypt and send a message $M = (m_1, m_2)$ to Benin, he chooses a random positive integer e and produces the ciphertext C_m consisting of the pair of points $C_m = \{C, eB\}$ and send it to Benin, where $C = (c_1, c_2)$ and:

$$c_1 = m_1.k_1 \bmod p,$$
$$c_2 = m_2.k_2 \bmod p,$$
$$eQ = (k_1, k_2).$$

- Benin likes to decrypt the ciphertext, she computes the following:

$$(k_1, k_2) = d(eB), \text{ and then}$$
$$m_1 = c_1.k_1^{-1} \bmod p,$$
$$m_2 = c_2.k_2^{-1} \bmod p.$$

Proposition to Variant ElGamal ECC

To vary the encryption and decryption of ElGamal ECC, let $E(F)$ be an Elliptic Curve group and let B be a base point on E. The user Benin first selects a private key d and generates a public key $Q = dB$. If Ali would like to encrypt and send a message M to Benin, he should choose a random positive integer e and produce the ciphertext C_M, such that $C_M = \{C, eB\}$ where $C = M - eQ$. To decrypt the ciphertext, Benin computes the following:

$$C + d(eB) = M - eQ + d(eB) = M - e(dB) + d(eB) = M.$$

Proposition to Development of MVECC

The development of the encryption and decryption of MVECC are as follows:

(1) Suppose Ali wants to send a message $M = (m_1, m_2)$ to Benin. Let d denote Benin's secret key and $Q = dB$ [B is a point on E] denote Benin's public key . Ali chooses a random integer e and sends C_M: $C_M = \{C, eB\}$, where $C = (c_1, c_2)$, $(k_1, k_2) = eQ$,
$c_1 = (m_1 + k_1 k_2) \bmod p$, $c_2 = m_1 (m_2 + k_2 k_1) \bmod p$.
To decrypt the ciphertext Benin computes:
$(k_1, k_2) = d(e B)$, $m_1 = (c_1 - k_1 k_2) \bmod p$, $m_2 = (m_1^{-1} c_2 - k_1 k_2) \bmod p$.

(2) Suppose Ali wants to sent a message $M = (m_1, m_2)$ to Benin, Let d denotes Benin's secret key and $Q = dB$ (B is a point on E) denotes Benin's public key. Ali chooses a random integer e and sends C_M: $C_M = \{C, eB\}$, where $C = (c_1, c_2)$, $(k_1, k_2) = e Q$,
$c_1 = (m_1 * (k_1 k_2 - k_1)) \bmod p$, $c_2 = (m_2 * (k_1 k_2 - k_2)) \bmod p$. To decrypt the ciphertext Benin computes: $(k_1, k_2) = d(e B)$, $m_1 = (c_1 * (k_1 k_2 - k_1)^{-1}) \bmod p$, $m_2 = (c_2 * (k_1 k_2 - k_2)^{-1}) \bmod p$.

(3) Suppose Ali wants to send a message $M = (m_1, m_2)$ to Benin. Let d denotes Benin's secret key and $Q = dB$ [B is a point on E] denotes Benin's public key. Ali chooses a random integer e and sends C_M: $C_M = \{C, eB\}$, where $C = (c_1, c_2)$, $(k_1, k_2) = e Q$,
$c_1 = m_1 + (k_1 k_2^{k_1})^{-1} \bmod p$, $c_2 = m_2 + (k_2 k_1^{k_2})^{-1} \bmod p$. To decrypt the ciphertext Benin computes: $(k_1, k_2) = d(e B)$, $m_1 = (c_1 - (k_1 k_2^{k_1})^{-1}) \bmod p$, $m_2 = (c_2 - (k_2 k_1^{k_2})^{-1}) \bmod p$.

Propositions Algorithms for Elliptic Curves Cryptosystem

In these algorithms they have tried to benefit from the Diffie-Hellman Key Exchange to use this key (the key comes from DHEK algorithm) as secret key in the following algorithms:

Algorithm of (PA_1)

- Ali and Benin Compute $edB = S = (s_1, s_2)$. (Using DHEK algorithm)
- Ali sends a message $M \in E(F_p)$ to Benin as follows:
  - Compute $(s_1 * s_2) (\mathrm{mod} N) = K$. (Such that $\gcd(s_1 * s_2, N) = 1$)[1]
  - Compute $K * M = C$, and send C to Benin.
- Benin receives C and decrypts it as follows:
  - Compute $(s_1 * s_2) (\mathrm{mod} N) = K$.
  - Compute $K^{-1} (\mathrm{mod} N)$. (Where $N = \#E$)
  - $K^{-1} * C = K^{-1} * K * M = M$.

Algorithm of (PA_2)

- Ali and Benin Compute $edB = S = (s_1, s_2)$.(Using Diffie–Hellman Scheme)
- Ali sends a message M to Benin as follows:
  - Compute $(s_1^{s_2}) (\mathrm{mod} N) = K$. (Such that $\gcd(s_1^{s_2}, N) = 1$)[2]
  - Compute $K * M = C$, and send C to Benin.
  - Benin receives C and decrypts it as follows:
- Compute $(s_1^{s_2}) (\mathrm{mod} N) = K$.
  - Compute $K^{-1} (\mathrm{mod} N)$.
  - $K^{-1} * C = K^{-1} * K * M = M$.

The public keys are eB and dB where B is the base point on $E(F_p)$ and the secret keys for Ali and Benin are e and d respectively.

Example

Let E be an elliptic curve define over F_p where $p = 3023$ with parameters $a = 1, b = 2547$ where $(4a^3 + 27b^2) \bmod p = 2027 \neq 0$, and $\#E = N = 3083$. Since $\#E$ is prime number then, every point on E is base point (Al-Saffar, 2005), so let $B = (2237, 2480)$.

To apply Algorithm of (PA_2), at first we must apply Diffie–Hellman Exchanging key

- Ali chooses a secret random integer $e = 2313$.

$eB = 2313 * (2237, 2480) = (934, 29)$. And send $(934, 29)$ to Benin.

- Benin chooses a secret random integer $d = 1236$.

$dB = 1236 * (2237, 2480) = (1713, 1709)$. And send $(1713, 1709)$ to Ali

- Ali computes the secret key $e(dB) = 2313 * (1713, 1709)$.

$edB = (2537, 1632) = S$.

- Benin computes the secret key $d(eB) = 1236 * (934, 29)$.

$deB = (2537, 1632) = S$

Now, Ali and Benin have the same point $S = (2537, 1632)$.

If Ali send a message $M = (2284, 2430)$ to Benin, he does the following:

- Compute $s_1^{s_2} \bmod N = 25371632 \bmod 3083 = 323 = K$.

---

[1] If $\gcd(s_1 * s_2, N) \neq 1$, then Ali will search about a smallest integer number r such that $\gcd(s_1 * s_2 + r, N) = 1$.

[2] If $\gcd(s_1^{s_2}, N) \neq 1$, then Ali will search about a smallest integer number r such that $\gcd(s_1^{s_2} + r, N) = 1$.

— Compute $K * M = 323*(2284, 2430) = (2555, 1066) = C$, and send it to Benin.

— Benin receives C and decrypts it as follows:

— Compute $s_1^{s_2} \bmod N = 323 = K$.

— Compute $K^{-1} \bmod N = 323^{-1} \bmod 3083 = 1594$.

$$K^{-1}C = 1594*(2555, 1066)$$
$$= (2284, 2430)$$
$$= \text{M}.$$

Analysis of Elliptic Curves Cryptosystems

The development of elliptic curves cryptosystems based on the mathematical framework of complexity theory and the time which is taken to implement them. In this section we will analyses the above cryptosystems according to the mathematical complexity and the time implementation.

According to the Mathematical Complexity

The complexity of elliptic curve cryptosystem (the difficulty of breaking it) is exactly equivalent to solving the discrete logarithm problem. Finding the discrete logarithm of one element in the elliptic will not help find the logarithm of any other element. In fact, let $\#E$ denote group order of E, and let r be the largest prime factor of $\#E$. Then the best known algorithms for finding discrete logarithms in E have complexity $O\left(\sqrt{r}/n\right)$, where n is the number of processors working on the problem. Therefore the mathematical complexity of elliptic curve cryptosystem depends on the largest prime factor of the group order of the elliptic which is used in the system. And on the number of operations which are used during the processing of encryption and decryption algorithms. So, we can discuss the mathematical complexity according to the above fact as follows:

1. When we study the scheme of ElGamal elliptic curve cryptosystem, we see that a variant of this scheme can be developed, but with the same complexity, as in the proposition to variant ElGamal elliptic curve cryptosystem because the addition and subtraction have the same computational complexity.
2. The proposed development 1 of Menezes-Vanstone elliptic curve cryptosystem is more efficient than the Menezes-Vanstone elliptic curve cryptosystem, where in the encryption scheme there are three multiplication operations (k_1k_2, m_1m_2 and $m_1k_2k_1$) and two addition operations. While the decryption scheme needed to compute the inverse operations for m_1, and three multiplication operations ($k_1k_2, m_1^{-1}c_2$ and $m_1^{-1}k_1k_2$) and two subtraction operations.
3. The proposed development 2 of Menezes-Vanstone elliptic curve cryptosystem is more efficient than the previous proposition, where in the encryption scheme there are three multiplication operations ($k_1k_2, m_1k_1k_2, m_1k_1, m_2k_1k_2$ and m_2k_2) and two subtraction operations. On other hand, the decryption scheme needs to compute the inverse operations for ($k_1k_2 - k_1$ and $k_1k_2 - k_2$), and also there were two multiplication operations $(c_1(k_1k_2 - k_1)^{-1}$ and $c_2(k_1k_2 - k_2)^{-1})$.
4. The proposed development 3 of Menezes-Vanstone elliptic curve cryptosystem is more efficient than the previous propositions development 1 and 2, where in the encryption scheme they used the exponentiation operation between two keys to make the key more secure ($k_2^{k_1}$ and $k_1^{k_2}$), and this scheme needs to compute the inverse operations for ($k_1k_2^{k_1}$ and $k_2k_1^{k_2}$) also two addition operations. The decryption scheme needs to compute all the above operations in the encryption scheme and two subtraction operations.
5. The two propositions (Algorithm of (PA_1) and Algorithm of (PA_2)) which have new design to encrypt and decrypt the ciphertext which should be a point on elliptic curve that has been used in the system. The second one is more complex than the first one that is because of the fact that the process of exponential operation is more complex than mathematical process of multiplication operation.

According to the Time Implementation

In order to measure the amount of time required to encrypt and decrypt any text we have simulated all programs with the MATLAB/ version 7.10.0.499/ 32-bit (The Language of Technical Computing).
Cryptosystems often take slightly different amounts of time to process different inputs, so in this section we used different elliptic curves with different primes numbers (size of digits) and different messages to compare between all above systems accordance with the time required to implement each process.
In each term we found that the encryption process in all systems has taken a longer time if we compare it with time which has been taken in the decryption process except the process in the proposed algorithms 2 for elliptic curve cryptosystems, where the time to decrypt the ciphertext is longer than the time to encrypt it.
The ElGamal elliptic curve cryptosystem is the longer system to encrypt and decrypt followed by Menezes-Vanstone elliptic curve cryptosystem and then the development 3 of Menezes-Vanstone elliptic curve cryptosystem, the development 1 of Menezes-Vanstone elliptic curve cryptosystem, the development 1 of Menezes-Vanstone elliptic curve cryptosystem, Variant of ElGamal elliptic curve cryptosystem, the development 1 of Menezes-Vanstone elliptic curve cryptosystem and Proposed Algorithms 1 for elliptic curve cryptosystems, while the faster system was the proposed algorithms 2 for elliptic curve cryptosystems.

All in all, however the difference between them was very small, but the systems which have been introduced in (Al-Saffar, 2005) were faster than the popular systems such as Elgamal or Menezes-Vanstone elliptic curve cryptosystem. We will samples the above by the following:

Example 1/ Suppose that we have E be an elliptic curve define over F_{8233} with parameters $a=0$ and $b=139$ where $\left(4a^3+27b^2\right) \bmod 8233 \equiv 2988 \neq 0$. And $\#E=8089$, with base point $B=(8216,7477)$. If Ali wishes to send the message M to Benin using different elliptic curves cryptosystems he will choose a random integer e as a secret key (let $e=6234$) and Benin will choose a random integer d as a secret key (let $d=3541$). Now we will compute the time it takes to encrypt and decrypt M.

Messages	$M=(8228,5025)$		$M=(8219,7676)$		$M=(7570,7470)$	
Times / Cryptosystems	Encryption Time/ seconds	Decryption Time/ seconds	Encryption Time/ seconds	Decryption Time/ seconds	Encryption Time/ seconds	Decryption Time/ seconds
ElGamal ECC	0.292592	0.176354	0.290878	0.170969	0.283419	0.203476
MVECC	0.276297	0.203651	0.291875	0.178164	0.269145	0.15916
Variant of ElGamal Elliptic Curve Cryptosystem	0.276215	0.18720	0.287232	0.170789	0.298354	0.205623
Development 1 of MVECC	0.278417	0.159984	0.273756	0.156647	0.252891	0.163366
Development 2 of MVECC	0.275221	0.162163	0.277906	0.157675	0.256112	0.211674
Development 3 of MVECC	0.257683	0.200873	0.273627	0.222853	0.284028	0.1973921
PA_1	0.194398	0.198476	0.184653	0.118473	0.218362	0.1234291
PA_2	0.158134	0.143794	0.135682	0.163982	0.153319	0.1855610

Example 2/ Suppose that we have E be an elliptic curve define over F_{11317} with parameters $a=9817$ and $b=47$ where $\left(4a^3+27b^2\right) \bmod 11317 \equiv 7090 \neq 0$. And $\#E=11489$, with base point $B=(11117,3663)$. If Ali wishes to send the message M to Benin using different elliptic curves cryptosystems he will choose a random integer e as a secret key (let $e=6693$) and Benin will choose a random integer d as a secret key (let $d=7391$). Now we will compute the time it takes to encrypt and decrypt M.

Messages	M = (10498,1304)		M = (10502 ,2413)		M = (11312,8637)	
Times / Cryptosystems	Encryption Time/ seconds	Decryption Time/ seconds	Encryption Time/ seconds	Decryption Time/ seconds	Encryption Time/ seconds	Decryption Time/ seconds
ElGamal ECC	0.303633	0.200691	0.288211	0.193807	0.284580	0.201079
MVECC	0.303031	0.203651	0.264538	0.191914	0.295950	0.196345
Variant of ElGamal Elliptic Curve Cryptosystem	0.292426	0.199810	0.287838	0.192543	0.292264	0.202633
Development 1 of MVECC	0.305693	0.205576	0.284990	0.185032	0.271444	0.202973
Development 2 of MVECC	0.299248	0.1936698	0.266064	0.189023	0.293386	0.200534
Development 3 of MVECC	0.302547	0.211924	0.287557	0.210300	0.291263	0.192026
PA_1	0.196150	0.114944	0.199117	0.119267	0.204562	0.124658
PA_2	0.162633	0.195674	0.141658	0.171439	0.160308	0.188047

Example 3/ Suppose that we have E be an elliptic curve define over F_{105557} with parameters $a = 1111$ and $b = 2224$ where $\left(4a^3 + 27b^2\right) \bmod 105557 \equiv 10021 \neq 0$. And $\#E = 105143$, with base point $B = (105280,12229)$. If Ali wishes to send the message M to Benin using different elliptic curves cryptosystems he will choose a random integer e as a secret key (let $e = 66612$) and Benin will choose a random integer d as a secret key (let $d = 85611$). Now we will compute the time it takes to encrypt and decrypt M .

Messages	M = (105551,81862)		M = (72235,49583)		M = (105272,97099)	
Times / Cryptosystems	Encryption Time/ seconds	Decryption Time/ seconds	Encryption Time/ seconds	Decryption Time/ seconds	Encryption Time/ seconds	Decryption Time/ seconds
ElGamal ECC	0.304600	0.223485	0.315133	0.207181	0.399384	0.289173
MVECC	0.307071	0.213422	0.264538	0.215553	0.338914	0.299122
Variant of ElGamal Elliptic Curve Cryptosystem	0.300871	0.227340	0.288938	0.199833	0.299892	0.248201
Development 1 of MVECC	0.305693	0.205576	0.229170	0.195232	0.279134	0.281244
Development 2 of MVECC	0.299248	0.1936698	0.272649	0.188261	0.294489	0.293852
Development 3 of MVECC	0.302547	0.211924	0.293721	0.247238	0.299913	0.199912
PA_1	0.196150	0.114944	0.199872	0.119473	0.222349	0.123821
PA_2	0.162633	0.195674	0.199821	0.192371	0.163326	0.192741

Conclusion

ElGamal cryptosystem is dependent on the additive operation on elliptic curve group. If the sender wants to send any message to the receiver, the sender must use the public key of receiver (as the other public key cryptosystem), and in way, it can change it with the same complexity as in proposition 4, because the addition and subtraction have the same computational complexity. However, the MVECC is a very important public key cryptosystem because of the following:

- It does not depend on additive operation on elliptic curve group.
- The message need not be a point on elliptic curve.

Therefore Al-Saffar (2005) have used this to develop the encryption and decryption scheme with more complexity than the original scheme. The two have different methods to encrypt and decrypt the message. We have discussed all of these propositions and compared them with the original schemes (ElGamal and MVECC) according to the complexity and the time which they took to implement each scheme.

References:

Al-Saffar, Najlae Falah Hameed (2005). *Proposed Developments of Elliptic Curves Cryptosystem*, Master's thesis, University of Babylon.

Hankerson, D. and Menezes, A., (2003). *Elliptic Curve Cryptography*, University of Waterloo.

Koblitz, N. (1987). Elliptic curve cryptosystems, *Mathematics of Computation*, Vol. 48, 203-209.

Meng, T.K., (2001). *Curves for the Elliptic Curve Cryptosystem*, M.S.C. Thesis, University of Singapore.

Miller, V. (1986). *Use of elliptic curves in cryptography*, Advances in cryptology - CRYPTO 85, Springer Lecture Notes in Computer Science vol. 218, 417-426.

Saeki, M.K. (1997), *Elliptic Curve Cryptosystems*, M.S.C. Thesis, McGill University, Montreal.

Sagheer, A.M. (2004). *Enhancement of Elliptic Curves Cryptography Methods,* M.S.C. Thesis, University of Technology, Baghdad.

Pietiläinen, H. (2000). *Elliptic Curve Cryptography on smart cards,* M.S.C. Thesis, University of Technology.

A SURVEY AND IMPLEMENTATION OF CERTIFICATELESS SIGNATURE SCHEMES

Kae-Woei Kang and Ji-Jian Chin
Faculty of Engineering,
Multimedia University
kkwoei88@yahoo.co.uk, jjchin@mmu.edu.my

Abstract:

Certificateless public key cryptography was first introduced by Al-Riyami and Paterson which was meant to solve the key escrow problem and eliminate the use of certificates in traditional Public Key Cryptography (PKC). It can be described as an intermediate model between identity based cryptosystems and traditional PKC. In this research, we carry out a survey on the existing Certificateless Signature (CLS) schemes in literature, including variants of CLS with additional features, and then implement them using a simulator to compare on their run-time efficiency.

Keywords- certificateless public key cryptography; signature; bilinear pairing; MIRACL; run-time efficiency.

Introduction

In traditional Public Key Cryptography (PKC), a Trusted Authority (TA) binds an entity, Alice to her public key by using a certificate. Otherwise, anyone can replace Alice's public key and masquerade as Alice, decrypting messages intended for her and signing messages on her behalf. However, as the number of users in the PKC increased, this gave rise to a new problem - the certificate management problem. In 1984, Shamir [16] introduced the new paradigm of identity-based cryptography (IDC), where Alice was bound to her public key through an identity string which uniquely identifies her. While identity-based cryptography does away the need to manage certificates, it still requires a Private Key Generator (PKG) to generate the user keys for every user in the cryptosystem. Therefore, the key escrow problem was still inherent in both PKC and IDC, where a malicious trusted third party could seriously compromise the entire cryptosystem since they have access to every user's keys.

To deal with the key escrow problem, Al-Riyami and Paterson [1] proposed the concept of certificateless public key cryptography in year 2003, where the Key Generation Center (KGC) computes the partial private key for each user by using his master key. There is no authentication necessary for the public key; hence there is no need of a certificate. The KGC also only holds part of the private key and has no access to the complete key, which is generated by the user. Therefore, it solves the key escrow problem.

In certificateless signatures (CLS), the user's partial private key is generated by KGC with his master key and the user's identity. The complete private key is then generated by the user himself by using the partial private key and his secret value. He also generates the corresponding public key to be published. A message is signed using the user's secret key and the verification is done using his public key, which is publicly available. After the introduction of certificateless public key cryptography, many CLS schemes were proposed and most of them involved the use of bilinear pairings.

Related to certificateless research, Alexander Dent conducted a survey in [5], but his paper covered only certificateless encryption (CE) schemes. Our contribution is twofold: 1) to complement the existing survey for CE schemes done in [5] with CLS schemes as well, and 2) to implement them using a simulator to compare their run-time efficiency.

The remaining paper is separated into the following sections. In section 2 we provide the preliminaries for CLS, including bilinear pairings, intractable mathematical problems the security of CLS schemes are based on, and the formal definition and security model for CLS schemes. In section 3 we provide the survey of existing CLS schemes, defining the proof models, security against adversaries of Type I, II and also the intractable mathematical problems they are based on. In section 4, we present our findings of the runtimes of the schemes we implemented. We conclude in Section 5.

Preliminaries

Bilinear Maps

A bilinear map is used to construct the pairing based function. Consider three groups G_1, G_2 and G_T with the prime order q.There are three types of pairing, but only type-1 and type-3 pairing are used for the pairing based cryptography. The construction of type-1 and type-3 pairings is described in [2] and [3]:

Type-1 Pairing: Let $G_1$is an additive group of prime order q and $G_2$is a multiplicative group of the same order. Let P be the generator of G_1 and the mapping is defined as $e: G_1 \times G_1 \rightarrow G_2$. The following are the properties of Type-1 Pairing:

1) *Bilinear:* $e(aR, bS) = e(R,S)^{ab} \forall\, R,\ S \in G_1$ and $a, b \in Z_q^*$. This can be restated as for all $R, S, T \in G_1$ $e(R+S,T) = e(R,T)e(S,T)$*and* $e(R,S+T) = e(R,S)e(R,T)$.
2) *Non-degenerate:* There exists $R, S \in G_1$ such that $e(R,S) \neq I_{G2}$ where I_{G2} denotes G_2's identity element.
3) *Computable:* There exists an efficient algorithm to compute $e(R,S) \forall R, S \in G_1$.

Type-3 Pairing: Let G_1 and G_2 is additive group of prime order q with the possibility of G_1=G_2. $G_T$is a multiplicative group of the same order. P and $Q$are the generator of G_1 and G_2 and the mapping is defined as $e: G_1 \times G_2 \rightarrow G_T$. The following are the properties of Type-3 Pairing:

1) Bilinear:$\forall (R, S) \in G_1 \times G_2, \forall a, b \in F_q$: $e(aR, bS) = e(R, S)^{ab}$ where F_q is a finite field of order q.
2) Non-degenerate: $\forall R \in G_1$: $e(R, S) = 1_{G_T}$ for all $S \in G_2$ if and only if $R = O$, where O is the identity element of G_1
3) Computable: $\forall (R, S) \in G_1 \times G_2$ where $e(R, S)$can be computed in polynomial- time.

Mathematical Problems

In this section we give a brief description of the intractable mathematical problems that are used in proving CLS secure against adversaries.

Discrete Logarithm Problem (DLP): Given that q, P and $Q \in G_1^*$. Find an integer $x \in Z_q^*$ where $Q = xP$.
Computational Diffie-Hellman Problem (CDHP): Given than <P, aP, bP> for any $a, b \in Z_q^*$. Compute abP.
Decisional Diffie-Hellman Problem (DDHP): Given that <P, aP, bP, cP> for any $a, b, c \in Z_q^*$. Decide whether c is same with $ab \bmod q$.
Bilinear Diffie- Hellman Problem (BDHP): Given that <P, aP, bP, cP> for any $a, b, c \in Z_q^*$. Compute $e(P,P)^{abc}$.
Inverse Computational Diffie-Hellman Problem (ICDHP): Given that P and aP for any $a \in Z_q^*$, compute $\frac{1}{a} P$
Decisional Bilinear Diffie-Hellman Problem (DBDHP): Given that <P, aP, bP, cP>for any $a, b, c \in Z_q^*$ and $h \in G_2$. Decide whether h is same with $e(P,P)^{abc}$.
Modified Inverse Computational Diffie-Hellman Problem (mICDHP): Given <b, P, aP> for any $a, b \in Z_q^*$; Compute $(a+b)^{-1} P$.
k-CAA Problem: Given <$P, sP, t_1, t_2, \cdots, t_k \in Z_q^*, (s+t_1)^{-1}P, (s+t_2)^{-1}P, \cdots, (s+t_k)^{-1}P$> for some $t_o \in Z_q^*$. Compute $(s+t_o)^{-1}P$.
Gap Diffie-Hellman Problem (GDHP): Refer to a class of problem where CDHP is hard while DDHP is easy.
Gap Bilinear Diffie- Hellman Problem (GBDHP): Given a randomly chosen $P \in G_1$, as well as aP, bP and cP (for any $a, b, c \in Z_q^*$), compute $e(P,P)^{abc}$ with the help of DBDH oracle.
Weak Diffie-Hellman Problem (WDHP): Given that <P, S, aP> for $S \in G_1$ and for some $a \in Z_q^*$. Compute aS.
q- strong Diffie-Hellman Problem (q-SDHP): Given $g_1 \in G_1, g_2 \in G_2$ and $x \in Z_p^*$, and the $(q+1)$-tuple $(g_2, g_2^x, \cdots, g_2^{x^q}) \in G_2^{q+1}$ as input. Compute a pair $(g_1^{\frac{1}{x+c}}, c)$, where $c \in Z_p$ (Type-1 pairing).
Bilinear Pairing Inversion Problem (BPI): With the input ($Q \in G_1$,$e(P,Q) \in G_2$),compute $Q \in G_1$.

Formal Definition of a Certificateless Signature Scheme

Table 1 shows the algorithms of a CLS as defined by Al-Riyami and Paterson [1]. It consists of 7 algorithms which are Setup, Set Secret Value, Partial Private Key Extraction, Set Private Key, Set Public Key, Sign and Verification.

Alex Dent's survey [5] noted that a second significant departure from the original definition of [1] was restrict the computation of a public key to after a partial private key has been obtained, as proposed by Baek et al. to provide security for their CE scheme based on the CDHP [2]. This enables the grouping of 3 algorithms Set Secret Value, Set Private Key and Set Public Key under 1 algorithm of Set User Keys.

Table 1 : Basic Flow of Normal CLS

KGC:	User A:
Setup: Security parameter k →params and master private key *msk* Partial Private Key Extract: ID_A, params, *msk* → partial private key D_A	Set Secret Value: ID_A and params →secret value t_A Set Private Key: D_A,ID_A and t_A → user private key S_k Set Public Key: ID_A , t_A and params → P_k
Signer A- *Sign:* M (and) ID_A (and) S_k (and) params → σ	
Verifier- *verification:* params (and) M (and) ID_A (and) P_k(and) σ → accept or reject	

Security Model of Certificateless Signature Scheme

In this section, we describe the security model of CLS schemes. In most of the schemes, they are declared to be proven secure against Type I and Type II adversaries, or forgers *(not to be confused with types of pairings)*. The Type I forger knows the public parameters and tries to obtain the KGC's master key. The Type II forger is the malicious KGC who knows user's public key and partial private key and tries to obtain user's private key. The Type III forger is newly proposed notion by Harn et al. [12] in their proposed CLS scheme. They describe that the Type III forger has the capability of the adaptive chosen-message attack and tries to fake a valid CLS. Type III can be further divided into two types. The first type is where the master key and user's partial private key are known by the dishonest KGC in user key generation. The second type is basically a third party who doesn't know the KGC's master key and user's private key. Due to type III forger being newly proposed, there has been no rigorous treatment for it as yet. Besides Harn et al's scheme, no other schemes have taken this model into consideration. We therefore omit Type III from our survey.

We also take a special note that Harn et al. [12] does not follow the conventional definition for CLS, as Partial Private Key Extract requires Set Secret Value to be run first to generate a 'KGC public value' on upon its identity request for the KGC to run Partial Private Key Extract on. The partial private key is therefore linked to the secret value through this 'KGC Public value'. The implications of this deviation are yet to be studied.

As what had been defined by Chow and Yap [4], they provide a formal definition of existential unforgeability of CLS under adaptive chosen message and identity attack for the first two types of forgers.

We only consider the security of schemes under the strongest security notion of existential unforgeability under adaptive chosen message attack (EUF-CMA). In the EUF-CMA security model, a forger is given access to a signing oracle and is able to produce valid signatures on any message of his choice, even multiple signatures on the same

message. The forger wins if at the end it is able to produce a valid message-signature pair on its own. For CLS the notion extends to producing a valid message-signature pair on an identity of the adversary's choice, called the challenge identity. The forger is also, depending on the Type of forger, allowed different capabilities in corrupting honest users.

The following games show the differences between Type 1 and Type II forgers. The games are described for the forgers which attempts forgeries and a challenger which simulates the CLS environment:

Game for type I forger (models a malicious user):

1. Setup: The setup algorithm is initiated by the challenger C and system's parameters is generated and sent to the Type I forger, F1.
2. Attack: A series of queries can be performed by F1:
   a) Hash Queries: Hash values of any input can be requested by F1.
   b) Partial Private Key extract: the partial private key can be requested by F1 for any identity except for the identities which has been associated with the forgery.
   c) Private key Extraction: the private key can be requested by F1 for any ID except the challenged identities.
   d) Public key request: the public key can be requested by F1 for any identity from the challenger C.
   e) Public key replacement: A new secret value is chosen by F1 and the new public key is computed. The new public key is set as the identity's new public key.
   f) Signature queries: A signature is received by F1 after he has submitted the message and identity.
3. Forgery: A message-signature-identity tuple is outputted by the F1. F1 wins if the identity has never been queried to the private key and the message and identity has never been queried to the signing oracle.

Game for type II forger (models a malicious KGC):

1. Setup: The setup algorithm is initiated by the challenger and system's parameters is generated and sent to the Type II forger, F2.
2. Attack: A series of queries is performed by F2 like F1 in an adaptive manner (as described in Game for type I adversary). However, the public key cannot be replaced by him.

Forgery: A message-signature-identity tuple is outputted by F2. F2 wins if the message and identity has never been queried to the signing oracle.

A Survey on Existing Schemes

Since the introductory of certificateless cryptosystem by Al-Riyami and Paterson, there are a lot of schemes being proposed and different methods of constructing the schemes have been introduced. Our survey also takes into account the additional features of CLS which includes Mediated, Aggregate, Ring, Blind, Proxy and Proxy Blind CLS. Below is a table of summary of the surveyed schemes according to the year they were proposed.

Table 2 : Table of Schemes and Security Level

Schemes	Hard Problems	EUF-CMA		Additional Features	Schemes	Hard Problems	EUF-CM		Additional Features
		I	*II*				I	II	
[GGDS05] [11]	- DLP(master key security) - CDHP (EUF-CMA) - WDHP(collude with TA)	A	A		[R08] [14]	- CDHP	I	I	Partially Blind
[HSMZ06] [13]	-GBDHP	S	S	Designated Verifier	[ZZ08] [26]	- CDHP	S	S	
CPHL07[3]	-k-CAAP(Type I) -mICDHP(Type II)	S	S		[DZ09] [7]	- CDHP (Type I) -mICDHP(Type II)	S	S	Mediated
[CY07] [4]	-k-CAAP(Type I) -mICDHP(Type II)	S	S	Ring	[DW09] [6]	-k-CAAP(Type I) -ICDHP(Type II)	S	S	
[TG07] [18]	- q-SDHP(Type I) - BPI(Type II)	S	S		[GCH09] [9]	- DLP	S	S	
[DC08] [8]	- BDHP (EUF-CMA) - DBDHP(Invisibility)	S	S	Undeniable	[HRL09] [12]	- DLP	A	A	
[GLHC08a] [10]	- CDHP	S	S	Aggregate	[SW09] [17]	-k-CAAP(Type I) -mICDHP(Type II)	F[3]	F[3]	Blind
[GLHC08b] [10]	- CDHP	S	S	Aggregate	[TX10] [19]	-CDHP	A	A	Proxy, Blind

Legend: EUF CMA- Existentially Unforgeable Against Chosen Message Attack, I- Insecure, S- secure, A- ad hoc proof, F-inferred from

Remarks:
The above schemes are all proven secure in the random oracle model except TG07. Cryptanalysis of Certificateless Partially Blind Signature and Proxy Blind Scheme by Zhang et al. [23] on R08 [14] has shown two of the schemes are insecure, as they show the existence of a common flaw: linkability.

Implementation

In this part, the schemes are implemented using C++ and their run time efficiency is compared. The implementation of these CLS schemes has proved that they can function properly without any error. The implementation of CLS involves mathematical functions found in libraries that are not commonly used. Some of these libraries are open source and can be found in the internet.

The library which we chose is the MIRACL library. MIRACL is written by [15]. It was written by Dr Michael Scott who has since been employed by Certivox, a cloud computing information security company, in December 2011.The library was downloaded from the official website on 22nd February 2011 (ver. 5.5). The hardware platform is Intel Core 2 Duo processor T6500 (2.1GHz, 800MHz FSB) with 4GB memory.

Due to a well-defined interface offered by MIRACL library which hides many technical details, substantial parts of the code can be reused by just adding the related header and source files inside. The implementation of the codes becomes less complicated and easy to understand. C++ is chosen as programming language mainly because it is object-oriented and it is more powerful compared to other object-oriented languages, for example Java.

Average run time efficiency for Sign and Verification based on the same message and same identity

Due to time constraints we only implemented ten schemes from the survey. The constructed schemes have been simulated for 1000 times to get the 1000 run times and the average run time efficiency computed. The result is based on the same message and same identity. The size for the Identity is 5 bytes and size for the message is 20 bytes. For the scheme HSMZ06 [13], the result is based on the same message, same identity and same verifier. Size of the verifier is 3 bytes. The test time is measured in unit second.

The run time efficiency for the Signing and Verification algorithm for same message and same identity are also analyzed. Below are the time taken by these algorithms for the schemes. The codes have been simulated for 100 times and the average run-time is computed. The test time is measured in unit second.

Table 3 : Run-Time of Sign and Verification Algorithm (Fixed Parameters)

Schemes	Type of Pairing	Average Time (Sign)	Average Time (Verification)	Total Time	Types of CLS
[GGDS05] [11]	1	0.846704	1.6271	7.16601	Normal
[HSMZ06] [13]	1	0.641071	1.51332	5.85216	Normal
[CPHL07] [3]	1	0.495716	0.974906	2.49120	Normal
[CPHL07] [3]	1	0.676675	0.692166	3.03828	Normal
[TG07] [18]	3	0.0575956	0.188692	1.22114	Normal
[DW09] [6]	1	0.243036	0.452492	2.22519	Normal
[SW09a] [17]	1	0.993432	0.969467	3.20975	Blind
[SW09b] [17]	1	1.18674	0.601426	3.57315	Blind
[WLT09] [20]	1	0.444844	1.34396	4.52485	Normal
[ZG10] [24]	1	1.00717	0.495319	3.01762	Blind

Average run time efficiency for Sign and Verification based on the different messages and different identities

The codes are compiled once again by using different messages and identities. This means that different messages and identities were used for each compilation and there are a total of 1000 valid signatures with 1000 messages and 1000 identities. The size of the identity varies from 9 bytes until 12 bytes while the size of the message varies from 21 bytes until 24 bytes. The size is depends on the length of the identity and message. For the scheme HSMZ06 [13], the compilation is done by verifying the IDs, designated verifier IDs and. Size of verifier varied from 9 bytes until 12 bytes. The test time is measured in unit second.

The run time efficiency for the Key Generation, Signing and Verification algorithm for different messages and different identities are also analyzed. The key generation algorithm consists of Partial Private Key Extract, Set Secret Value, Set Private Key and Set Public Key. Below are the time taken by these algorithms for the schemes. The codes have been simulated for 100 times and the average run-time is computed. The test time is measured in unit second.

Table 4 : Run-Time of Sign and Verification Algorithm (Varied Parameters)

Schemes	Type of Pairing	Average Time (Sign)	Average Time (Verification)	Total Time	Types of CLS
[GGDS05] [11]	1	0.964279	1.8152	7.43394	Normal
[HSMZ06] [13]	1	0.699681	1.61829	5.4233	Normal
[CPHL07] [3]	1	0.497161	1.07015	2.35543	Normal
[CPHL07] [3]	1	0.632774	0.708761	2.74690	Normal
[TG07] [18]	3	0.0614925	0.19045	1.13121	Normal
[DW09] [6]	1	0.236115	0.451646	2.35050	Normal
[SW09a] [17]	1	1.16251	0.722287	3.20034	Blind
[SW09b] [17]	1	1.00914	1.04493	3.93223	Blind
[WLT09] [20]	1	0.422751	1.28215	4.56290	Normal
[ZG10] [24]	1	0.973797	0.495381	2.40151	Blind

The results for the Part A and B are similar. The run-time efficiency is dependent on the complexity of the schemes. The scheme proposed by Gorantla et. al. [2] uses 8 seconds approximately, which has the longest run-time among all the schemes, due to the checking of the validity of parameters. Hence, the process has been slowed down and the run-time has been increased. Type-3 pairing which the scheme is proposed by Terada and Goya [3] has the fastest run time efficiency. It can be concluded that type-3 is more efficient in practice and more suitable for computer applications. The number of bilinear pairing based equations used in the schemes also affect the average run time. The more pairing based equations used, the longer run time it will take.

By observing the results, it can be noticed that Blind CLS have takes significantly longer computational time for the signing algorithm because the blind signature includes extra step to blind and unblind the signature.

The results also show that the scheme proposed by Terada and Goya [3] is the fastest in terms of run time for signing and verification algorithms. Hence, type-3 pairing is the efficient for constructing the CLS schemes.

Conclusion

Certificateless cryptography can be described as a method of solving the weakness of public key infrastructure and identity-based cryptosystem in terms of key escrow. From the research, most of the schemes are constructed based on bilinear pairing, particularly using two types of pairing, which are pairing-1 and pairing-3. Pairing-1 is less complicated and is usually chosen to be implemented in most of the pairing based scheme, but is less efficient. Pairing-3, on the other hand, has better time efficiency and is therefore more suitable in practice.

In this research, we presented a survey of CLS schemes to complement the CE scheme survey by [5]. We provided the formal definition, security model and a presentation of all the CLS schemes currently in literature according to their security against existential forgers under adaptive chosen message attack based on the intractable mathematical problems their security is based on. Subsequently, we also presented the results of our implementations of certain schemes in the survey. The initial results we find are encouraging, signing and verification of various messages averaging at around one second. We believe the results can be further improved by tweaking the code, and as hardware specifications get more advanced.

We find that in our survey there are many schemes without formal reduction proofs. Therefore one open problem would be to supply the proofs of security based on a reductionist approach, rather than by ad hoc security, where flaws are commonly overlooked.

Another open problem we propose is to explore the development of more CLS schemes with proof of security in the standard model, rather than the random oracle model. This is because there are certain flaws that may be inherent with the random oracle model when instantiated with a real hash function since the random oracle is an idealistic hash function which does not exist.

One final open problem is to investigate the relationship between CE, CLS and also other certificateless primitives. Just as identity-based encryption schemes can be converted to digital signatures and digital signatures can be converted into identity-based identification schemes through transformations, we believe intuitively such relationships should exist for CE and CLS schemes as well.

Acknowledgment

The authors would like to thank the Exploratory Research Grant Scheme EP20110815001 for sponsoring this research.

References:

Al-Riyami, S.S., & Paterson, K.G. (2003) "Certificateless Public Key Cryptography", *Advances in Cryptology - ASIACRYPT2003*, Vol. 2894, pp.452-473. Springer-Verlag: Lecture Notes in Computer Science (LNCS).

Baek, J.,Safavi-Naini, R., Susilo, W. (2005) "Certificateless Public Key Encryption Without Pairing". *The Eighth International Conference on Information Security*, ISC 2005. Lecture Notes in Computer Science, Vol:3650, pp. 134-148.

Choi, K.-Y., Park, J.-H., Hwang, J.-Y. and Lee, D.-H. (2007) "Efficient Certificateless Signature Schemes". *Applied Cryptography and Network Security ACNS 2007. Lecture Notes in Computer Science*, Vol:4521/2007, pp 443-458.

Chow, S.-M.S,. and Yap, W.-S. (2007) "Certicateless Ring Signatures". *Cryptology ePrint Archive.* [On-line] Report 2007/236. Available: http://eprint.iacr.org/2007/236.pdf

Dent, A. (2008). "A Survey of Certificateless Encryption Schemes and Security Models". *International Journal of Information Security*, Vol:7(5), pp. 349-377.

Du, H. and Wen, Q. (2009) "Efficient and Provably-Secure Certificateless Short Signature Scheme from Bilinear Pairings". *Journal Computer Standards & Interfaces.* Vol:31(2), pp 390-394.

Du, H. and Zhang, X.. (2009) "An Efficient Security Mediated Certificateless Signature Scheme". *Second International Conress on Image and Signal Processing*, CISP 2009.

Duan S. and Cao , Z. (2008) "Certificateless Undeniable Signature Scheme", *Information Sciences*, Vol:178(3), pp 742-755.

Ge, A. and Chen, S. and Huang, X.. (2009) "A Concrete Certificateless Signature Scheme without Pairings". *Multimedia Information Networking and Security*, MINES 2009.

Gong, Z. and Long, Y. and Hong, X. and Chen, K. (2008) "Practical Certificateless Aggregate Signatures From Bilinear Maps". *Journal of Information Science and Engineering* [On-line] Vol. 26 (6), pp. 2093-2106.

Gorantla, M. and Gangishetti, R. and Das, M. and Saxena, A. (2005) "An Effective Certificateless Signature Scheme based on Bilinear Pairings". *International Workshop on Security in Information Systems*, WOSIS 2005.

Harn, L. and Ren, J. and Lin, C. (2009) "Design of DL-based Certificateless Digital Signatures", *Journal of Systems and Software*, Vol: 82(5), Issue 5, pp 789-793.

Huang, X. and Susilo, W. and Mu, Y. and Zhang, F. (2006) "Certificateless Designated Verifier Signature Schemes". *Twentieth International Conference on Advanced Information Networking and Applications*, AINA 2006.

Rong., W. (2008) "Certificateless Partially Blind Signature Scheme, *Journal of Zhangzhou Normal University*, Vol:4(2), pp 44-47.

Scott., M. (2011) "Multiprecision Integer and Rational Arithmetic C/C++ (Miracl) Library ", *CertiVox Laboratories*. https://certivox.jira.com/wiki/display/MIRACLPUBLIC/Home

Shamir, A. (1984). Identity Based Cryptosystems and Signature Scheme. *Advances in Cryptology - CRYPTO1984*, Vol. 196, 47–53. Springer-Verlag: Lecture Notes in Computer Science (LNCS).

Sun, S. and Wen, Q. (2009) "Novel Efficient Certificateless Blind Signature Schemes". *The Eighteenth International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, AAECC-18 '09.

Terada, R. and Goya, D.-H. (2007) "A Certificateless Signature Scheme Based on Bilinear Pairing Functions". *Symposium on Cryptography and Information Security, 2007*, Sasebo. SCIS 2007.

Tso, R. and Xun, Y. (2010) "Certificateless Proxy Signature and Its Extension to Blind Signature". *Fourth International Conference on Network and System Security*, NSS 2010.

Wang, C. and Long, D. and Tang, Y. (2009) "An Efficient Certificateless Signature from Pairings". *International Journal of Network Security*, Vol:8(1) pp 96-100.

Xiong, H. and Li, F. and Qin, Z. (2010) "A Provably Secure Proxy Signature Scheme in Certificateless Cryptography". *Informatica*, Vol:21(2), pp. 277-294.

Yu, M. and Wu, X. and Guan, J. and Yu, H. (2009) "A Certificateless Proxy Blind Signature Scheme". *World Congress on Software Engineering*, WCSE 2009.

Zhang, J. and Chen, H. and Geng, Q. (2009) "Cryptoanalysis of Certificateless Partially Blind Signature and Proxy Blind Signature Scheme". *Second Internatioanl Congress on Image and Signal Processing*, CISP 2009.

Zhang, J. and Gao, S. (2010) "Efficient Provable Certificateless Blind Signature Scheme". *IEEE International Conference on Networking, Sensing and Control,* ICNSC 2010.

Zhang, B. and Xu, Q. (2009) "Certificateless Proxy Blind Signature Scheme from Bilinear Pairings". *Second International Workshop on Knowledge Discovery and Data Mining*, WKDD 2009.

Zhang, L. and Zhang, F. (2008) "A New Provably Secure Certificateless Signature Scheme". *IEEE International Communications Conference*, ICC 2008.

THRESHOLD SIGNATURE WITH HYBRID PROBLEMS

Mohd Saiful Adli bin Mohamad and Eddie Shahril bin Ismail
School of Mathematical Sciences, Faculty of Science and Technology, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia
exshams_2001@yahoo.com, esbi@ukm.my

Abstract:

The threshold signature schemes with hybrid problems are rapidly developing recently, since it is understood that the single problem-based threshold signature will no longer secure in a near future. In this paper, we propose a new threshold signature with hybrid problems; residuosity and discrete logarithms. The advantage of our scheme is that the scheme provides a greater security due to the fact that it is very unlikely the two problems can be solved simultaneously. The newly developed scheme is also shown secure against several algebraic attacks and requires a reasonable time complexity in both signing and verifying phases.

Introduction

It is important to tie the electronic message or document with the owner's identity. It is different with hand signature, where the digital signature cannot be copy out from a document to another document easily. To guarantee that, a digital signature scheme must be secure, so adversary cannot forge the signature for the electronic message.

For the last three decades, many digital signature schemes have being developed based on various number theoretic problems such that factoring, residuosity (Rivest et. al., 1978), and discrete logarithms (ElGamal, 1985). Although the single-problem schemes remain unsolved today, but it is almost inevitable that one day such problems could be solved. When this happens, the signature based on those problems no longer be secure. That's why recent digital signatures were developed based on hybrid problems (He, 2001; Laih and Kuo, 1997; Lee and Hwang, 1996; Wang and Chang, 2003). The security of these schemes is based on the difficulty to solve multiple hard number theoretic problems simultaneously.

Nowadays, many electronic documents need to be signed by more than one person. This problem brings the idea of society oriented cryptography, which is as known as threshold cryptography (Desmedt, 1988). The development of threshold cryptosystem (Desmedt and Frankel, 1989) used the concept of Shamir's secret sharing (Shamir, 1979), which is based on Lagrange interpolation technique. Then, in 1991, Desmedt and Frankel proposed the first (t, n) threshold digital signature scheme based on the RSA assumption (Desmedt and Frankel, 1991), while Harn proposed another (t, n) threshold digital signature scheme from modified ElGamal scheme (Harn, 1994).

The Proposed Threshold Signature Scheme

The security of our threshold signature scheme is based on the difficulty of solving residuosity and discrete logarithm problems simultaneously. In our scheme, a trusted dealer (TD) is required to generate the parameters and keys for the group. TD also plays the role to verify the partial signatures and construct the group signature.

A digital signature scheme consists of three following steps: (i) generating keys, (ii) signing message; and (iii) verifying signature. The following parameters and notations are used throughout this paper unless otherwise specified:

- $h(m)$ is the one-way hash function for the message m.
- p is a 1024-bits prime number.
- $n = PQ$ is a factor of $p - 1$, where P and Q are two safe primes.
- g is a primitive root mod p, satisfying $g^n \equiv 1 \pmod{p}$.

Step 1: Generating keys

Let u_i denote the group users and there are n users so t of them $(u_1, u_2, \ldots, u_t)$ can represent to sign the message.

1) TD picks randomly $e \in \mathbb{Z}_n^*$ such that $\gcd(e^2, n) = 1$.

2) Then, he calculates $w \equiv g^{e^2} (\text{mod } p)$.
3) After that, he constructs a (t, n) threshold function,

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \ (\text{mod } n),$$

where a_i are random integers between 1 and $n-1$, and $i = 0,1,2, \ldots, t-1$.
4) Sets the group secret key, $P(0) = a_0$, and calculates the corresponding group public key, $V \equiv g^{P(0)} \ (\text{mod } p)$.
5) Set a pair $(x_i, P(x_i))$ for each user, where x_i is the public identity and $P(x_i)$ is the secret key for each user.
6) After each user receives their $(x_i, P(x_i))$, each of them compute the corresponding individual public key $y_i \equiv g^{P(x_i)} \ (\text{mod } p)$.

The public and secret keys for individual and group for the scheme are shown in Table 1.

Table 1 : The public and secret keys of the scheme.

	Public key	**Secret key**
Individual	y_i	$P(x_i)$
Group	w, V	$e, P(0)$

Step 2: Signing message

Each group user can sign the message simultaneously. Here, the steps of signing the message are described.

1) Each user selects r_i such that $0 < r_i < n$ and $\gcd(r_i, n) = 1$.
2) Computes $k_i \equiv g^{r_i} \ (\text{mod } p)$.
3) Each user broadcasts their k_i to other users via secure channel. After all k_i are received, each of them calculates $K \equiv \prod_{i=1}^{t} k_i \ (\text{mod } p)$.
4) By using the information of the public identity x_i of other participating users, each of them calculates $v_i \equiv \prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{-x_j}{x_i - x_j} \ (\text{mod } n)$.
5) Each user calculates $s_i \equiv K \cdot r_i + h(m) \cdot P(x_i) \cdot v_i \ (\text{mod } n)$.
6) Each user sends K and v_i along with (k_i, s_i) as the partial signature for the hash-function message $h(m)$ to TD. Then, TD checks the validity of the partial signature by showing that the following equality holds:

$$g^{s_i} \equiv {k_i}^K \cdot {y_i}^{v_i \cdot h(m)} \ (\text{mod } p)$$

7) After TD shows that all partial signatures are valid, then he solves $S^2 \equiv e^{-2} \sum_{i=1}^{t} s_i \ (\text{mod } n)$ for S. He produces (K, S) as the group signature for the hash-function message $h(m)$.

Step 3: Verifying signature

Any outsider can verify the signature, as long as he has information about the public key. After he receives the group signature (K, S), he checks

$$w^{S^2} \equiv K^K \cdot V^{h(m)} \ (\text{mod } p).$$

If the equation holds, then the group signature is valid.

Theorem 1. *Following the applied protocol, then the verification in the signature verification phase is true.*

Proof:

The equation in signature verification phase is true for valid signature since,

$$
\begin{aligned}
w^{S^2} &\equiv \left(g^{e^2}\right)^{e^{-2}\sum_{i=1}^{t} s_i} && (\mathrm{mod}\, p)\\
&\equiv g^{\sum_{i=1}^{t} s_i} && (\mathrm{mod}\, p)\\
&\equiv g^{\sum_{i=1}^{t} K\cdot r_i + \sum_{i=1}^{t} h(m)\cdot P(x_i)\cdot v_i} && (\mathrm{mod}\, p)\\
&\equiv \left(g^{\sum_{i=1}^{t} r_i}\right)^{K} \left(g^{\sum_{i=1}^{t} P(x_i) v_i}\right)^{h(m)} && (\mathrm{mod}\, p)\\
&\equiv \left(\prod_{i=1}^{t} k_i\right)^{K} (g^{a_0})^{h(m)} && (\mathrm{mod}\, p)\\
&\equiv K^K \cdot V^{h(m)} && (\mathrm{mod}\, p)
\end{aligned}
$$

Security Analysis

In this analysis, some possible attacks are briefly examined.

(i) The attacker wishes to obtain the group secret key e and $P(0)$ by using all information from the system. In this case, he has to solve $w \equiv g^{e^2} (\mathrm{mod}\, p)$, which is clearly infeasible because the difficulty of solving residuosity and discrete logarithms problems simultaneously. The attacker also cannot find $P(0)$ from the group public key, $V \equiv g^{P(0)} (\mathrm{mod}\, p)$ due to the difficulty of solving discrete logarithms problem.

(ii) Derivation of the individual secret key, $P(x_i)$ from the individual public key, $y_i \equiv g^{P(x_i)} (\mathrm{mod}\, p)$ is equivalent to solve the discrete logarithms problem.

(iii) Attacker might try to impersonate member u_i by randomly selects an integer r_i and broadcasts $k_i \equiv g^{r_i} (\mathrm{mod}\, p)$. Since the group signature is determined by all t members, without knowing the individual secret key $P(x_i)$, the attacker cannot generate a valid partial signature (k_i, s_i) to satisfy the verification equation.

(iv) Attacker tries to derive their own group signature (K, S) for a given message m by letting one integer fixed and finding the other one. For example, attacker selects K and tries to figure out the value of S. In this case, he calculates $\gamma \equiv K^K \cdot V^{h(m)} (\mathrm{mod}\, p)$. Then, he has to solve the equation $\gamma \equiv w^{S^2} (\mathrm{mod}\, p)$. Unfortunately, the attacker cannot find S due to the difficulty of solving residuosity and discrete logarithm problem simultaneously. Attacker may also tries to select S and find K. In this case, he calculates $\lambda \equiv w^{S^2} \cdot V^{-h(m)} (\mathrm{mod}\, p)$ and try to solve $\lambda \equiv K^K (\mathrm{mod}\, p)$. This is worse scenario, because even if he can solve residuosity and discrete logarithm problems, the value of K is still hard to find.

(v) Suppose that residuosity problem is breakable, means the attacker knows the prime factorization of n, which is P and Q. Unfortunately, he still cannot obtain S^2 from $\gamma \equiv w^{S^2} (\mathrm{mod}\, p)$ due to discrete logarithm problems and thus fail to generate S.

(vi) Let us assume discrete logarithm problem is breakable, means the attacker knows S^2. However, he still cannot find S due to the difficulty of solving residuosity problem.

Performance Evaluation

In this section, we investigate the performance of our scheme in terms of number of keys, computational complexity, and size of parameters. We use the following notation to analyze the performance of the scheme:

- SK and PK are the number of secret and public keys respectively.
- T_{exp} is the time complexity for executing the modular exponentiation computation.
- T_{mul} is the time complexity for executing the modular multiplication computation.
- T_{inv} is the time complexity for executing the modular inverse computation.
- T_{sq} is the time complexity for executing the modular square computation.
- T_{sqrt} is the complexity for executing the modular square root computation.
- T_h is the time complexity for performing hash function.
- $|\eta|$ denotes the bit length of η.

The performance of our scheme is listed in Table 2.

Table 2 : The performance of our threshold signature scheme.

		Our scheme
No of keys	SK	$t+2$
	PK	$t+2$
Computational complexity	Sign	$(4t)\,T_{exp} + (3t^2 + t + 1)\,T_{mul} + (t^2 - t + 1)\,T_{inv} + T_{sq} + T_{sqrt} + T_h$
	Verify	$3\,T_{exp} + T_{mul} + T_{sq}$
Size of parameters / communication cost		$(2t+1)\|n\| + (3t+1)\|p\|$

Conclusion

In this paper, we proposed a new threshold digital signature scheme based on two problems in cryptography; residuosity and discrete logarithms. Beside the scheme, we show that the system that has being developed is secure against some attacks. We also show the system only requires a reasonable time complexity in both signing and verifying phases.

Acknowledgement

The second author acknowledges the financial support received from the Universiti Kebangsaan Malaysia under research grant UKM-DLP-2011-208.

References:

Desmedt, Y. (1988). Society and group oriented cryptography: a new concept. *Advances in Cryptology, Proceedings of Crypto '87*, 120-127.

Desmedt, Y. and Frankel, Y. (1989). Threshold cryptosystem. *Advances in Cryptology, Proceedings of Crypto '89*, 307-315.

Desmedt, Y. and Frankel, Y. (1991). Shared generation of authenticators. *Advances in Cryptology, Proceedings of Crypto '91*, 457-469.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transaction on Information Theory*, IT-31(4), 469-472.

Harn, L. (1994). Group oriented (*t,n*) threshold digital signature scheme and digital multisignature. *IEE Proceedings-Computers and Digital Techniques*, 141(5), 307-313.

He, W. (2001). Electronic signature scheme based on residuosity and discrete logarithms. *Electronic Letters*, 37(4), 220-222.

Laih, C. S. and Kuo, W. C. (1997). New signature scheme based on residuosity and discrete logarithms. *IEICE Transactions on Fundamentals on Cryptography and Information Security E80-A1*, 46-53.

Lee, N. Y. and Hwang, T. (1996). Modified Harn signature scheme based on residuosity and discrete logarithms. *IEE Proceedings-Computers and Electronic Techniques*, 143(3), 196-198.

Rivest, R., Shamir, A. and Adleman, L. (1978). A method for obtaining digital signature and public-key cryptosystem. *Communication of the ACM*, 21(2), 120-126.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, 22(11), 612-613.

Wang, C. T. and Chang, C. C. (2003). Signature scheme based on two hard problems simultaneously. *Proceeding of the 17th International Conference on Advanced Information Networking and Application*, 557-560.

PROTECTION OF TEXTS USING SHA1 AND BASE64

[1]Mohammad A. Ahmad, [1]Imad Alshaikhli and [2]Hanady Mohammad Ahmad
[1]*Department of Computer Science, International Islamic University of Malaysia, 53100 Jalan Gombak Kuala Lumpur, Malaysia*
[2]*Department of Computer, Basic Education College, Public Authority of Applied Education and Training, 34053 Alshamiya, Kuwait,*
malahmads@yahoo.com, imadyaseen39@yahoo.com, hanadym.1359@windowslive.com

Abstract:

Protection of information is a prerequisite demand in the world of computers today. Protection of information can be accomplished in different methods. The main objective of the use of the protection of information is to protect data and information in order to achieve privacy. This paper discusses two methods of protection of information, an encryption method called Base64, which is a set of encoding schemes that convert the same binary data to the form of a series of ASCII code. Also, The SHA1 hash function is used to hash the encrypted file performed by Base64. As an example of an ASCII code, Arabic letters are used to represent the texts. So using the two protection methods together will increase the security level for protecting the data.

Keywords: Encryption, Hash, Base64, SHA1

Introduction

Protection of information is a prerequisite demand in the world of computers today. Protection of information can be accomplished in different methods. The main objective of the use of the protection of information is to protect data and information in order to achieve privacy. The encryption process combines mathematics and computer science. Cryptography consists of a set of algorithms and techniques to convert the data into another form so that the contents are unreadable and unexplainable to anyone who does not have the authority to read or write on these data. The main objective of the use of encryption algorithms is to protect data and information in order to achieve privacy. The protection mechanism choices are applied based on the data sensitivity. For example, the data bank "ex, clients accounts" needs to be protected by latest security and protection mechanisms. In fact, with the available tools for intrusion in the internet today, computer intruders can hack to secure systems easily. Consequently, combining more than one protection mechanisms is so crucial to achieve the highest level security against intruders. (Imad F. Alshaikhli, 2011)

There are several functions for the protection processes to protect the information and files from intrusion. It is possible to employ encryption in various fields. In this paper, an encryption method is presented to protect the texts. One way to protect the texts from changes is by encryption. This paper will explain the method of encryption using Base64. The first step of the encryption method using Base64 is to convert text to unreadable text and create the ASCII for each character and convert it to a binary number. Then we convert the binary number to a decimal number and find the character that corresponds to the decimal number, and in so doing, the text will be rendered incomprehensible by the encryption process. Also, Secure Hash Algorithm "SHA1" is used as protection mechanism associated with Base64 encryption method. SHA1 is an algorithm that is used to verify data integrity through the creation of a 160-bit from data input (which may be a message of any length); the product is claimed to be as unique to that specific data as a fingerprint is to the specific individual. (Rivest, 1992)

SHA1and Base64 are used together to increase the security level of the data that needs protection. The details are explained in this paper.

Proposed System

Computer security is a major challenge for all computer users, and use of encryption protects data and information from modification. Many businessmen, professionals, and home users employ encryption to protect their data and to maintain strict confidentiality. The system proposed in this paper is to encrypt the texts through the use of the Visual Basic program, as well as the use of encryption method of Base64 and hash function SHA1.

The particular choices for the 64 characters required for the base varies between implementations. The general rule is to choose a set of 64 characters that is both part of a subset common to most encodings, and also printable. This combination leaves the data unlikely to be modified in transit through information systems, such

as email, that were traditionally not 8-bit clean.[1] For example, MIME's base64 implementation uses A–Z, a–z, and 0–9 for the first 62 values. Other variations, usually derived from Base64, share this property but differ in the symbols chosen for the last two values; an example is UTF-7.

SHA1 Hash

Definition of SHA1Hash

SHA1 (Secure Hash Algorithm 1) is message-digest algorithm, which takes an input message of any length < 2^64 bits and produces a 160-bit output as the message digest. Based on the SHA1 RFC document, the SHA-1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify. The original specification of the algorithm was published in 1993 as the Secure Hash Standard, FIPS PUB 180, by US government standards agency NIST (National Institute of Standards and Technology). This version is now often referred to as "SHA0". SHA-0 was withdrawn by the NSA shortly after publication and was superseded by the revised version, published in 1995 in FIPS PUB 180-1 and commonly referred to as "SHA1". (D. Eastlake Septemper 2001)

The technique of Hash SHA1

The SHA-1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify. (D. Eastlake Septemper 2001)

Definitions of Bit Strings and Integers

The following terminology related to bit strings and integers will be used:
a. A hex digit is an element of the set {0, 1, ... , 9, A, ... , F}. A hex digit is the representation of a 4-bit string. Examples: 7= 0111, A = 1010.

b. A word equals a 32-bit string which may be represented as a sequence of 8 hex digits. To convert a word to 8 hex digits each 4-bit string is converted to its hex equivalent as described in (a) above. Example:1010 0001 0000 0011 1111 1110 0010 0011 = A103FE23.

c. An integer between 0 and 2^32 - 1 inclusive may be represented as a word. The least significant four bits of the integer arerepresented by the right-most hex digit of the word representation.
Example: the integer 291 = 2^8+2^5+2^1+2^0 =256+32+2+1 is represented by the hex word, 00000123. If z is an integer, 0 <= z < 2^64, then z = (2^32)x + y where 0 <= x < 2^32 and 0 <= y < 2^32. Since x and y can be represented as words X and Y, respectively, z can be represented as the pair of words (X,Y). d. block = 512-bit string. A block (e.g., B) may be represented as a sequence of 16 words. (D. Eastlake Septemper 2001)

Operations on WordThe following logical operators will be applied to words:

a. Bitwise logical word operations
X AND Y = bitwise logical "and" of X and Y.
X OR Y = bitwise logical "inclusive-or" of X and Y.
X XOR Y = bitwise logical "exclusive-or" of X and Y.
NOT X = bitwise logical "complement" of X.

Example:

```
        01101100101110011110100100111110
XOR     01100101110000010110100110110111
        --------------------------------
    =   00001001011110001011101111001100
```

b. The operation X + Y is defined as follows: words X and Y represent integers x and y, where $0 <= x < 2^{32}$ and $0 <= y < 2^{32}$. For positive integer's n and m, let n mod m be the remainder upon dividing n by m. Compute $z = (x + y) \bmod 2^{32}$. Then $0 <= z < 2^{32}$. Convert z to a word, Z, and define Z = X +Y.

c. The circular left shift operation $S^n(X)$, where X is a word and n is an integer with $0 <= n < 32$, is defined by $S^n(X) = (X << n) \text{ OR } (X >> 32-n)$.
In the above, X << n is obtained as follows: discard the left-most n bits of X and then pad the result with n zeroes on the right (the result will still be 32 bits). X >> n is obtained by discarding the right-most n bits of X and then padding the result with n zeroes on the left. Thus $S^n(X)$ is equivalent to a circular shift of X by n positions to the left. (D. Eastlake September 2001)

Message Padding

SHA-1 is used to compute a message digest for a message or data file that is provided as input. The message or data file should be considered to be a bit string. The length of the message is the number of bits in the message (the empty message has length 0). If the number of bits in a message is a multiple of 8, for compactness. we can represent the message in hex. The purpose of message padding is to make the total length of a padded message a multiple of 512. SHA-1 sequentially processes blocks of 512 bits when computing the message digest. The following specifies how this padding shall be performed. As a summary, a "1" followed by m "0"s followed by a 64-bit integer are appended to the end of the message to produce a padded message of length 512 * n. The 64-bit integer is the length of the original message. The padded message is then processed by the SHA-1 as n 512-bit blocks. (D. Eastlake Septemper 2001)

- Suppose a message has length $l < 2^{64}$. Before it is input to the SHA-1, the message is padded on the right as follows:

a. "1" is appended. Example: if the original message is "01010000", this is padded to "010100001".

b. "0"s are appended. The number of "0"s will depend on the original length of the message. The last 64 bits of the last 512-bit block are reserved for the length l of the original message.

Example: Suppose the original message is the bit string

01100001 01100010 01100011 01100100 01100101.

After step (a) this gives

01100001 01100010 01100011 01100100 01100101 1.

Since l = 40, the number of bits in the above is 41 and 407 "0"s are appended, making the total now 448. This gives (in hex)

61626364 65800000 00000000 00000000

00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000

00000000 00000000.

c. Obtain the 2-word representation of l, the number of bits in the original message. If $l < 2^{32}$ then the first word is all zeroes. Append these two words to the padded message.

Example: Suppose the original message is as in (b). Then l = 40 (note that l is computed before any padding). The two-word representation of 40 is hex 00000000 00000028. Hence the final padded message is hex

61626364 65800000 00000000 00000000

00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000028.

The padded message will contain 16 * n words for some n > 0. The padded message is regarded as a sequence of n blocks M(1) , M(2), first characters (or bits) of the message. (D. Eastlake Septemper 2001)

The technique of Base64

The Base64 method is used to protect the text and files from changes and that is discussed in this paper (Baccala, 1997). The Base64 method involves finding all the ASCII characters, converting them to binary numbers, and then dividing the binary number for the text to 6 bits and converting them to their corresponding values in Base64.

Base64 Mechanism

To encrypt this line using Base64:
الحمدلله رب العالمين -
1. First find the ASCII code for each character.

Letter	ASCII
ا	199
ل	225
ح	205

2. Second, convert the ASCII number of the characters to a binary number.

Letter	ASCII	Binary
ا	199	11000111
ل	225	11100001
ح	205	11001101

3. Third, divide the Binary number to parts and identify a number of bits so that the total is less than or equal to 64 bits. In this example, the Binary number divided to 6-bit.

Letter	ASCII	Binary	Divided binary
ا	199	11000111	11000111
ل	225	11100001	11100001
ح	205	11001101	11001101

4. Fourth, convert parts of the binary number, which has been divided into a decimal number.

Letter	Divided binary	Index
ا	110001	49
ل	111110	62
ح	000111	7
م	001101	13

5. Next, find the character (Char) that corresponds to the number (Value) in the Index Table below.

Index Table

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Letter	Divided binary	Index	Base64-encoded
ا	110001	49	x
ل	111110	62	+
ح	000111	7	H
م	001101	13	N

6. Then perform the encryption for the letters.

Letter	Base64-encoded
ا	x
ل	+
ح	H
م	N

x+HN ← الح

The Steps of Encrypting the Text

Letter	Ascii	Binary	Divided binary	Index	Base64-encoded
ا	199	11000111	110001	49	x
ل	225	11100001	111110	62	+
ح	205	11001101	000111	7	H
م	227	11100011	001101	13	N
د	207	11001111	111000	56	4
ل	225	11100001	111100	60	8
ل	225	11100001	111111	63	/
ه	229	11100101	100001	33	h
" "	32	00100000	111000	56	4
ر	209	11010001	011110	30	e
ب	200	11001000	010100	20	U
" "	32	00100000	100000	32	g

ا	199	11000111	110100	52	0
ل	225	11100001	011100	28	C
ع	218	11011010	100000	32	G
ا	199	11000111	100000	32	G
ل	225	11100001	110001	49	X
م	227	11100011	111110	62	+
ي	237	11101101	000111	7	H
ن	228	11100100	011010	26	A
			110001	49	X
			111110	62	+
			000111	7	H
			100011	35	J
			111011	59	7
			011110	30	E
			010000	16	Q

Conclusion and Future Work

This paper presented two methods of protection, Base64 encryption and Secure Hash Algorithm 1 function to protect the text from being changed. The most important points raised by the paper include:

1. Use of a Base64 encryption method to protect of the texts from modification. This relies on finding the ASCII for each character, converting them to binary numbers, then dividing them into a number of bits and converting them to their corresponding values in Base64.
2. Use of the Visual Basic program for the application program.
3. Use of SHA1 hash function for more security so that each file has its own hash number. When any change occurs in the files, it will change the original hash number and the user will know the file is compromised.

In the future, the protection mechanisms algorithms will be developed. The developed algorithms will be applied and used to protect the electronic Holy Quran from being tampered, changed or modified. More precisely, this paper is the first stage of other series of papers that will lead to a complete project of protecting the different formats of the electronic Holy Quran.

References:

Binark, I., Eren, H., & İhsanoğlu, E. (1986). World bibliography of translations of the meanings of the Holy Qur'an: printed translations, 1515-1980 (Vol. 1): Research Centre for Islamic History, Art, and Culture.

Blaze, M., & Keromytis, A. D. (2000). DSA and RSA key and signature encoding for the KeyNote trust management system.

D. Eastlake, P. J. (Septemper 2001). "Secure Hash Function 1." Network Working Group 10 pages. definition SHA1. (2011, march 12). retrieved from http://searchsecurity.techtarget.com/definition/SHA1 Den Boer, B., & Bosselaers, A. (1994). Collisions for the compression function of MD5.

Imad F. Alshaikhli, M. A. A. (2011). Security Threats of Finger Print Biometric in Network System Environment. [Journal]. Advanced Computer Science and Technology Research, 1(1), 15.

Josefsson, S. (2006). The base16, base32, and base64 data encodings.

Klima, V. (2006). Tunnels in hash functions: SHA1 collisions within a minute.

Morin, R. C. (2001). How to base64.

Quran, H., & Ahmad-UK, F. (1996). Al Islam. The Review of Religions.

Rivest, R. (1992). The SHA1 message-digest algorithm.

Touch, J. D. (1995). Performance analysis of SHA1. ACM SIGCOMM Computer Communication Review, 25(4), 77-86.

Tuszynski, J. (2008). caTools: Tools: moving window statistics, GIF, Base64, ROC AUC, etc. R package version, 1.

Wang, X., & Yu, H. (2005). How to break SHA1 and other hash functions. Advances in Cryptology–EUROCRYPT 2005, 561-561.

http://quran.alahmad.net

POLYNOMIAL BASED KEY DISTRIBUTION SCHEME FOR WPAN

Vimalathithan. R*, D. Rossi†, M. Omaña†, C. Metra† and M.L.Valarmathi‡
*KPR Institute of Engineering and Technology, Coimbatore, India
†University of Bologna, Bologna, Italy
‡Government College of Technology, Coimbatore, India
athivimal@gmail.com

Abstract:

In WPAN the data has to be transmitted in a secured manner, where the security of the data depends upon the Key used for encryption/decryption. A secret key has to be shared among the nodes in order to establish a secure link among the nodes. The secret key should be resilient to attacks. Key distribution technique in WSN is a challenging task. In this paper, a polynomial based Key distribution scheme is proposed for secure communication protocol. The node capture impact (NCI) for the proposed scheme is compared with other existing scheme. The proposed scheme features an NCI equal to zero for even any number of nodes that are compromised, which is recommended characteristic of a key distribution scheme.

Introduction

Sensor nodes are battery operated devices, usually small in size with an inbuilt low power RF transreceiver which can be capable of transmitting (receive) data within (from) a small range. The valuable datas are transmitted in free space and have to be secured. Hence the cryptography is applied for secure transmission. For secure transmission, a secret key is to be shared among the sender and receiver. Usually this secret key is distributed among the sender and receiver by a trusted third party (Key Distribution centre).

An effective key management system is important in the WSN environment as it reduces the communication overheads of sensor nodes. This in turn reduces the battery consumption and increases the life span of such devices. There are numerous key distribution schemes [2-5]. Public key cryptography mechanism is one among them and well suited for key distribution. But public key cryptography requires a large number of mathematical computations. As previously mentioned, the nodes have limited amount of energy since they are battery operated, and using public key cryptography mechanism the nodes consume a lot of energy in order to perform mathematical computations, thus not being suitable for WPANs. On the other hand, Private-key cryptography is suited for WPANs due to its low energy requirements [5]. Key distribution is usually done off-line before deployment of nodes. Once the nodes are placed, they can communicate each other and compute a common key for highly secured data exchange among the nodes.

In case of IEEE 802.15.4, the key used for encryption /decryption is stored in memory of each nodes and can be identified at the time of requirement, by the key identifier mode in the security control filed and key lookup table [0]. In this case, the nodes can use only a set of predefined keys. If the number of nodes is increased, then a large number of keys have to be stored in the memory, which requires more memory space and key accessing time. Moreover, the key used for data traffic must be periodically refreshed, in order to prevent the antagonist from acquiring the information about key. This may take long and time consuming sequence of procedures. Finally, a further threat to network security comes from the fact that, since the nodes are placed in unmanned environment, there is a possibility of node capture by an antagonist. Node Capture is one type of attack in sensor networks, where an antagonist can acquire the node and have control over the entire node by accessing information stored in the memory. Even a single captured node can imperil the entire network thereby the entire key is known to the antagonist. NCI gives the information about the number of nodes to be attacked by antagonist to imperil the entire network.

B.Maala et.al [0] analyzed the Key management schemes for heterogeneous networks, derived the NCI and analyzed for Asymmetric Pre-distribution key management (AP), Hierarchical Key Management Protocol for Heterogeneous WSN (HERO), and Two Level Architecture for Key Management Scheme (TLA). From their analysis it can be derived that the secure communication can be broken for AP scheme if 30% of sensor nodes are compromised; for HERO scheme, if 70% of nodes are compromised then the secure communication can be broken. In case of TLA, if 100% of sensor node is captured then the NCI is only 10%. Here we have proved that our proposed Polynomial based key distribution scheme have even less NCI when compared to NCI for TLA.

Rossi et.al [0] has developed a secure communication protocol for WPAN. In the protocol in [6], message integrity and authenticity are guaranteed by a Message Authentication Code (MAC), similarly to the standard IEEE 802.13.4. Instead, as for message freshness, in [6] authors propose to provide it by using a technique based on rolling code (RC) instead of simple frame counter as in IEEE 802.13.4. In this paper, a polynomial based key distribution scheme is proposed to improve the security of communication protocol used in WPAN. Also the proposed scheme can be used for other WPAN where high security is required even after the nodes get compromised.
The rest of the paper is organized as follows: Section 2 describes the Key generation technique using linear feedback shift register, while our proposed polynomial based Key distribution scheme is explained in Section 3. Node Capture Impact is derived in Section 4 for the proposed key distribution scheme and is compared with that of alternative solutions. Section 5 concludes our paper.

Key generation with Linear Feedback Shift registers (LFSRs)

In our proposed approach, a linear feedback shift registers (LFSR) is employed to generate 128 bit key used for AES encryption. Feedback shift registers contains a Shift registers in the forward path and a linear function in the feedback path. The simplest form of feedback shift register is linear feedback shift registers (LFSRs) that, when clocked, shifts the data through the register from one bit to the next most-significant bit [0-11]. LFSR is used as keystream generators, Design for Test (DFT), Built in Self-Test design (BIST) and in wireless communication systems employing spread spectrum techniques. Moreover, strong cryptographic binary sequences can be produced using LFSRs, and the produced sequence can have a large period if the polynomial used to build-up the LFSR is primitive (if all its coefficients are relatively prime). LFSRs can be implemented both in hardware and software: the main advantages of hardware LFSRs are that they are faster and easy to implement, since the hardware uses simple XOR gates and summation [12].

An LFSR of length L consists of L flip-flops each capable of storing one bit and having one input and one output. A common clock is used to control the shifting of data stored in each FF. As an example, let us consider a simple LFSR as shown in Figure 1. For each clock pulse, a bit in the each shift register is shifted to the right, and the new left-most bit is computed as a function of the other bits in the register as follows:

$$C_L = \sum_{k=0} C_k S_k \quad (1)$$

The output of the register S_0 is the output of the LFSR which is 1 bit for a single clock.

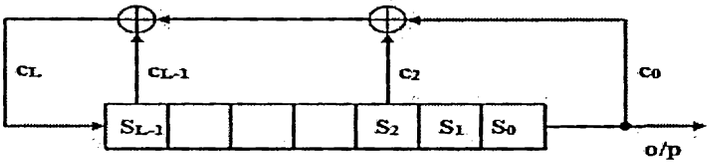


Figure 1 : Linear Feedback Shift Register.

An LFSR is usually denoted by <L, C(D)>, where C (D) = $1+c_1D+c_2D^2+c_3D^3+ \ldots +c_LD^L$. The parameter L is the number of FSR or the order of the polynomial, D^i is the content of register S_i, and the connection to the feedback position is defined by the power of D in the polynomial.

Starting from the XOR (XNOR) gates, shift registers and properly selected coefficients c_i in C(D) (provided c_0 and c_L always takes the value one), a pseudorandom binary sequence with large period 2^L-1 can be generated. The pattern with all zeros is excluded in order to avoid the system get stuck into the same all zeros sequence. (in case if XNOR gates are used in the feedback, all ones must be excluded). An LFSR is said to be Non-singular if C_L=1 i.e., C(D) is of order L. As already said if C(D) is primitive then maximum period sequence can be obtained. Also the reciprocal of a primitive polynomial C(D) is primitive, which is denoted by $C^*(D)$ and reciprocal of Non-Primitive Polynomial is also Non-Primitive.

A polynomial C(D) is said to be reciprocal iff: $C^*(D) = D^L . C(1/D)$.
There is no reciprocal for a primitive polynomial with L=2 and 3, since the polynomial and its reciprocal are the same. The sequence produced by the LFSR that uses reciprocal polynomial is in reverse order and LFSR using

reciprocal polynomial is called reverse order Pseudo Random Binary sequence Generator PRBG. The sequence generated by LFSR is used as key for encryption and decryption.

Polynomial Based Key Distribution Scheme

Here we propose a polynomial based key distribution scheme for secured communication protocol. Figure 2 and figure 3 show the transmitter protocol and receiver protocol. The transmitter id, receiver id, RC sequence (employed to guarantee message freshness) and useful message, transmitted in clear text, are encrypted using AES to generate the MAC (employed to guarantee message integrity and authentication). The numbers shown in each block represent the corresponding bit size. The RC sequence is generated using Non-Linear Feedback Shift Register (NLFSR), which is more robust than LFSR against cryptanalysis. A set of Primitive polynomial [13] is stored in all the nodes and the information about the polynomials stored in each node must be shared with the Master node. Whenever a Master wants to communicate with a particular node, it has to send two components: one component is the information about the seed of the NLFSR, which is determined from the RC sequence and the second component is the polynomial identifier, which is determined from the two least significant bit of RC. It should be noted that Master node does not require any extra bits to identify these parameters, which instead can be derive from the RC sequence, thereby reducing the transmission time, power and computational time. The seed is generated using 16-128 bit expansion algorithm (copies 16bit RC eight times to generate 128 bit). Using a simple hardware and minimum number of polynomials, a large number of keys can be generated by simply varying the seed. The key is generated using 128bit LFSR (Galois Type). For each and every communication the seed and primitive polynomial is varied, hence a variety of key can be generated using simple hardware. Using 128 bit LFSR, 2^{128}-1 sequences can be generated. A system operating at 100GHz would require 10^{12} years to circulate all possible sequences. Since different keys were used for each transmission, the number of encrypted data available in free space (channel) for an attacker (for cryptanalysis) is considerably smaller than the other schemes with shared keys for all nodes, thus making the proposed solution highly secure against attacking.

At the receiver side, the data received are encrypted using AES to generate MAC and compared with the received MAC. If they are equal then the receiver validates the received message. To generate the key at the receiver, RC is used as input for expansion algorithm to generate the seed for LFSR. The 128bit key generated by LFSR is used by AES encryption algorithm to generate the MAC for validation. In this case even if a node gets compromised, only the polynomial coefficient is accessed by the antagonist. Since the seed value is changed for each transmission (encryption/decryption), the key used for each transmission will be different. This is equivalent to one key per transmission, which provides high level of security. In fact, the difficulties usually encountered to exchange one key for each transmission, are elegantly solved by using polynomial based key distribution.

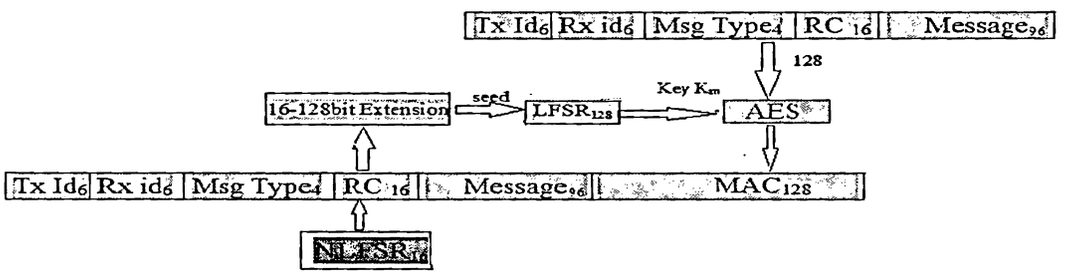


Figure 2 : Transmitter Protocol

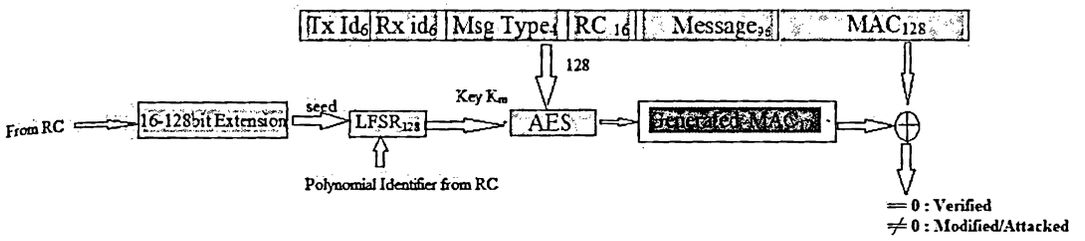


Figure 3 : Receiver Protocol

Node Capture Impact Evaluation

In a wireless Personal Area Network (WPAN), usually the nodes are placed in an unmanned environment. It is unavoidable to prevent the attacker to hack these unmanned nodes. Once the node is captured (compromised), the antagonist may try to access the memory in the node with ultimate goal to find out the keys stored in the node, in order to hear the future communication amongst the non-compromised (con-captured) nodes.

Here we derive the Node Capture Impact factor for our proposed key distribution scheme and compared it with TLA scheme. An attacker may attack the network through compromising one or more sensor nodes which may be super node or normal node. Usually the super node is highly secure and tamper resistant to such attacks. Hence we assume that the attacker can hack only normal nodes.

Suppose that the key pool is $\chi = \{K_1,K_2,K_3,K_4,K_5,K_6,K_7,K_8\}$ and the number of keys stored in each node is $\sigma = 2$; we assume that the nodes a, b and c store the keys $\{K_1,K_2\} = \sigma_a$, $\{K_3,K_4\} = \sigma_b$ and $\{K_5,K_6\} = \sigma_c$, respectively. Each set of keys stored in a node is called key ring. In this case the key rings are independent, because there is no common element between any two nodes, that is: $\sigma_a \cap \sigma_b = \sigma_a \cap \sigma_c = \sigma_b \cap \sigma_c = \{\emptyset\}$. This type of key rings are called independent key rings. Instead, if at least one common key is found between any subset of key ring (as it is usually the case in normal sensor nodes) then the corresponding key ring is called dependent key ring. For example if a, b and c store the keys $\{K_1, K_2\} = \sigma_a$, $\{K_2, K_4\} = \sigma_b$ and $\{K_1,K_4\} = \sigma_c$, respectively. In this case it is $\sigma_a \cap \sigma_b = \{K_2\}$, $\sigma_a \cap \sigma_c = \{K_4\}$ and $\sigma_b \cap \sigma_c = \{K_1\}$.
Let us assume that each normal node stores σ keys, and let χ be the total number of keys in the pool. Let us consider also the following notation:

- λ_1 is the event that the key rings of the compromised nodes are independent.
- λ_2 is the event that the key rings of the compromised nodes are non-independent.
- P_1 is the probability of the total number of compromised keys when the key rings of the compromised nodes are independent. Then, $P_1 = \text{Prob}(\lambda_1)$.
- P_2 is the probability of the total number of compromised keys when the key rings of the compromised nodes are non-independent. Then, $P_2 = \text{Prob}(\lambda_2)$.

Therefore, the Node Capture Impact is [4]:

$$\text{NCI} = P_1 + P_2 \tag{2}$$

The probabilities P_1 and P_2 are calculated as described in the next paragraphs.
The probability that a key belongs to a particular node N_n is σ/χ, while the probability that a key does not belong to a particular node N_n is $1 - (\sigma/\chi)$.
Considering C_P compromised nodes, the probability that a key does not belong to a compromised node is:

$$x_1 = \left(1 - \frac{\sigma}{\chi}\right)^{C_P} \tag{3}$$

Therefore, the probability of the total number of compromised keys when all key rings are independent is:

$$P_1 = 1 - x_1,$$

while the probability of the total number of compromised keys if all key rings are not independent is:

$$P_2 = \left[1-\left(1-\frac{\sigma}{\chi}\right)^{Cp}\right] * \sum_{j=2}^{Cp}\sum_{i=1}^{\sigma} P(i,j) \tag{4}$$

where j ϵ [2,c] is the number of compromised N_n normal sensor nodes and *P(i,j)* is the probability of having i ϵ [1, σ] shared keys between any j compromised N_n sensor nodes. It is:

$$P(i,j) = \frac{(\chi!)^{(1-j)} * (\sigma!(\chi-\sigma)!)^j}{i!*(\chi-i-j*(\sigma-i))!*(\sigma-i)!*(j*(\sigma-i)-\sigma+i)!} \tag{5}$$

From these equations we can derive NCI as:

$$\mathrm{NCI} = P_1 + P_2 = \left[1-\left(1-\frac{\sigma}{\chi}\right)^{Cp}\right] * \left[1+\sum_{j=2}^{Cp}\sum_{i=1}^{\sigma} P(i,j)\right] \tag{6}$$

For TLA, the number of keys stored in each node is σ=1 (therefore i =1). Hence: $P(1,j)=\chi^{1-j}$. Therefore, the NCI for the TLA solution is:

$$\mathrm{NCI}_{TLA} = \left[1-\left(1-\frac{\sigma}{\chi}\right)^{Cp}\right] * \left[1+\sum_{j=2}^{Cp}(\chi)^{1-j}\right] \tag{7}$$

Instead, for the proposed Polynomial based Key Distribution scheme (*Poly*), the number of keys stored in each node is σ=0 (therefore i =0). Therefore, the NCI turns out to be:

$$\mathrm{NCI}_{poly} = 0. \tag{8}$$

Figure 4 shows the plot of NCI for TLA and Polynomial based scheme. From the figure it is observed that, for TLA, the NCI increases as the number of capture node increases, whereas in our case, the NCI is zero for any number of captured nodes. This confirms that polynomial based Key Distribution scheme can be effectively used for key distribution among the nodes.

Conclusions

A polynomial based key distribution scheme is proposed for WPAN. From the Node Capture Impact analysis, we found that, differently from alternative solutions, for the proposed scheme NCI is zero independently of the number of nodes that are captured or compromised. Hence the node can be placed in any environment, even in unsecured environment. Also the number of nodes is scalable; therefore any number of nodes can be introduced in the network without increasing the memory capacity. This proposed key distribution scheme provides high level of security and is suitable for WPAN.

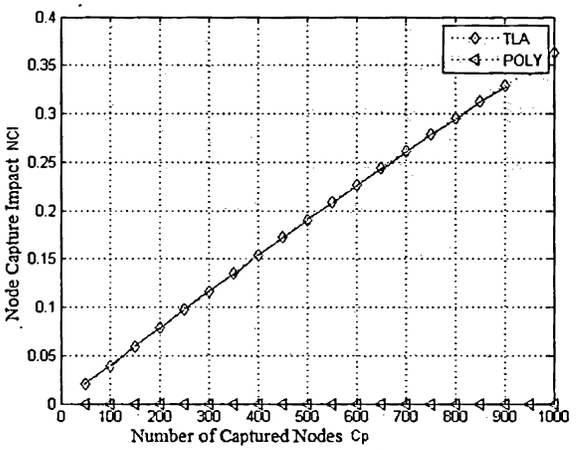


Figure 4 : Node capture Impact (NCI) for TLA and Polynomial based key distribution.

References:

IEEE Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements .IEEE Std 802.15.4™-2006.

X. Du, Y. Xiao, M. Guizani, and H.H (2007). Chen, "An Effective Key Management Scheme for Heterogeneous Sensor Networks," *Ad Hoc Networks*, vol. 5, no. 1, pp. 24-34.

Z.Liu, "Asymmetric Key Pre-Distribution Scheme for Sensor Networks," *IEEE Transactions on Wireless Communication*, Vol.8 , No.3 Mar 2009, pp. 1366-1372.

B. Maala, H. Bettahar and A. Bouabdallah, "TLA: A Tow Level Architecture for Key Management in Wireless Sensor Networks," in *Proceeding of IEEE Sensor Comm 2008*, Cap Esterel, France, August 2008, pp. 639-644.

Yee Wei Law and Marimuthu Palaniswami, "Key Management in Wireless Sensor Networks", Guide to Wireless sensor networks, Computer Communications and Networks, pp. 513-531, Springer-Verlag London Limited 2009.

D.Rossi, M.Omaña, D.Giaffreda, C.Metra, "Secure Communication Protocol for wireless Networks", *IEEE East-West Design and Test Symposium 2010.*

William Stallings, Cryptography and Network Security Principles and Practices, Pearson Education, 2004.
Behrouz A. Forouzan, Cryptography and Network Security, Tata McGraw hill Education, 2nd edition 2008.

Kencheng Zeng, Chung-Huang Yang, Dah-Yea Wei, and T.R.N. Rao, "Psuedorandom Bit generators in Stream cipher Cryptography," *IEEE Computer*, Feb 1991, pp. 8-17.

Shun-lung Su, Ko-ming Chiu, Lih-chyau Wuu, "The Cryptanalysis of LFSR/FCSR Based Alternating Step Generator", Proc. of *The 2006 IEEE International Conference on Computer Engineering and Systems*, 2006, pp. 228-231.

A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

W.Ling, L.Jing, "A Cryptographic Algorithm Based on Linear Feedback Shift Register", *Proc. of IEEE International Conf. on Computer Application and System Modeling*, ,2010, pp. 526-529.

http://theory.cs.uvic.ca/inf/neck/PolyInfo.html.

KEY EXCHANGE FOR NEW CRYPTOSYSTEM ANALOGOUS TO LUCELG AND CRAMER-SHOUP

[1]Norliana Muslim and [2]Mohamad Rushdan Md. Said
[1]*Asia Pacific University College of Technology and Innovation,Technology Park Malaysia, Bukit Jalil 57000, Kuala Lumpur, Malaysia*
[2]*Institute for Mathematical Research, Universiti Putra Malaysia,43400 UPM Serdang, Selangor, Malaysia*
norliana@ucti.edu.my, rushdan@math.upm.edu.my

Abstract:

Key exchange or key establishment is any process in cryptography by which users are able to share or exchange a secret key. The problem on the key exchange is how to exchange any keys or information so that no third party can obtain a copy. This paper will discuss the key exchange for new cryptosystem analogous to LUCELG and Cramer-Shoup that have been proposed by the same author in 2009. In the analog cryptosystem, the encryption and decryption algorithm are based on the defined Lucas function and its security have been proved that is polynomial time equivalent to the generalized discrete logarithm problems. Hence, one protocol will be proposed to provide the key establishment. Basically the protocol uses the second order linear recurrence relation and the multiplicative group of integers modulo p. In the protocol, the third party will not be able to alter the contents of communication between three parties.

Keywords: Key exchange, key establishment, protocol, analogous LUCELG and Cramer-Shoup

Introduction

The new variant cryptosystem of LUCELG (ElGamal, 1985) and Cramer-Shoup (Cramer and Shoup, 1998) was proposed by utilize the second order linear recurrence relation as cryptographic keys. In both encryption and decryption process, the Lucas cipher was derived as $V_n(P,Q) \bmod p$ (Muslim and Md. Said, 2009).

Back to the year 1976, the Diffie-Hellman algorithm provides a method to securely exchange the keys that encrypt information by creating a shared secret key (Hellman, 1976). The process starts when two parties generates a private key, continue by determine the public key and then exchange the keys. At the end of the process, both parties has same key. In this present paper, we propose a cryptographic protocol for the variant cryptosystem by showing the corresponding process between Ali, Borhan and Eka. The idea for the key agreement protocol for cryptosystem analogous to LUCELG and Cramer-Shoup is derived from the following key exchange figure:

Ali	Eka	Borhan
Ali and Borhan agree to exchange keys:	Eka can sees: P_1, P_2, prime number p, $Q=1$	Borhan and Ali agree to exchange keys:
Ali generates one secret key, k and α then calculate u_1, u_2, e and v		Borhan generates five secret keys (x_1, x_2, y_1, y_2, z) then calculate c, d and h
Ali and Borhan exchange keys		
Ali receives c, d and h	Eka can see the value of c, d, h, u_1, u_2, e and v	Borhan receives u_1, u_2, e and v
Ali determined common shared key, s		Borhan determined common shared key, s

Figure 1 : Key Exchange for Variant Cryptosystem

Key Agreement Protocol for Variant Cryptosystem

Definition 1 (Menezes et al., 1996)

A cryptographic protocol is a distributed algorithm defined by a sequence of steps precisely specifying the actions required of two or more entities to achieve a specific security objective.

Now, let say there are three parties between Ali, Borhan and eavesdropper Eka. The guys Ali and Borhan have chosen the variant encryption scheme to use in communicating over an unsecured channel. To encrypt messages, they require a key and the communication protocol is proposed as the following:

1. Ali and Borhan agree to use prime number $p = 7, P_1 = 2, P_2 = 3$ and $Q = 1$.
2. Borhan chooses secret key $(x_1, x_2, y_1, y_2, z) \in F_{p^2}^*$ that are $(2,3,3,2,3) \in F_{7^2}^*$, then sends his public keys c, d and h to Ali such that

$$c \equiv V_{x_1}(P_1,1) \cdot V_{x_2}(P_2,1) \bmod p \equiv V_2(2,1) \cdot V_3(3,1) \bmod 7 \equiv 2 \cdot 4 \bmod 7 \equiv 1 \bmod 7$$
$$d \equiv V_{y_1}(P_1,1) \cdot V_{y_2}(P_2,1) \equiv V_3(2,1) \cdot V_2(3,1) \bmod 7 \equiv 2 \cdot 7 \bmod 7 \equiv 0 \bmod 7$$
$$h \equiv V_z(P_1,1) \bmod p \equiv V_3(2,1) \bmod 7 \equiv 2 \bmod 7$$

3. Ali generates a key for the variant encryption scheme by chooses a secret key $k = 2$.
4. Ali encrypts the key u_1, u_2, e and v using Borhan's public key and sends the encrypted key to Borhan. The encrypted process are:

$$u_1 \equiv V_k(P_1,1) \bmod p \equiv V_2(2,1) \bmod 7 \equiv 2 \bmod 7$$
$$u_2 \equiv V_k(P_2,1) \bmod p \equiv V_2(3,1) \bmod 7 \equiv 0 \bmod 7$$
$$G \equiv V_k(h,1) \bmod p \equiv V_2(2,1) \bmod 7 \equiv 2 \bmod 7$$
$$e \equiv G \cdot m \bmod p \equiv 2 \cdot 5 \bmod 7 \equiv 3 \bmod 7$$
$$\alpha = H(u_1, u_2, e) = 2$$
$$v \equiv V_k(c,1) \cdot V_{k\alpha}(d,1) \bmod p \equiv V_2(1,1) \cdot V_4(0,1) \bmod 7 \equiv 6 \cdot 2 \bmod 7 \equiv 5 \bmod 7$$

5. Borhan decrypts using his private key and recovers the secret key by calculating

$$s \equiv e \cdot V_z(u_1,1)^{-1} \bmod p \equiv 3 \cdot V_3(2,1)^{-1} \bmod 7 \equiv 3 \cdot 2^{-1} \bmod 7 \equiv 5 \bmod 7$$

6. Ali and Borhan begin communicating with privacy and now share a common secret key s.

Both Ali and Borhan have reached at the same value because $V_k(c,1) \cdot V_{k\alpha}(d,1) \bmod p$ and $e \cdot V_z(u_1,1)^{-1} \bmod p$ are equal. In the protocol, only $(2,3,3,2,3) \in F_{7^2}^*$ and k =2 are kept secret. All other values such as $P_1 = 2, P_2 = 3, c = 1, d = 0, h = 2,$ and $F_{7^2}^*$ can be clearly seen by the eavesdropper, Eka. Unfortunately, she is not able to construct any combination to alter the communications in the channel.

The shared secret key now can be used as an encryption key by Ali and Borhan in order to send messages across the same open communications channel. To enhance the security, large numbers of (x_1, x_2, y_1, y_2, z) in the multiplicative group, k and prime number p are needed.

Conclusion

A key agreement protocol for the new cryptosystem analogous to LUCELG and Cramer-Shoup has been defined. Further research can be continued by discussing same protocol for more than two parties or relating the current protocol to other scenarios in key agreement such as password-authenticated or secure remote password protocol.

References:

Cramer, R., and Shoup, V. 1998. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. *CRYPTO'98, LNCS* 1462, pp. 13-25.

ElGamal, T. 1985. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transaction on Information Theory*, 31(1985): 469-472.

Hellman, D. W. 1976. New directions in cryptography. *IEEE Transaction on Information Theory*, 22(6): 644-654.

Menezes, P., Oorschot, P., and Vanstone, S. 1996. Handbook of Applied Cryptography. CRC Press. 33-35

Muslim, N., and Md. Said, M. R. 2009. A new cryptosystem analogous to Lucelg and Cramer-Shoup. International Journal of Cryptology Research, 1(2): 191-204.

ELLIPTIC CURVE POINT MULTIPLICATION USING WZOT

Hani Mimi, Azman Samsudin and Shahram Jahani
School of Computer Sciences, Universiti Sains Malaysia, Penang 11800, Malaysia
hani_mimi@yahoo.com, azman@cs.usm.my, jahani2001@yahoo.com

Abstract:

The dominant operation in elliptic curve cryptography schemes is the point multiplication of the form kP. A radix-2 representation of k is called w-NAF if w≥2 and the window values are in the digit set $B = \{\mp 1, \mp 3, \dots, \mp 2^w - 1\}$. ***Researchershave been trying to enhance the EC point multiplication by employing the window methods, such as w-NAF method. ZOT is a new recoding technique that uses different digit set. The left-to-rightproperty is addressed as one of the advantages of ZOT. Moreover, it uses the available memory in more efficient way since you can limit the number of precomputed points. Thus, it is more suitable for limited storage devices.***

Introduction

The hardness, efficiency, and the small key size of Elliptic Curve Cryptography (ECC) are attractive points over other public key methods (William 2006). Elliptic Curve (EC) complexity is based on Elliptic Curve Discrete Logarithm Problem (ECDLP) which is considered exponential(Darrel, Alfred et al. 2003; Eisentrager, Lauter et al. 2003). It can be seen that ECC is more suitable than other public key cryptosystem for limited processing power devices (Tsaur and Chou 2005). Elliptic curve operations are defined over finite fields, such as prime or binary (Darrel, Alfred et al. 2003), where prime fields are more suitable than binary fields for software implementations(William 2006).

Elliptic curve operations canbe improved by many techniques (Mimi, Samsudin et al. to appear 2012). Finding a new recoding method which transforms the exponent k to k'that has lower Hamming weight is one of the techniques that may crucially affect the efficiency of an EC scheme. These recoding methods are classified into window and non-window methods. Non-window methods are out of this research scope. Window methods are considered a generalization of non-window methods (Koyama and Tsuruoka 1993; Blake, Seroussi et al. 1999; Solinas 2000; Moller 2002; Okeya, Schmidt-Samoa et al. 2004; Schmidt-Samoa, Semay et al. 2006).Window methods are used when extra memory is available to store some precomputed values (Darrel, Alfred et al. 2003).It is also of interest to have a left-to-right recoding method since it enhances the efficiency of computing kP due to the fact that there is no need to store the recoded exponent k.

There are three ways for applying window methods: the first one is fixed window method such as the 2^w-ary method. The second method is applying a more dynamic technique over the recoded exponent which is the sliding window method. The third method is converting the exponent k to its window representation before applying the sliding window technique (Okeya, Schmidt-Samoa et al. 2004). Zero runs are skipped while applying window method, therefore only odd window values will be precalculated and stored (Gordon 1998). The number of elements in the precomputed digits set$B = \{1,3, \dots, 2^w - 1\}$ will be decreased if negative digits are included.

Elliptic Curve Arithmetic

The following simplified Weierstrass equation, which is defined over F_{p^c}, can beused to implement an ECC scheme.

$$E: y^2 mod p = (x^3 + ax + b)\, mod p \qquad (1)$$

where , $b, x, y \in F_{p^c}$, $c > 3$, and $\Delta = -16(4a^3 + 27b^2)$

The point at infinityis considered the identity point. The most common method for computing kP is called double and add method (also known the binary method)(Knuth 1997; Darrel, Alfred et al. 2003). If $G = (x_1, y_1)$ and $Q = (x_2, y_2)$are two points on the previous elliptic curve and $G \neq -Q$, then the quantity $R = (x_3, y_3) = G + Q$can be calculated as follows: $x_3 = (\lambda^2 - x_1 - x_2)\, mod p$, and $y_3 = (\lambda(x_1 - x_3) - y_1) mod p$, where $\lambda = \left(\frac{y_2 - y_1}{x_2 - x_1}\right) mod p$if $G \neq Q$ and $\lambda = \left(\frac{3x_1^2 + a}{2y_1}\right) mod p$ if$G = Q$.Single scalar point multiplication kP is the major operation

in ECC, where $k \in I$and $P \in E(F_p)$.As stated earlier, recoding method crucially affect the efficiency of this computation. Window methods are used when extra memory is available to store some precomputed points(Darrel, Alfred et al. 2003; Frey 2006).

Related Work

Window method was firstly proposed by Koyoma and Tsuruoka(Koyama and Tsuruoka 1993). Miyaji et al. proposed a window methods for fixed and random point(Miyaji, Ono et al. 1997). Sliding window method over NAF andwidth w-NAF was introduced by Solinas(Solinas 1997; Solinas 2000). The fractional window method was presented by Moller(Moller 2002). Following were a fewleft-to-right window methods proposed by Okeyaet al. (Okeya, Schmidt-Samoa et al. 2004), Avanzi(Avanzi 2005), Muir and Stinson(Muir and Stinson 2005), and by Khabbazian et al. (Khabbazian, Gulliver et al. 2005). The properties of the proposed methods were either proved in the previous papers or by some other papers. For example, the minimality property of w-fractional window method was proved by Moller (Moller 2004). Some properties of non-sparse optimal singed binary representation and its window method were analyzed by Kong and Li (Kong and Li 2005). Muir and Stinson showed that width w-NAF has a minimal number of nonzero digits (Muir and Stinson 2006).

Sliding window technique can be implemented over signed and unsigned binary where the value of each window is odd. It can also be implemented in both directions. The number of precomputed points is $(\frac{2(2^w-(-1)^w)}{3} - 1) \times \frac{1}{2}$. It follows that the expected running time for the sliding window methods over NAF(k) is $\left[D + \left(\frac{2^{w-1}(-1)^w}{3}\right)A\right] + \frac{n}{w+v(w)}A + nD$ where $v(w) = \frac{4}{3} - \frac{(-1)^w}{3.2^{w-2}}$and $n = \log_2 k$(Darrel, Alfred et al. 2003).

In width w-NAF (see Algorithm 1), window method is combined with NAF representation. The Hamming weight of width w-NAF is $\frac{n}{w+1}$.It is proved by Muir and Stinson that w-NAF has the least Hamming wait among other recoding methods. In addition, they proved that the number of digits of a window signed representation is at most greater than the length of binary representation by one digit (Muir and Stinson 2006). The expected running time of Algorithm 1 is$[D + (2^{w-2} - 1)A] + \left[\frac{n}{w+1}A + nD\right]$(Darrel, Alfred et al. 2003). The number of precomputed values (windows) that should be stored is $\frac{2^{w-1}}{2} = 2^{w-2}$, where the set of precomputed digits is $B = \{\mp 1, \mp 3, \ldots, \mp 2^w - 1\}$. The recoding method is implemented right-to-left while the EC multiplication method is implemented in the reverse order (Solinas 2000). Thus the recoded exponent should be stored which consumes memory, which can be a problem for devices with limited memory.For w>3, it was proved(Blake, Seroussi et al. 1999) that width w-NAF is asymptotically better than sliding window on NAF.

Algorithm 1: w-NAF recoding

Input $k \in I, w \geq 1$
Output $k_{wNAF} = (k_{i-1}, k_{i-2}, \ldots, k_1, k_0)$
$i = 0$
while $k \geq 1$
    if k *is odd* : $k_i = k \bmod 2^w : k = k - k_i$
    else : $k_i = 0$
    $k = k/2 : i = i + 1$
return k_{wNAF}

Proposed Method

A positional and non-redundant ZOT-binary numbering system was proposed by Jahani and Samsudin (Jahani 2009). They aimed to reduce the complexity of big number multiplications by representing the multiplicands using ZOT-binary. The number $k = (\hat{b}_{n-1}, \hat{b}_{n-2}, \ldots, \hat{b}_1, \hat{b}_0)_{ZOT}$of a bit length $m = \log_2 k$is considered a ZOT-binary number if the number of zeros followed a non-zero big-digit $(\hat{b}_i)$ is at least i consecutive zeros. The Hamming weight of ZOT-binary numbering system is $\frac{m}{4.6}$ compared to $\frac{m}{2}$for binary , $\frac{m}{3}$ for NAF and $\frac{m}{w+1}$ for w-NAF(Jahani

2009).Let $k = (\hat{b}_{n-1}, \hat{b}_{m-2}, \dots, \hat{b}_1, \hat{b}_0)_{ZOT}$, where each big-digit $\hat{b}_i = (t_i, g_i)$ is described by the type t_i(big-one or big-two) and the bit-lengthg_i,be the ZOT-binary representation of the positive integer $k_2 = (k_{m-1}, k_{l-2}, \dots, k_1, k_0)_2$. Any positive integer k can be converted to ZOT-binary in both directions and with the property$\log_2 k_{ZOT} \leq \log_2 k_2$.

In this paper, the ZOT-binary numbering system is modified by including a big-zero digits. Given $k_2 = (k_{n-1}, k_{l-2}, \dots, k_1, k_0)_2$, Algorithm 2 is used to convert k_2 to its ZOT form $k_{ZOT} = (\hat{b}_{m-1}, \hat{b}_{m-2}, \dots, \hat{b}_1, \hat{b}_0)$, where $\hat{b}_i = (t_i, g_i)$, g_i is the bit-length of the big-digit, and $t_i \in \{0,1,2\}$. The big-digits, big-zero (Z_i), big-one (O_j) and big-two (T_l) are denoted by 0,1, and 2 respectively. As it can be seen from Algorithm 2, the length of big-zero digits is equal to the length of the zero run and the length of the previous big-digit.

Algorithm 2: ZOT recoding method

$$Input \quad k = \sum_{i=0}^{n-1} k_i 2^i, k_i \in \{0,1\}$$

$Output \quad k_{ZOT} = \{\hat{b}_{m-1}, \hat{b}_{m-2}, \dots, \hat{b}_1, \hat{b}_0\}$
$e = 0$
while $i < n$
    if the sequence $(k_i, \dots, k_j) =$ *bigOne* : $k_{ZOT}[e].t = 1$
    elseif the sequence = *bigTwo* : $k_{ZOT}[e].t = 2$
    elseif the sequence = *bigZero* :$k_{ZOT}[e].t = 0 : k_{ZOT}[e].g = k_{ZOT}[e-1].g$
    $k_{ZOT}[e].l = j - i + 1$
    $Increment(e, i)$
return k_{ZOT}

Single scalar multiplication using window ZOT recoding method (w-ZOTEC)

Let k be a positive integer, then Algorithm 3 is thepropose method that can calculate the quantity kP, where $P \in E(F_p)$.

Algorithm 3: w-ZOTEC Single scalar point multiplication

Input: $G, k_{ZOT} = \{\hat{b}_{m-1}, \hat{b}_{m-2}, \dots, \hat{b}_1, \hat{b}_0\}$
Output: $Q = k_{ZOT}G$
Precompute the points $B = \{O_i, T_j\}, 2 \leq i \leq 5$ *and* $j \in \{3,5,7\}$
$Q = \infty$
For $i(m-1$ *to* $0)$
    If $type(\hat{b}_i) \neq zero : Q = Q + \hat{b}_i(G)$
    Else : $Q = 2^{g_i}(Q)$
return Q

Metrics

In this section, an explanation of the metrics which are used in the comparison and analysis phase is introduced. The following are the metrics with their respective descriptions:

- Hamming weight is equivalent to the number of EC additions
  It is the number of nonzero digits in the recoded exponent k. The number of EC additions and Hamming weight are the same.
- Number of pre-computed points (windows)
  This parameter affects the efficiency of memory usage. Less number of pre-computed windows is more suitable for devices with limited storage.
- Left-to-right recoding
  In practice, left-to-right EC multiplication methods are preferable since it is natural for the window techniques. If the recoding method processes the exponent from left-to-right, it can be combined with the multiplication method. It reduces the required memory for storing the recoded exponent.

Results and Analysis

It is found in (Mimi, Samsudin et al. to appear 2012) that 94% of big-ones have a bit-length of 5 or less. Thus, all the rest of big-ones O_nP, where$n \geq 6$ should be divided into smaller big-digits. It is also found that the lengths for more than 98% of the big-twos are ≤ 7. This means that T_n, where $n > 7$, should be divided into smaller digits.This division limits the number of the precomputed points, sinceT_9 is rarely found in the recoded exponent. Thus, the efficiency of the proposed method may not be affected by these divisions. The length of big-zeros (zero runs) in an EC key plays a significant role in enhancing the scalar multiplication method. For example, Sakai method depends heavily on the length of big-zeros in the EC key(Sakai and Sakurai 2001). The efficiency ofwZOTECmethod is improved when combined with Sakai method since 99.4% of the doublings are repeated doublings (i.e. when $d \geq 2$ in $Z_dP = 2^dP$)(Mimi, Samsudin et al. to appear 2012).

Table 1 : Comparing sliding window and w-NAF to ZOT

Cost	Sliding window NAF	w-NAF	ZOT
Number of pre-computed points	$\left(\frac{2(2^w-(-1)^w)}{3}-1\right)\times\frac{1}{2}$	2^{w-2}	7
Number of doublings	m	m	m
Number of additions	$\frac{m}{w+\frac{4}{3}-\frac{(-1)^w}{3.2^{w-2}}}$	$\frac{m}{w+1}$	$\frac{m}{4.6}$
Additional memory	$O(n)$	$O(n)$	$O(w)$
Note: Left-to-right	yes	no	yes

In this research, the ZOT window size is varied such that $w \in \{1,2,\ldots,7\}$.Its maximum value is 7.The number of the precomputed points for ZOT method will be fixed to 7 points.These points are $B = \{O_i, T_j\}, 2 \leq i \leq 5\ and j \in \{3,5,7\}$. According to the previous discussion on the nature of big-digits inside the ZOT recoded key, the big digits O_6,$O_7$are not included. Table 1 shows the results by comparing ZOT to sliding window and w-NAF methods. For w>3, it was proved(Blake, Seroussi et al. 1999) that width w-NAF is asymptotically better than the sliding window on NAF.As it can be seen, ZOT can be computed left-to-right. This leads to another advantage which is memory savings since the ZOT method does not need to store the whole recoded key, therefore, the recoding and the multiplication methods can be combined together. The Hamming weight for ZOT is fixed, which needs further investigation to compare it with the other methods. The number of precomputed points is also fixed to 7. More investigation is required to determine if the window size should be varied, and if the number of the precomputed points should be fixed. With such result, comparison study can be made to identify the method that has the least number of precomputed points related to each window size.

In Table 2, the expected running time was calculatedby including the time taken by the pre-computation phase. The cost of the pre-computation phase is fixed for ZOT method since the number of pre-computed points has been fixed to 7. This formula will be affected when variable window size and variable number of pre-computed points are investigated for ZOT method.

Table 2 : Total running time for sliding window, w-NAF and ZOT

Expected running time of EC multiplication method (the cost of precomputations + the cost of the EC multiplication)	
Sliding window NAF	$\left[D+\left(\frac{2^w-1(-1)^w}{3}\right)A\right]+\frac{m}{w+v(w)}A+mD$, where $v(w)=\frac{4}{3}-\frac{(-1)^w}{3.2^{w-2}}$
w-NAF	$[D+(2^{w-2}-1)A]+\left[\frac{m}{w+1}A+mD\right]$
ZOT	$3D+9A+\left[\frac{m}{4.6}A+mD\right]$

Conclusions and Future Work

In this paper, a new window ZOT EC multiplication method was proposed. The proposed method is a left-to-right multiplication method, whichdoes not require muchcomputing memory. Therefore, the proposed method is highly suitable for devices with limited memory. Our proposed method can be compared to wNAF with $w=5$. The number of precomputed points is 7 for both methods. The Hamming weight is almost the same. The Hamming weight for ZOT recoded keys is fixed to $\frac{n}{4.6}$. Other window recoding methods such as wMOF, wFractional, and other left-to-right methods will be included in the future comparisons. The size of the available memory can be considered as anindicatorto determine the number of pre-computed windows that can be used. For example, if we have only 4 locations, then the maximum window size that can be used is 4 and, in this case, the maximum window size for wZOTEC should be lower.

References:

Avanzi, R. (2005). A Note on the Signed Sliding Window Integer Recoding and a Left-to-Right Analogue Selected Areas in Cryptography. H. Handschuh and M. Hasan, Springer Berlin / Heidelberg. 3357: 130-143.

Blake, I. F., G. Seroussi, et al. (1999). Elliptic Curves in Cryptography, Cambridge University Press.
Darrel, H., J. M. Alfred, et al. (2003). Guide to Elliptic Curve Cryptography, Springer-Verlag New York, Inc.

Eisentrager, K., K. Lauter, et al. (2003). Fast elliptic curve arithmetic and improved Weil pairing evaluation. Topics in Cryptology - Ct-Rsa 2003, Proceedings.

Frey, H. C. a. G. (2006). Handbook of Elliptic and Hyperelliptic Curve Cryptography, Chapman & Hall/CRC.

Gordon, D. M. (1998). "A survey of fast exponentiation methods." Journal of Algorithms27(1): 129-146.
Jahani, S. (2009). ZOT-MK: A New Algorithm for Big Integer Multiplication. Department of Computer Science. Penang, Universiti Sains Malaysia. MSc.

Khabbazian, M., T. A. Gulliver, et al. (2005). "A new minimal average weight representation for left-to-right point multiplication methods." Computers, IEEE Transactions on54(11): 1454-1459.

Knuth, D. E. (1997). The art of computer programming: seminumerical algorithms. Boston, MA, USA, Addison-Wesley Longman Publishing Co., Inc.

Kong, F. Y. and D. X. Li (2005). A note on signed binary window algorithm for elliptic curve cryptosystems. Cryptology and Network Security, Proceedings.

Koyama, K. and Y. Tsuruoka (1993). Speeding up Elliptic Cryptosystems by Using a Signed Binary Window Method. Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology, Springer-Verlag: 345-357.

Mimi, H., A. Samsudin, et al. (to appear 2012). "Elliptic Curve Scalar Multiplication Algorithm Using ZOT Recoding."

Mimi, H., A. Samsudin, et al. (to appear 2012). "Evaluating Composite EC Operations and their Applicability to the On-the-Fly and Non-Window Multiplication Methods."

Miyaji, A., T. Ono, et al. (1997). Efficient elliptic curve exponentiation. Information and Communications Security. Y. Han, T. Okamoto and S. Qing, Springer Berlin / Heidelberg. 1334: 282-290.

Moller, B. (2002). Improved techniques for fast exponentiation. Iformation Security and Cryptology - Icisc 2002. 2587: 298-312.

Moller, B. (2004). Fractional windows revisited: Improved signed-digit representations for efficient exponentiation. Information Security and Cryptology - Icisc 2004. 3506: 137-153.

Muir, J. and D. Stinson (2005). New Minimal Weight Representations for Left-to-Right Window Methods Topics in Cryptology – CT-RSA 2005. A. Menezes, Springer Berlin / Heidelberg. 3376: 366-383.

Muir, J. A. and D. R. Stinson (2006). "Minimality and other properties of the width-w nonadjacent form." Mathematics of Computation75(253): 369-384.

Okeya, K., K. Schmidt-Samoa, et al. (2004). Signed binary representations revisited. Advances in Cryptology - Crypto 2004, Proceedings.

Sakai, Y. and K. Sakurai (2001). "Efficient scalar multiplications on elliptic curves with direct computations of several doublings." Ieice Transactions on Fundamentals of Electronics Communications and Computer SciencesE84a(1): 120-129.

Schmidt-Samoa, K., O. Semay, et al. (2006). "Analysis of fractional window recoding methods and their application to elliptic curve cryptosystems." Ieee Transactions on Computers55(1): 48-57.

Solinas, J. A. (1997). "An improved algorithm for arithmetic on a family of elliptic curves." Advances in Cryptology - Crypto'97, Proceedings1294: 357-371.

Solinas, J. A. (2000). "Efficient Arithmetic on Koblitz Curves." Des. Codes Cryptography19(2-3): 195-249.

Tsaur, W.-J. and C.-H. Chou (2005). "Efficient algorithms for speeding up the computations of elliptic curve cryptosystems." Applied Mathematics and Computation168(2): 1045-1064.

William, S. (2006). Cryptography and Network Security: Principles and Practice, Pearson-Prentice Hal.

A PROPOSED IND-CCA2 SCHEME FOR IMPLEMENTATION ON AN ASYMMETRIC CRYPTOSYSTEM BASED ON THE DIOPHANTINE EQUATION HARD PROBLEM

Muhammad Rezal Kamel Ariffin[1&2]
[1]*Al-Kindi Cryptography Research Laboratory,*
Institute for Mathematical Research, Universiti Putra Malaysia
[2]*Mathematics Department, Faculty of Science, Universiti Putra Malaysia*
rezal@putra.upm.edu.my

Abstract:

Recently an asymmetric cryptosystem (i.e. AA_β- public key cryptosystem) based upon the Diophantine Equation Hard Problem (DEHP) together with the difficulty of factoring p^2q was proposed. The AA_β- public key cryptosystem security reduction is given by Decryption $\leq_T$ AA_β – DEHP-1 (where AA_β – DEHP-1 is the AA_β type DEHP) and Decryption $\leq_T$ Factoring p^2q. Also, AA_β – $DEHP - 1 \leq_T$ Factoring p^2q, however the converse is still unknown. It is a probabilistic scheme, hence providing IND-CPA security. In this work, we propose an IND-CCA2 scheme for implementation on the AA_β- public key cryptosystem whose security is equivalent to a total break of the AA_β- public key cryptosystem under the random oracle model.

Introduction

The motivation behind the attempt to formalize what is to be known as the Diophantine Equation Hard Problem (DEHP) is to further enhance asymmetric cryptosystem models. The discrete log problem (DLP) has the source of various asymmetric models such as the Diffie-Hellman Key Exchange and the El-Gamal cryptosystem to name a few. The elliptic curve discrete log problem (ECDLP) has been the source for difficulty in the elliptic Curve Cryptosystem (ECC). As for the renowned RSA algorithm, the integer factorization problem (IFP) coupled with the e -th root problem modulo N (where N is a product of 2 primes p and q) is its source of difficulty (Rivest et.al., 1978). The shortest vector problem gave rise to lattice based asymmetric algorithms such as NTRU – which boasts encryption/decryption speeds of complexity order $O(n^2)$ (Hoffstein et.al., 1998) (Hermans, 2010). A lot of research has been done to gauge the efficiency between the above mentioned asymmetric algorithms. Among research angles in gauging the efficiency of asymmetric algorithms include (but not limited to):

1. Key length
2. Computational "intensiveness"
3. Speed

Suggestions have been made that ECC is able to utilize shorter keys than RSA, but still maintaining the same level of security (Vanstone, 2006). However, in certain situations where a large block needs to be encrypted, RSA is the better option than ECC because ECC would need more computational effort to undergo such a task (Scott, 2008). As for speed, NTRU currently holds the record when compared to RSA and ECC which runs at a complexity order of $O(n^3)$.

In this work, the Diophantine Equation Hard Problem (DEHP) is presented (work to formalize the DEHP can be traced back since 2009 with little or no success by the author). The author proposes that the DEHP as outlined in this paper is also another hard mathematical problem that has secure cryptographic qualities coupled with the above described "cryptographic efficiency" qualities. An asymmetric cryptosystem modeled after the DEHP is presented – known as the AA_β cryptosystem. Then, security against lattice based attacks is discussed. The underlying security reduction principle will be then presented. After which, a comparison table between RSA, ECC, NTRU and AA_β will be provided. Finally, indistinguishability results will be proposed.

Diophantine Equation Hard Problem (DEHP)

Definition 1
Let $U = \sum_{i=1}^{j} V_i x_i$ be a summation of unknown integers $\{x_i\}$ which are of the same bit length where $\{V_i\}$ is a public sequence of constants. We define the DEHP is solved when U is *prf*-solved. That is, the preferred integer set $\{x_i^*\}$ is found from the set of all possible integers $\{x_i\}$ such that $U = \sum_{i=1}^{j} x_i$.

Example 1
Let $U = 8 + 10 + 13 = 31$. Here $x_1^* = 8, x_2^* = 10$ and $x_3^* = 13$. A possible incorrect combination could be $x_1' = 9, x_2' = 10$ and $x_3' = 12$. Another possible incorrect combination could be $x_1' = 8, x_2' = 11$ and $x_3' = 12$.

The AA_β Public Key Cryptosystem

We begin with stating that the communication process is between A (Along) and B (Busu), where Busu is sending information to Along after encrypting the plaintext with Along's public key. Along's secret parameters are two prime integers p and q each of n-bit length and $pq > 2^{2n-1} + 2^{2n-2}$.

Definition 1 (Public keys)
Along's public keys are given by

1. $e_{A1} = p^2 q$.
2. $e_{A2} = e$ where $ed \equiv 1 \pmod{pq}$ and e is of $3n$-bit length.

Busu's secret parameters are as follows:

1. The session key given by the integer k_1 of $4n$-bit length.
2. The message M is given by a $2n$ bit even number and $M < 2^{2n-1} + 2^{2n-2}$.

Encryption

Definition 2 (Ciphertext)
The ciphertext is given by $C = k_1 e_{A1} + M^2 e_{A2}$.

Remark 1

- The length of the ciphertext is approximately $7n$ bits, while the length of the message is $2n$ bits. The ratio size between message and ciphertext is 2:7.
- The ratio size between message and public key set is 1:3.

Decryption

Proposition 1
The decryption algorithm is as follows:

i. To begin decryption do $W \equiv Cd \equiv M^2 (\text{mod } pq)$.
ii. Solve the square root of $W (\text{mod } pq)$ (with the help of the Chinese Remainder Theorem).
iii. For each 4 possible message test whether $k_1' = \frac{C - (M_i')^2 e_{A2}}{e_{A1}} \in \mathbb{Z}$ or not (where $i = 1,2,3,4$).
iv. If an integer value is obtained, then $M_i' = M$.

Proof:
See (Ariffin et.al., 2012) for the proof of correctness.

Example

Key Generation

This is an example for $n = 32$ bits. Along's secret parameters are:

i. $p = 4103191423$
ii. $q = 4138639117$
iii. $d = 2705738027224175602$

Along's public keys are:

i. $e_{A1} = 6967887252370441407734112769 3$
ii. $e_{A2} = 52101475710031396056335959259$

Busu's secret parameters are:

i. $k_1 = 171768918882977375440912959061197956270$
ii. $M = 9783938282534345065$

Encryption

The ciphertext is given by
$C = 16956101722672426819946448654344245938538555368011680255863149004385.$

Decryption

Upon receiving the ciphertext Along will compute $W = C_1 d(\text{mod } \theta) = 7042873210696671480$. Then he will proceed to compute the following values $M_1' = 14515469047415614243$, $M_2' = 7197690245232348426$, $M_3' = 9783938282534345065$, and $M_4' = 2466159480351079248$. Only M_3' will provide an integer value for procedure (iii) in Proposition 1.■

Lattice Based Attacks

Lattice based attacks utilizing the LLL algorithm has been given extensive attention by the author. Up to until publication of this proceeding no lattice based attack utilizing the LLL algorithm has been successful (Ariffin et.al., 2012). During the course of research, a literature by Herrman and May pointed out by Prof. Abderrahmane Nitaj resembles to structure of the AA_β algorithm (Herrman & May, 2008). We reproduce the core objective as stated in the paper.

The work by Herrman and May

As stated in their abstract and introduction: "to find solutions for linear equations modulo an unknown divisor p of a known composite $N = pq$". From:

$$f(x_1, \ldots, x_n) = 0 \ (\text{mod } N) \qquad (1)$$

for some N with unknown factorization. Equation (1) has many solutions $(y_1, \ldots, y_n) \in \mathbb{Z}_N^n$. It is stated that if X_i are upper bounds such that $|y_i| \leq X_i$, then one can roughly expect a unique solution when $\prod_i X_i \leq N$. And the work by Herrman and May suggests a method to obtain the solution.

Analogy to the work by Herrman and May?

The ciphertext produced by the AA_β algorithm results in $|k_1 M^2| \approx |C|$. The equivalent statement in the case of the AA_β algorithm the statement is to be rephrased as follows:- "to find solutions for linear equations modulo an unknown divisor p and q of a known composite $e_{A1} = p^2 q$ ". We will go into detail in the next section.

Underlying Security Principle

$AA_\beta - DEHP - 1$

To find the unknown parameter M^2 from the public "summation composite" C. That is, to *prf-solve* C.

Integer Factorization

To find the unknown composite (p, q) from the public composite $e_{A1} = p^2q$.

Security Reduction

Proposition 2
Decryption $=_T AA_\beta - DEHP - 1$

Proof:
Let ϑ_1 be an oracle that is able to *prf*-solve C. Call $\vartheta_1(C)$ to obtain M^2. As a result M can be obtained. Thus, decryption has occurred. If decryption has occurred than $AA_\beta - DEHP - 1$ has been solved.■

Proposition 3
$AA_\beta - DEHP - 1 \leq_T$ Factoring p^2q

Corollary 4
Decryption $\leq_T$Factoring p^2q

Remark 3
The converse of Proposition 3 and Corollary 4 are unknown.

Table of comparison

The following is a table of comparison between RSA, ECC, NTRU and AA_β.

Table 1 : Comparison table for input block of length n

Algorithm	Encryption Speed	Decryption Speed	Message Expansion
RSA	$O(n^3)$	$O(n^3)$	1 – 1
ECC	$O(n^3)$	$O(n^3)$	1 – 2 (2 parameter ciphertext)
NTRU	$O(n^2)$	$O(n^2)$	Varies (Hoffstein et.al, 1999)
AA_β	$O(n^2)$	$O(n^3)$	2 – 7

A Proposed IND-CCA2 Scheme for the AA_β Cryptosystem

Observing the structure of the ciphertext, and adversary may construct an illegal ciphertext given by the equation $C' = k_1{'}e_{A1} + k_1e_{A1} + M^2e_{A2}$. It is obvious that $D(C') = M$. We will now proceed to overcome this problem, hence ensuring IND-CCA2 security for the scheme. Let H be a mapping from $n + k$ bits to k_0 bit strings. It is treated as a random oracle. The scheme is as follows:

Encryption Algorithm

Let E denote the AA_β encryption algorithm and (k_1, M) be the private parameters from Busu to Along. Busu will do the following procedures:

1. $C_1 = E(M) = k_1 e_{A1} + M^2 e_{A2}$.
2. $C_2 = H(M + k_1)$

The ciphertext of M is given by (C_1, C_2).

Decryption Algorithm

Let D denote the AA_β decryption algorithm. Along will compute $D(C) = M$. From M, Along can obtain k_1. He will then compute $h = H(M + k_1)$. If $y = h \oplus H \neq 0$, then output $\perp$ which means the input ciphertext is illegal. Otherwise if $y = 0$, then D outputs M. As a note, in order to successfully substitute C_2, the adversary has to be able to decrypt C_1 successfully to obtain the pair (k_1, M) in order to construct $C_2' = H(M + k_1 + k_1')$.

Conclusion

The DEHP, is proposed to be another source of cryptographic primitive, that if utilized correctly could give rise to other possible asymmetric algorithms differing from classical algorithms based on integer factorization, discrete log problem (DLP), elliptic curve discrete log problem (ECDLP), e -th root modulo N, square root problem and others. In this work, we also propose a scheme to ensure that the AA_β cryptosystem is IND-CCA2 secure. It is not difficult to see that, the scheme could also be used by other algorithms in order to achieve IND-CCA2 security (especially schemes that utilize session keys that could be reconstructed by the recipient).

References:

M. R. K.Ariffin, M. A. Asbullah & N. A. Abu (2012). AA_{\beta} Public Key Cryptosystem – An Asymmetric Cryptosystem based on the Diophantine Equation Hard Problem. [Online] Available: http://eprint.iacr.org/2011/467.pdf .

J. Hermans et. al. (2010). Speed Records for NTRU, *CT-RSA 2010, LNCS 5985*, 73-88.

J. Hoffstein, J. Pipher, and J.H. Silverman (1998). NTRU: A Ring Based Public Key Cryptosystem, *Algorithmic Number Theory (ANTS III) Lecture Notes in Computer Science 1423*. Springer-Verlag, Berlin. 267-288.

J. Hoffstein, D. Lieman, J. Pipher, J. H. Silverman (1999). NTRU: A Public Key Cryptosystem. [Online] Available: HTTP://GROUPER.IEEE.ORG/GROUPS/1363/LATTPK/SUBMISSIONS/NTRU.PDF

M. Herrmann, A. May (2008). Solving Linear Equations Modulo Divisors: On Factoring Given Any Bits. *ASIACRYPT 2008*. 406-424

M. Scott, (2008, November 15). When RSA is better than ECC. [Online] Available: http://www.derkeiler.com/Newsgroups/sci.crypt/2008-11/msg00276.html

R.L. Rivest, A. Shamir and L. Adleman (1978). A method for obtaining digital signatures and public key cryptosystems, *Commun. ACM,* 21(2), 120-126.

S. Vanstone, (2006, March 18). ECC holds key to next generation cryptography. [Online] Available: http://www.design-reuse.com/articles/7409/ecc-hold-key-to-next-gen-cryptography.html

PRE-CONDITIONS FOR DESIGNING ASYMMETRIC CRYPTOSYSTEM BASED ON DIOPHANTINE EQUATION HARD PROBLEM

Muhammad Asyraf Asbullah and Muhammad Rezal Kamel Ariffin
Al-Kindi Cryptography Research Labarotary,
Institute for Mathematical Research
Universiti Putra Malaysia
ma_asyraf@putra.upm.edu.my, rezal@putra.upm.edu.my

Abstract:

The Diophantine Equation concept has been occasionally attempted to be implemented as a security primitive for asymmetric cryptography. However, success in producing such asymmetric schemes is not forthcoming. Apart from succumbing to cryptanalysis, the concept of utilizing Diophantine equations is poorly defined and is only mentioned at a glance in its respective literatures. This paper discusses the Diophantine Equation Hard Problem (DEHP) which was recently proposed as cryptographic primitive for the AA_{β}-cryptosystem. We analyze the differences between a DEHP based asymmetric cryptosystem (i.e. the AA_{β}-Cryptosystem) and other cryptographic schemes that have been designed based on Diophantine equations. Furthermore, we also present the underlying security features regarding to the implementation of the proposed cryptographic primitive for the AA_{β}-cryptosystem. In addition, we also provide some improper design via the DEHP that would lead to successful passive adversary attacks.

Introduction

Since the introduction on the key exchange mechanism of Diffie and Hellman (1976), followed then by the well-studied RSA public key cryptosystem by the trio Rivest-Shamir-Adlemen (1978), the notion of asymmetric cryptographic drastically changed the cryptographic world. These two papers are considered as the trigger for the afterwards development of many others asymmetric cryptographic schemes. Hoffstein et al. (2008) provides a numbers of literatures on the others public key cryptosystem such as the ElGamal, the Elliptic Curve and the Knapsack Cryptosystem. The most interesting fact behind the structure of these asymmetric scheme is that their sources of security solely lies on the difficulties to solve hard number theoretic problems such as the discrete logarithm problem, the integer factorization and the subset sum problem.

A Diophantine equation is an equation of the form $F(x_1, x_2, \ldots x_n) = 0$ where F is a polynomial with integer coefficients. One of the most celebrated problems concerning the Diophantine equation is the Hilbert's tenth problem. Regarding to this problem, Hilbert raise a question asking is there any algorithm to decide whether solutions in integers can be found? In the classical sense, the Diophantine equation is claimed to be hard to solve and following the work of Matiyasevich (1993) the solvability of Diophantine equation is undecideable. The authors proposed another problem on the Diophantine equation what is defined as the Diophantine Equation Hard Problem (DEHP). The DEHP is taking a difference perspective from the Hilbert's tenth problem since the DEHP always has integral solutions. In its context, the DEHP asks for an algorithm to find a specific solution from an equation that has so many solutions.

Generally, the Diophantine equation has been tried to implement several public key encryptions such as Ong et al. (1985) and Lin et al. (1995) and as a key exchange mechanism proposed by Yosh (2011). However, success in producing such asymmetric schemes is not forthcoming. Apart from succumbing to cryptanalysis, the concept of utilizing Diophantine equations is poorly defined and is only mentioned at a glance in its respective literatures. Thus, the immediate objective is to propose a new paradigm of the hardness based on the Diophantine equation. In this paper, a new asymmetric cryptosystem is discussed that utilized the DEHP as its security primitive.

The paper is organized as follows. Section 2, the DEHP will be described. In section 3, we present some previous work based on the Diophantine equation. The fourth section describes the AA_{β}-Cryptosystem and the underlying security features is discuss in section 5. In the next section of the paper, we illustrate two improper designs via DEHP. Conclusions appear in section 7.

Diophantine Equation Hard Problem (DEHP)

The DEHP is based upon the linear Diophantine equation which is of the form $U = \sum_{i=1}^{n} V_i x_i$. The following definition would give the precise idea regarding the DEHP.

Definition 2.1. Let $U = \sum_{i=1}^{n} V_i x_i^*$ where the integers U and $\{V_i\}_{i=1}^{n}$ are known. We define the sequence of integers $\{x_i^*\}_{i=1}^{n}$as the preferred integers used to obtain U. The sequence $\{x_i^*\}_{i=1}^{n}$ is particular elements from the solutions set of $U = \sum_{i=1}^{n} V_i x_i^*$ that contains infinitely many elements. The problem to determine such sequence $\{x_i^*\}_{i=1}^{n}$is known as the DEHP.

In general, if one can solve the equation $U = \sum_{i=1}^{n} V_i x_i^*$, then it has infinite number of solutions. However, for cryptographic purposes, one always dealing with restricted or fixed lengths of parameters thus making the solution is finite or unique. Therefore, the setting for reasonable parameter sizes is indeed important to provide a reasonable security. On the other hand, the difficulty of DEHP arises when one needs to determine correctly the 'preferred' sequence $\{x_i^*\}_{i=1}^{n}$ from vastly many solutions.

Definition 2.2. The Diophantine equation given by $U = \sum_{i=1}^{n} V_i x_i^*$ is defined to be *prf*-solved when the sequences of integers $\{x_i^*\}_{i=1}^{n}$ are found. The DEHP is solved when U is *prf*-solved. The following illustration would be sufficient for us to grasp the understanding of the term '*prf*-solved'.

Example 2.3. Consider an equation $U = 20 = x_1 + x_2$. Let $x_1 = 9$, $x_2 = 11$ be the *prf*-solution of the equation, where x_1 and x_2 are n-bits long (i.e. this example $n = 4$). An attacker would be faced with the DEHP in determining the preferred integer $x_1 = t$ in order to determine the remaining preferred integer $x_2 = 20 - t$ that form the *prf*-solution set for the above Diophantine equation. Since the solution set is restricted to a finite set (i.e. in this case x_1 is 4-bits long), the possible values of t resides within the interval $(2^3, 2^4 - 1)$. Hence the solution set can be found in polynomial time. Observed that $x_1 = 8$, $x_2 = 12$ and $x_1 = x_2 = 10$ also give the solution. But, we argue that even though the attacker can find the *prf*-solution $x_1 = 9, x_2 = 11$ there exist no indicators for such solution to be considered as the *prf*-solution for the DEHP in the first place. We are proposing to highlight this notion of hardness within DEHP.

Previous Work Based on Diophantine Equations

In this section, we will discuss three types of the asymmetric cryptographic schemes which are a digital signature scheme, a public key encryption algorithm and a key exchange mechanism regarding to the Diophantine equation. We will present only the relevant aspect based on the DEHP. The rigorous treatments are omitted here and the interested one could refer to the original work for its technical details.

Ong-Schnorr-Shamir Signature Scheme

Ong et al. (1985) proposed Ong-Schnorr-Shamir signature scheme as a method for digital signature. The main aspect of their work is to provide a mean for easy implementation of signature. Briefly, the system consists of integers n and k which made public. The mechanism for their signature scheme is as follows:

Signing. Compute the large integer n which is a composite number and its factorization is kept secret. Choose an integer k as the same size to n. For any message m where $0 < m < n$, its signature is any pair of integer x, y such that

$$x^2 + ky^2 \equiv m(mod\ n) \qquad (3.1)$$

The structure of the scheme is based on polynomial equations modulo n. For any attacker, the task is to find any solution of integer x and y from given value of n, k and m, which is believed as difficult as factoring the modulus n. Observe that the equation $x^2 + ky^2 = m$ is one of Diophantine equation. Pollard and Schnorr (1987) describe an algorithm that easily solves this particular Diophantine equation without knowing the factorization of modulus n. Thus, the algorithm can efficiently be used to attacks Ong et al. signature scheme. For simplicity we frame the description of the algorithm exactly as mentioned in the Pollard and Schnorr paper.

Pollard and Schnorr claims that the algorithm for solving (3.1) does not require knowledge of the factorization of n instead it is based on the well-known identity $x_1^2 + ky_1^2(x_2^2 + ky_2^2) = X^2 + kY^2$ where $X = x_1x_2 \pm ky_1y_2$, $Y = x_1y_2 \mp x_2y_1$ and solve (3.1) for $k, m \in \mathbb{Z}_n^*$. Note that the signature is any pair of integer x, y but not a unique pair of (x, y). There are many possible signatures for a particular message. Hence, any value of x and y obtained via the above algorithm could solve the equation (3.1). We conclude that the fall out of this scheme is due to the pair of (x, y) is not unique; no need to *prf-solved.*

Lin-Chang-Lee Cryptosystem

Lin et al. (1995) introduced a public key system which security is based on the Diophantine equations. Besides the descriptions of the key generation, the encryptions and the decryptions process, this paper also provides some security analysis from the linear Diophantine views. Their results claims that it is indeed difficult for successfully breaking the scheme which is based on the hardness of the linear Diophantine equation. For details see Lin et al. (1995).

Unfortunately, their scheme is being cryptanalyst by Cusick (1995), also by Laih and Gau (1997). Cusick state that the major shortcoming of Lin et al. scheme is due to the construction of its public key which consists of integers any two that have a large common factor. Hence this lead to the total breaks of the scheme. On the contrary, Laih and Gau relegates Lin et al. scheme as a type of an easy knapsack sequence and concurrently developed an efficient method to solve the easy knapsack sequence. Both of the cryptanalysis was done without solving any Diophantine equations.

A note on the knapsack cryptosystem

The knapsack or the subset sum problems were used as a primitive for a cryptosystem, but they were broken every which way. One also is recommended to consults with Odlyzko (1990) which provide more details on historical aspects that lead to fall out of the knapsack based cryptosystem. Even though the general knapsack problem is proven to reside in the class of NP-hard, however most knapsack based schemes easily solved by using lattice reduction algorithm. Another turn out of event, most of the knapsack based cryptosystem can easily be broken if their density is very low. A very efficient algorithm so called low-density attack could be used in order to solve the low density knapsack problem. Recent literature on low-density attack and its variants can be found in Nguyen and Stern (2005). Herewith, we define the knapsack problem.

Definition 3.3. The knapsack (or subset sum) problem is the following: given a set $\{a_1, a_2, \ldots, a_n\}$ of positive integers and a sum $S = \sum_{i=1}^{n} m_i a_i$, where $m_i \in \{0,1\}$, recover the $m_i's$. Obviously, the sum $S = \sum_{i=1}^{n} m_i a_i$ is a kind of a Diophantine equation and it is well-known that this problem is NP-hard, however the knapsack cryptosystem have special characteristics as listed as follows:

1. Given a set of public key $\{a_1, a_2, \ldots, a_n\}$, choose only several subset
2. The messages represented by $M = (m_1, m_2, \ldots, m_n)$ are equal in sizes.
3. Each pair wise product $m_i a_i$ (i.e. $m_i a_i$ for $i = 1,2, \ldots, n$) will be sums up to become the ciphertext.
4. A general subset sum problem is infeasible to solve it directly, however for its cryptographic purpose (i.e. for decryption to occur) a special structure need to be implemented such as the superincreasing sequence and Graham-Shamir sequence.
5. The Hamming weight of the message space is small (normally less than $\frac{n}{2}$).

Yosh Key Exchange Cryptosystem

The idea of the key exchange mechanism based on the Diophantine equation was proposed by Yosh (2011). This work is the based on the system of higher order Diophantine equations. The system conjectured that an adversary would not be able to solve the Diophantine equation without the trapdoor information. As stated within the paper, there is quite a significant number between the two communicating parties before they can agree on a shared key. In order to avoid the usage of a particular Diophantine equation, both sender and receiver can choose the form of Diophantine equation arbitrarily and by some means both parties could securely recover the intended shared key.

By referring to Yosh (2011), the whole procedure requires a lot of computational process due to the usage of the higher degree of the Diophantine equation, compared to the DEHP which only utilizes the linear Diophantine equation. In addition, large number of information being exchanged in this scheme can lead to advantages for the adversary. As a conclusion, the scheme seems too complicated for practical cryptographic purposes.

The AA_β Public Key Cryptosystem

We begin with stating that the communication process is between A (Along) and B (Busu), where Busu is sending information to Along after encrypting the plaintext with Along's public key.

Key Generation.
Along's secret parameters are two prime integers p and q each of n-bit length and $pq > 2^{2n-1} + 2^{2n-2}$.

Along's public keys are given by
1. $e_{A1} = p^2 q$.
2. $e_{A2} = e$ where $ed \equiv 1 \pmod{pq}$ and e is of $3n$-bit length.

Busu's secret parameters are as follows:
1. The session key given by the integer k_1 of $4n$-bit length.
2. The message M is given by a $2n$ bit even number and $M < 2^{2n-1} + 2^{2n-2}$.

Encryption.
The ciphertext is given by $C = k_1 e_{A1} + M^2 e_{A2}$.

Decryption.
Proposition 4.2. The decryption algorithm is as follows:
i. To begin decryption do $W \equiv Cd \equiv M^2 (\text{mod } pq)$.
ii. Solve the square root of $W (\text{mod } pq)$ (with the help of the Chinese Remainder Theorem).
iii. For each 4 possible message test whether $k_1' = \frac{C-(M_i')^2}{e_{A1}} \in \mathbb{Z}$ or not (where $i = 1,2,3,4$).
iv. If an integer value is obtained, then $M_i' = M$.

Proof: See (Ariffin et.al., 2012) for the proof of correctness■

Proposition 4.3. The AA_β-Cryptosystem is not a knapsack (subset sum) based cryptosystem.
Proof: We will proof by contradiction. Assume that the AA_β-Cryptosystem is a knapsack based cryptosystem. It is obvious that the AA_β-Cryptosystem sums up all the public key values rather than several selected subset. This is a contradiction. Thus the AA_β-Cryptosystem is not a knapsack based cryptosystem■

Underlying Security Features

We will now observe the underlying security features that the AA_β Public Key Cryptosystem based upon.

The AA_β-DEHP

To find the unknown parameter M^2 from the public "summation composite" C. That is, to *prf-solve* C.

Integer Factorization

To find the unknown composite (p, q) from the public composite $e_{A1} = p^2 q$.

Preconditions Design via the DEHP

It is important to note that, an improper design of an asymmetric cryptosystem via the DEHP would lead to successful passive adversary attacks. To illustrate this fact, we will produce the following examples concerning improper integer size of parameters.

Proposition 6.1 (Euclidean division). Let $U = x_1V_1 + x_2V_2$ with $x_1 \approx x_2 < V_2 < V_1$. If $V_1 > x_2V_2$ then $x_1$and x_2 can be found in polynomial time.

Proof: Suppose $U = x_1V_1 + x_2V_2$ with $V_1 > x_2V_2$. Then by performing the Euclidean division, we get

$$x_1 = floor(\frac{U}{V_1}) \text{ and } x_2 = \frac{C - x_1V_1}{V_2} \tag{6.1}$$

If $V_2 > x_1V_1$, $x_1$and x_2 can be found in polynomial time in similar manner. ■

Proposition 6.2 (Extended Euclidean Algorithm). Let $U = x_1V_1 + x_2V_2$ with gcd $(V_1, V_2) = 1$ and $V_1 < V_2$. If $x_1 \approx x_2 \approx V_1 \approx V_2$ then $x_1$and x_2 can be found in polynomial time.

Proof: Suppose $U = x_1V_1 + x_2V_2$ where gcd $(V_1, V_2) = 1$. Then utilizing the extended euclidean algorithm we will proceed to determine the variable j within $x_1 = x_{10} + V_2j$ and $x_2 = x_{20} - V_1j$ where $V_1 \approx V_2$. The interval to determine j is in between the lower and upper bound of size $V_1$and V_2. Solving the interval of V_2 is not a wise choice since V_1 is relative smaller if compared to the size of V_2 (i.e within several bits). Upon obtaining those interval we have one candidate for $j = j^*$. By substituting j^* into $x_1 = x_{10} + V_2j^*$,thus x_1 can be obtained. By the procedure of the extended Euclidean algorithm we utilize the same j^* to obtain $x_2 = x_{20} - V_1j^*$.

Proposition 6.3 (Congruential relations and multiplicative inverse).
Let $U = x_1V_1 + x_2V_2$ with gcd $(V_1, V_2) = 1$. If x_1, x_2, V_1, V_2 roughly equal in size, then $x_1$and x_2 can be found in polynomial time.

Proof: Suppose one find an integer t such that $V_1.t\ (mod\ V_2)$ is a small integer r. Then compute $Ut \equiv x_1V_1t + x_2V_2t \equiv x_1V_1t \equiv x_1r\ (mod\ V_2)$. Since gcd $(V_1, V_2) = 1$, thus the multiplicative inverse of r exist. Hence compute $x_1 \equiv r^{-1}Ut\ (mod\ V_2)$ and $x_2 = \frac{C - x_1V_1}{V_2}$.

Proposition 6.4 (Gaussian Lattice Reduction)
Let $U = x_1V_1 + x_2V_2$ where the parameters $x_1$and x_2 are relatively short compare to V_1 and V_2 in size. If $\| W \|$ is relatively short as compare to Gaussian heuristic $\sigma(L)$, then tx$_1$and x_2 can be found in polynomial time.

Proof: We will look at the lattice L spanned by $(1,0,V_1), (0,1,V_2), (0,0,-C)$. The Gaussian heuristic for the lattice L is given by:

$$\sigma(L) = \sqrt{\frac{3}{2\pi e}}C^{\frac{1}{3}} \tag{6.2}$$

Observe that the vector $W = (x_1, x_2, 0)$ is in L with length of W be $\| W \|$. Suppose $\| W \|$ is relatively short as compare to the value $\sigma(L)$, then the LLL algorithm will be able to find W. Observe that if we multiply the lattice L with a large constant K then it will make the $\sigma(L)$ much greater by $K^{\frac{1}{3}}$ while the length of vector W maintain the same. Hence, we could always get $(L) > \| W \|$, so if K is large then the vector W becomes smaller which makes the LLL algorithm to find W even easier■.

Conclusion

In this paper, the DEHP is proposed as another hard mathematical problem that has secure cryptographic qualities. As a result, a new public key encryption scheme namely as the AA_β Public Key Cryptosystem is designed as resemblance to the security concept as defined by the DEHP. We also examined previous asymmetric cryptosystems

whose security is based upon the Diophantine equation. Furthermore, the result of this paper proves that it is possible to design a cryptographic scheme based upon the DEHP.

References:

Ariffin, M. R. K., Asbullah, M. A. & Abu, N. A. (2012). AA_{β} Public Key Cryptosystem – An Asymmetric Cryptosystem based on the Diophantine Equation Hard Problem. [Online] Available: http://eprint.iacr.org/2011/467.pdf.

Cusick T.W. (1995). Cryptanalysis of a Public Key system based on Diophantine Equation. *Information Processing Letters.* 56, 73-75.

Diffie, W. and Hellman, M. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory.* 22(26), 644–654.

Hoffstein, J., Pipher, J. and Silverman, J.H. (2008). An Introduction to Mathematical Cryptography. New York: Springer.

Laih, C.S. and Gau, M.J. (1997). Cryptanalysis of Diophantine Equation Oriented Public Key Cryptosystem. *IEEE Transactions on Computers.* 46(4), 511-512.

Lin, C.H., Chang, C.C., Lee, R.C.T. (1995). A New Public-Key Cipher System Based Upon the Diophantine Equations. *IEEE Transactions on Computers.* 44(1), 13-19.

Matiyasevich, Y. (1993). Hilbert's Tenth Problem. MIT Press, Cambridge, Massachusetts.

Nguyen, P.Q and Stern, J (2005). Adapting Density Attacks to Low-Weight Knapsacks. *Asiacrypt 2005, LNCS, Lee, P. Edition, Springer.* 3788, 41-58.

Odlyzko, A. M (1990). The rise and fall of knapsack cryptosystems. *In Cryptology and Computational Number Theory. Proceedings of Symposia in Applied Mathematics.* 42, 75–88.

Ong, H, Schnorr, C and Shamir, A (1985). An efficient signature scheme based on polynomial equations, *Lecture Note in Computer Science 196.* Springer-Verlag, New York, 37–46.

Pollard, J.M, and Schnorr, C.P (1987). An efficient solution of the congruence $x^2 + ky^2 \equiv m(mod\ n)$. *IEEE Trans. Inf. Theory.* 33(5), 702-709.

Rivest, R.L, Shamir, A and Adleman, L (1978). A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM.* 21(2), 120–126.

Yosh, H (2011). The Key Exchange Cryptosystem Used With Higher Order Diophantine Equations. *International Journal of Network Security and Its Applications.* 3(2), 43-50.

AN EFFICIENT TWO WAY ZERO KNOWLEDGE SCHEME BASED ON THE DIOPHANTINE EQUATION HARD PROBLEM

Tea Boon Chian[1] and Muhammad Rezal Kamel Ariffin[1&2]
[1]*Al-Kindi Cryptography Research Laboratory, Institute for Mathematical Research, Universiti Putra Malaysia*
[2]*Mathematics Department, Faculty of Science, Universiti Putra Malaysia*
teaboonchian@ymail.com, rezal@putra.upm.edu.my

Abstract:

Recently an asymmetric cryptosystem (i.e. AA_{β}- public key cryptosystem) based upon the Diophantine Equation Hard Problem (DEHP) was proposed. The ciphertext given by the equation $C = k_1 e_{A1} + M^2 e_{A2}$ could be utilized in designing a two way zero knowledge scheme with only one interaction. The proposed scheme does not inherit the attributes of a successful dishonest verifier as what will occur when one mainly depends on the structure of an asymmetric cryptosystem for a zero knowledge scheme. Since the scheme operates on a two way session (unlike established zero knowledge schemes that has minimum of 3 sessions) the process of establishing communication via zero knowledge protocol is fast. Furthermore, since one does also not require more than one interaction to prove or verify an honest verifier or prover (unlike established zero knowledge schemes that require multiple interaction to ensure the probability of lying party to be successful is reduce to $\frac{1}{2^k}$ where k is the number of interactions) the verifying process is also fast.

Introduction

Zero knowledge authentication and identification, involves two entities, the Prover and the Verifier. The Prover in the protocol is trying to authenticate to the Verifier in such a way that no important information (private message) is relayed throughout the communication (zero knowledge). Since both the parties are not facing each other in communication, there might be the case where both entities face difficulty to authenticate each other so as to ensure the security of the protocol.
Meanwhile, there exists adversary who is observing the protocol and tries to eavesdrop in the session.There are several ways that an adversary can be active in the session of authentication and identification scheme (Stinson, 2006):

1. The adversary tries to impersonate the honest Prover, hoping to cause the honest Verifier to accept.
2. The adversary tries to impersonate the honest Verifier, hoping to cause the honest Prover to accept.
3. The adversary is active in the session of the scheme involving both the honest Prover and honest Verifier, hoping to cause both the honest Prover and honest Verifier to accept.

Fiat-Shamir (FS) and Revised Feige-Fiat-Shamir (FFS) Protocol Schemes

The basic Fiat-Shamir protocol scheme is a classical and practical zero knowledge protocol scheme. Developed by Amos Fiat and Adi Shamir in 1986, this scheme involves two parties, the Prover and Verifier. The Prover will prove himself to the Verifier without revealing any useful knowledge (information). The basic Fiat-Shamir protocol scheme which utilizes the square root modulo integer as fundamental primitive is shown below:

Trusted Third Party (TTP) generates $v \equiv s^2 (mod\ n)$, sends s to Prover and v to the Verifier.

Prover		Verifier
Select random r		
Computes $x \equiv r^2 (mod\ n)$	$\longrightarrow$	Chooses $e \in \{0,1\}$
	$\longleftarrow$	
Computes $y \equiv rs^e (mod\ n)$	$\longrightarrow$	Computes $y^2 \equiv xv^e (mod\ n)$

Protocol 1 : Authentication and Identification of Fiat-Shamir Protocol Scheme.

In terms of security, protocol 1 provides no other useful knowledge in the scheme, the honest verifier can always re-run the authentication session until he is satisfied with the results. However, in terms of efficiency, it might not be the best, since running the scheme for several sessions requires time and hence causing the authentication and identification become slower. Since there is a probability of $\left(\frac{1}{2}\right)$ that a dishonest prover can fool the honest verifier, if the session is re-run for t times, then the probability of a dishonest prover cheats in the sessions will be at most $\left(\frac{1}{2}\right)^t = 2^{-t}$. Due to time consumption and efficiency purposes, Fiat-Shamir protocol scheme had been revised and improved by adding the bit lengththat is selected initially as the security parameter. The scheme was modified and revised as follows:

Prover		**Verifier**
Select the bit k as security parameter Select random r and random bit $b \in \{-1,1\}$		
Computes $x \equiv br^2 (mod\ n)$	⟶	Select possible matrices based on the bit chosen by Prover.
	⟵	Select i sub-matrices from the possible set.
Computes $y_i \equiv rs_i^{e_i}\ (mod\ n)$	⟶	
		Computes $y_i^2 \equiv \pm rs_i^{e_i}\ (mod\ n)$

Protocol 2 : Authentication and Identification of Revised Feige-Fiat-Shamir Protocol Scheme.

The Revised Feige-Fiat-Shamir above results in better security as well as efficiency. The security of the scheme is again zero knowledge since no any other information is leaked from the prover to the verifier throughout the session. As for efficiency, since bit commitment is utilized in the scheme, for one session of the protocol, the verifier has now $k!$ ways to form the sub matrices, and then randomly selects any i sub-matrices to send to the prover. Hence, the probability of the dishonest Prover cheats the honest Verifier will be at most $\left(\left(\frac{1}{2}\right)^i\right)^k$. If the bit length chosen is large enough, the probability of cheating the honest Verifier will be even smaller enough. Hence, if the session is running for t times, the probability of honest verifier being cheated turns into even smaller at most $\left(\frac{1}{2}\right)^{ikt} = 2^{-ikt}$. As one can observe, the efficiency is much higher and the security is assured in this revised scheme.

Diophantine Equation Hard Problem (DEHP)

Definition 1

Let $U = \sum_{i=1}^{j} V_i x_i$ be a summation of unknown integers $\{x_i\}$ which are of the same bit length where $\{V_i\}$ is a public sequence of constants. We define the DEHP is solved when $U$is *prf*-solved. That is, the preferred integer set $\{x_i^*\}$ is found from the set of all possible integers $\{x_i\}$ such that $U = \sum_{i=1}^{j} x_i$.

Example 1

Let $U = 8 + 10 + 13 = 31$. Here $x_1^* = 8, x_2^* = 10$and $x_3^* = 13$. A possible incorrect combination could be $x_1' = 9, x_2' = 10$and $x_3' = 12$. Another possible incorrect combination could be $x_1' = 8, x_2' = 11$and $x_3' = 12$.

The AA_{β} Public Key Cryptosystem

We begin with stating that the communication process is between A (Along) and B (Busu), where Busu is sending information to Along after encrypting the plaintext with Along's public key. Along's secret parameters are two prime integers p and q each of n-bit length and $pq > 2^{2n-1} + 2^{2n-2}$.

Definition 1 (Public keys)
Along's public keys are given by

1. $e_{A1} = p^2 q$.
2. $e_{A2} = e$ where $ed \equiv 1 \pmod{pq}$ and e is of $3n$-bit length.

Busu's secret parameters are as follows:

1. The session key given by the integer k_1 of $4n$-bit length.
2. The message M is given by a $2n$ bit even number and $M < 2^{2n-1} + 2^{2n-2}$.

Encryption

Definition 2 (Ciphertext)
The ciphertext is given by $C = k_1 e_{A1} + M^2 e_{A2}$.

Remark 1

- The length of the ciphertext is approximately $7n$ bits, while the length of the message is $2n$ bits. The ratio size between message and ciphertext is 2:7.
- The ratio size between message and public key set is 1:3.

Decryption

Proposition 1
The decryption algorithm is as follows:

i. To begin decryption do $W \equiv Cd \equiv M^2 (\text{mod } pq)$.
ii. Solve the square root of $W (\text{mod } pq)$ (with the help of the Chinese Remainder Theorem).
iii. For each 4 possible message test whether $k_1' = \frac{C-(M_i')^2}{e_{A1}} \in \mathbb{Z}$ or not (where $i = 1,2,3,4$).
iv. If an integer value is obtained, then $M_i' = M$.

Proof:
See (Ariffin et.al., 2012) for the proof of correctness.

In order to ensure the honesty of both the parties, upon communication, the authentication and identification schemes can be added to enhance the security of the cryptosystem. In this case, we improve the scheme of AA_{β}-cryptosystem by introducing the bit length into the scheme, similar as in the Revised Feige-Fiat-Shamir Protocol Scheme.

Along (Prover)		**Busu (Verifier)**
Sends e_{A1}, e_{A2} and e_{A3}	$\longrightarrow$	Encrypts k_1, k_2, M, Send challenge $C = k_1 e_{A1} + k_2 e_{A2} + M e_{A3}$
Reply response $u' = (k'_1 e_{A1}) \pmod{M}$	$\longrightarrow$	Check $u' \in \{odd, even\}$

Protocol 3 : AA_{β} Authentication and Identification scheme with even/odd response.

Upon communication, Busu (Verifier) will send the encrypted message to Along (Prover). Since Busu has generated a random integer k_1 and message M initially, he has $u = (k_1 e_{A1})(mod\ M)$. Prover in return proves himself to be honest by computing $u' = (k'_1 e_{A1})(mod\ M)$. If Along is indeed the honest prover, he can always reply $u' = u$. Hence, the process of authentication and identification has succeeded.

In terms of security, we can observe that in the authentication process the probability of an unsuccessful adversary is $1 - \left(\frac{1}{2}\right)^{l_{k_2}}$, where l_{k_1} is the length of k_1. If the prover is honest, he will be able to compute $u' = (k'_1 e_{A1})(mod\ M)$ correctly using his own private keys. As for the honest verifier, he will be able to verify the honesty of a prover since the computation of $u = (k_1 e_{A1})(mod\ M)$ is with him. Since an eavesdropper as well as both the honest entities learns no new information in the communication session, this ensures the security of the scheme where the probability of any dishonest party to cheat is sufficiently small.

Definition 1:Unconditionally (ε, Q)- secure

An authentication scheme is said to be unconditionally (ε, Q)- secure if the adversary cannot construct a valid response for any new challenge with probability greater than ε, given that the adversary has previously seen valid responses for at most Q challenges.

Proposition 1:
Protocol 1 and 3 are $\left(\frac{Q}{2^j} + \varepsilon, Q\right)$-secure.

Proof:
We observe the scheme for two (2) cases. For the first, suppose in protocol 3, $u = (k_1 e_{A1})(mod\ M)$ is constructed by Busu the verifier at the first stage. Assuming the adversary (dishonest prover) is observing the whole session in the scheme. Then the probability of the adversary successfully determining the correct $u' = u$ is at most ε. The ability to determine the correct u' would enable the adversary to identify whether u' is even or odd is $\left(\frac{1}{2}\right)$.

For the second case, suppose the adversary cannot find in any way to know the challenge of $k_1$and k_2. Then the adversary could only respond to Busu by guessing even or odd of $u' = (k'_1 e_{A1})(mod\ M)$. Since the adversary has the equal chance in guessing even or odd, then the probability of him passing the session is $\left(\frac{1}{2}\right)$. If there are at most Q challenges sent in j sessions, then the probability becomes $\left(\frac{Q}{2^j}\right)$.

Combining the two cases above, it is concluded that the adversary has the maximum probability of $\left(\frac{Q}{2^j} + \varepsilon\right)$ successfully passes the identification for total Q challenges sent. Hence, the protocol scheme is $\left(\frac{Q}{2^j} + \varepsilon, Q\right)$-secure.

Along (Prover)		**Busu (Verifier)**
Sends e_1, e_2 and e_3	⟶	
		Encrypts k_1, k_2, M_i, Send challenge
	⟵	$C_i = k_1 e_{A1} + k_2 e_{A2} + M_i e_{A3}$
Reply response $u' = (k'_1 e_{A1})\ (\text{mod}\ M_i)$	⟶	Check $u'_i \in \{odd, even\}$

Protocol 4 : AA_β Authentication and Identification scheme with multiple even/odd responses.

Proposition 2:

Protocol 4 is $\left(\frac{Q}{2^{nt}} + \varepsilon, Q\right)$-secure.

Proof:

Suppose Busu the verifier encrypt n messages, C_i for $i = 1,2,\ldots,n$ using the same challenge k_1, but different M. Then for one session, Busu will send $C_i = k_1 e_{A1} + M_i^2 e_{A3}$ for $i = 1,2,\ldots,n$for the authentication scheme $u'_i = (k'_1 e_{A1}) \pmod{M_i}$.

Again, we consider two (2) cases. Suppose the adversary is again observing the whole session. Then the probability of the adversary successfully determining every correct $u'_i = u_i$ is at most ε. The ability to determine the correct u' would enable the adversary to identify whether u' is even or odd is $\left(\frac{1}{2}\right)$.

For second case, suppose the adversary does not know the correct even or odd of $u'_i = (k'_1 e_{A1}) \pmod{M_i}$, then the adversary would just simply guess the answers of $u'_i = (k'_1 e_{A1}) \pmod{M_i}$ for every n challenge. Hence, the probability of the adversary successfully passing the identification by guessing whether $u'_i = (k'_1 e_{A1}) \pmod{M_i}$ is odd or even correctly will be at most $\left(\frac{1}{2}\right)$. If there are total of Q challenges sent in t session, then the probability becomes $\left(\frac{Q}{2^{nt}}\right)$. Combining the two cases above, it is concluded that the adversary has the maximum probability of $\left(\frac{Q}{2^{nt}} + \varepsilon\right)$ successfully passes the identification for total Q challenges sent. Hence, the protocol scheme is $\left(\frac{Q}{2^{nt}} + \varepsilon, Q\right)$-secure.

The following corollary indicates the similarity between Protocol 2 and Protocol 4.

Corollary 1:
Protocol 2 is $\left(\frac{Q}{2^{ikt}} + \varepsilon, Q\right)$-secure.

Along (Prover)		**Busu (Verifier)**
Sends e_1, e_2 and e_3	$\longrightarrow$	
		Encrypts k_1, k_2, M, Send challenge
	$\longleftarrow$	$C = k_1 e_{A1} + k_2 e_{A2} + M e_{A3}$
Reply response		
$u' = (k'_1 e_{A1}) \pmod{M}$	$\longrightarrow$	Check $u' = u$

Protocol 5 : AA_β Authentication and Identification scheme.

Proposition 3:
Protocol 5 is $\left(\frac{Q}{2^{2n}} + \varepsilon, Q\right)$-secure.

Proof:
In order to successfully pass the identification, the prover has to be compute $u' = (k'_1 e_{A1}) \pmod{M}$ and reply to the Verifier. Based on the AA_β scheme, the random integer k_1 is $4n$-bits and the message M is $2n$-bits. Also the public keys e_{A1} and e_{A2} are and $3n$-bits respectively. Hence, for every $u' = (k'_1 e_{A1}) \pmod{M}$ computed has the length of approximately $2n$-bits. Again, we consider two cases. As for the first, Busu the verifier sends the challenge$C = k_1 e_{A1} + M^2 e_{A3}$. At the same time, Busu computes $u = (k_1 e_{A1}) \pmod{M}$ for authentication purpose.

Suppose the adversary observe the whole communication session. Then the probability of the adversary successfully determining the correct $u' = u$ is at most ε. For the second case, suppose the adversary observed the whole communication session between the honest prover and the honest verifier, and suppose the adversary does not know anything about the random integers used. Then the adversary can reply the identification by guessing the challenge $u' = (k'_1 e_{A1}) \pmod M$. Since the challenge $u' = (k'_1 e_{A1}) \pmod M$ computed has the length of approximately $2n$-bits, hence the probability of the adversary successfully guessing all the bit correctly is at most $\left(\frac{1}{2^{2n}}\right)$. If there are at most Q challenges sent, then the probability becomes $\left(\frac{Q}{2^{2n}}\right)$. Combining the two cases above, it is concluded that the adversary has the maximum probability of $\left(\frac{Q}{2^{2n}} + \varepsilon\right)$ successfully passes the identification for total Q challenges sent. Hence, the protocol scheme is $\left(\frac{Q}{2^{4n}} + \varepsilon, Q\right)$-secure.

Comparison and Conclusion

Comparing the two scheme suggested in this paper, i.e. Revised Feige-Fiat-Shamir protocol scheme (as in Protocol 4) and AA_β Authentication and Identification scheme (as in Protocol 5), both the systems suggested the bit commitment to design the zero knowledge authentication and identification. In terms of speed, Protocol 4 provides faster speed in authenticating and identifying the prover as compared to Protocol 5. However, it requires more number of challenges in each session. In Protocol 5, the speed might not fast as Protocol 4, but one challenge is sufficient to authenticate and identify the prover's honesty. Clearly, it can be seen that the two-way zero knowledge AA_β Authentication and Identification scheme is more efficient in authenticating and identifying both the entities.

In terms of the size of response data, on the other hand, the response of protocol 4 is much shorter, of even or odd response. While protocol 5 requires one to compute the exact solution of $u = (k_1 e_{A1}) \pmod M$, which could be long enough is the size of integers chosen is sufficiently large.

Also, in terms of security, Protocol 5 uses the direct computation of $u' = (k'_1 e_{A1}) \pmod M$ which is AA_β-DHEP, is more secure. Based on the proofs above, the adversary is required to guess each bit correctly and thus the probability of getting all the bits correctly is relatively very small.

References:

M. R. K.Ariffin, M. A. Asbullah & N. A. Abu (2012). AA_β Public Key Cryptosystem – An Asymmetric Cryptosystem based on the Diophantine Equation Hard Problem. [Online] Available: http://eprint.iacr.org/2011/467.pdf.

M.K. Joseph (2010). Feige-Fiat-Shamir ZKP Scheme Revisited. *IJCIR 2010*, 9-19.

D. Ivan & B.N. Jesper (2008). Commitment Schemes and Zero-Knowledge Protocols.

D.R. Stinson (2006). Cryptography: Theory and Practice. *Chapman & Hall/CRC*, 363-364.

ISBN 978-967-394-084-4

School of Mathematical Sciences
11800 Universiti Sains Malaysia,
Pulau Pinang, MALAYSIA
Website : http://math.usm.my
E-mail : dean_mat@usm.my