UNIVERSITI PUTRA MALAYSIA

EFFICIENT IDENTIFICATION SCHEME IN STANDARD MODEL BASED ON BIVARIATE FUNCTION HARD PROBLEM

TEA BOON CHIAN

IPM 2015 21

EFFICIENT IDENTIFICATION SCHEME IN STANDARD MODEL BASED ON BIVARIATE FUNCTION HARD PROBLEM

By

TEA BOON CHIAN

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirement for the Degree of Master of Science

December 2014

COPYRIGHT

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Master of Science

EFFICIENT IDENTIFICATION SCHEME IN STANDARD MODEL BASED ON BIVARIATE FUNCTION HARD PROBLEM

By

TEA BOON CHIAN

December 2014

Supervisor : Muhammad Rezal Bin Kamel Ariffin, PhD
Institute : Institute for Mathematical Research

The existence of zero knowledge in authentication and identification has become important in cryptography due to the usefulness in authenticating and identifying honesty of both the prover and verifier without relaying any private message in communication. Many identification schemes have been set up, utilizing different assumptions in terms of hardness of the problems including RSA-problem, discrete log problem as well as the lattice problem. Even though many schemes are developed from time to time, the assurance on the scheme's security is important in order to prevent from being impersonated by any unauthorized and cheating parties, which either passively or actively attack the scheme.

Recently, the Diophantine Equation Hard Problem (DEHP) was proposed. With the advantage that this problem only involves simple addition and multiplication operation, it has the potential to be utilized in designing a new identification scheme in the standard model and is more desirable compared to the selected well-known schemes due to its high efficiency of time computation. The new scheme is proposed based on a specific problem of DEHP, that is the Bivariate Function Hard Problem (BFHP) and is proven to be secured against impersonation under passive, active and concurrent attacks, under the assumption that solving the DEHP is hard. Analysis of computation complexity also shows that the newly designed scheme is more efficient than selected well-known existing identification schemes.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

SKIM PENGENALPASTIAN CEKAP DALAM MODEL PIAWAI BERDASARKAN MASALAH SUKAR FUNGSI DUA PEMBOLEH UBAH

Oleh

TEA BOON CHIAN

Disember 2014

Penyelia : Muhammad Rezal Bin Kamel Ariffin, PhD
Institut : Institut Penyelidikan Matematik

Kewujudan ilmu sifar dalam pengesahan dan pengenalpastian menjadi semakin penting dalam kriptografi atas sebab fungsinya dalam menentusah dan mengenalpasti kejujuran kedua-dua pihak pembukti dan pengesah tanpa menyampaikan sebarang mesej rahsia semasa berkomunikasi. Banyak skim pengenalpastian telah dihasilkan dengan menggunakan andaian kesukaran masalah yang berbeza seperti masalah RSA, masalah logaritma diskrit dan juga masalah kekisi. Walaupun banyak skim telah dihasilkan dari semasa ke semasa, keselamatan skim tersebut perlu dipastikan agar dapat menghindari penyamaran oleh sebarang pihak yang tidak sah dan tidak jujur, sama ada secara pasif atau aktif.

Baru-baru ini, masalah sukar persamaan Diofantus telah dikemukakan. Kelebihan masalah tersebut ialah ia hanya melibatkan operasi penambahan dan pendaraban. Justeru ia berpotensi untuk digunakan dalam merekacipta satu skim pengenalpastian yang baru dalam model piawai dan lebih baik berbanding dengan skim-skim terkenal terpilih atas dasar kecekapan yang tinggi dari segi masa untuk melakukan pengiraan. Skim baru berdasarkan kes spesifik daripada DEHP, iaitu masalah sukar fungsi dua pemboleh ubah (BFHP) diperkenalkan dan dibuktikan selamat terhadap serangan penyamaran sama ada secara pasif, aktif mahupun serentak, dengan beranggapan bahawa penyelesaian DEHP adalah sukar. Analisis terhadap kompleksiti pengiraan juga menunjukkan bahawa skim baru ini lebih cekap berbanding dengan skim-skim pengenalpastian popular yang terkenal terpilih.

ACKNOWLEDGEMENT

I would like to express my appreciation to those who have guided me directly and indirectly in completing this research entitled ‘An Efficient Identification Scheme in Standard Model Based on Bivariate Function Hard Problem’. First and foremost, to my supervisor, Assoc. Prof. Dr. Muhammad Rezal bin Kamel Ariffin, who had put a lot of effort in guiding me and helped me to correct and polish this research, so that I am able to complete and present the work perfectly.

Secondly, my heartfelt thanks go to my co-supervisors of Assoc. Prof. Dr. Mohamad Rushdan bin Said and Assoc. Prof. Dr. Mat Rofa bin Ismail in teaching me new and extra knowledge in the field of cryptography and also methods in solving mathematical problems. Without this extra knowledge, I would not be able to produce better results.

Furthermore, I would like to express my appreciation to Mr. Chin Ji Jian, who is currently pursuing his PhD programme in Multimedia University of Cyberjaya. I would like to thank him, who had sacrifice a lot of time in guiding me to understand the zero knowledge identification schemes, which is my main research content and totally new to me. Without his guidance, I would not be able to complete the research in time.

Last but not least, I would like acknowledge my parents, my beloved family and my friends who are also under pressure in doing their research for giving me moral supports throughout my Master studies life.

I certify that a Thesis Examination Committee has met on December 2014 to conduct the final examination of Tea Boon Chian on his thesis entitled "Efficient Identification Scheme in Standard Model Based on Bivariate Function Hard Problem" in accordance with Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.
Members of the Thesis Examination Committee were as follows:

Sharifah Kartini bte Said Husain, PhD
Senior Lecturer
Faculty of Science
Universiti Putra Malaysia
(Chairman)

Azmi b Jaafar, PhD
Associate Professor
Faculty of Computer Science and Information Techonology
Universiti Putra Malaysia
(Internal Examiner)

Siti Hasana bt Sapar, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Internal Examiner)

Eddie Shahril Bin Ismail, PhD
Senior Lecturer
School of Mathematical Sciences
University Kebangsaan Malaysia
(External Examiner)

NORITAH OMAR, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Science. Thememembers of the Supervisory Committee were as follows:

Muhammad Rezal bin Kamel Ariffin, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Chairman)

Mohamad Rushdan bin Md Said, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Member)

Mat Rofa bin Ismail, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Member)

____
BUJANG KIM HUAT, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: ____________________________ Date: __________________

Name and Matric No.: ____

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: ________________________
Name of Chairman of Supervisory Committee: Assoc. Prof. Dr. Muhammad Rezal Bin Kamel Ariffin

Signature: ________________________
Name of Member of Supervisory Committee: Assoc. Prof. Dr. Mohamad Rushdan Bin Md Said

Signature: ________________________
Name of Member of Supervisory Committee: Assoc. Prof. Dr. Mat Rofa Bin Ismail

TABLE OF CONTENTS

Page

ABSTRACT i
ABSTRAK ii
ACKNOWLEDGEMENTS iii
APPROVAL iv
DECLARATION vi
LIST OF TABLES x
LIST OF FIGURES xi
LIST OF ABBREVIATIONS xii
LIST OF SYMBOLS xii

CHAPTER

1 INTRODUCTION 1
1.1 Cryptography 1
1.2 Provable Security in Cryptography 3
1.3 Zero Knowledge Identification Scheme 4
1.4 Research Background 6
1.5 Problem Statement 6
1.6 Research Objectives 7
1.7 Research Questions 7
1.8 Importance of Research 7
1.9 Layout of Thesis 8

2 LITERATURE REVIEW 9
2.1 Fiat-Shamir Identification Scheme 9
2.2 Guillou-Quisquater Identification Scheme 10
2.3 Schnorr’s Identification Scheme 12
2.4 Security of Identification Schemes and the Reset Lemma 14
2.5 Other Identification Schemes and Some Recent Researches 16
2.5.1 Identification Scheme Based on Permuted Kernel Problem 17
2.5.2 Identification Scheme Based on Syndrome Decoding Problem 19
2.5.3 Idenfication Scheme Based on Perceptron Problem 22

3 DIOPHANTINE EQUATION HARD PROBLEM 25
3.1 Linear Diophantine Equation with Infinitely Many Solutions 25
3.2 Diophantine Equation Hard Problem 26
3.3 Bivariate Function Hard Problem 26
3.4 RSA Bivariate Function Hard Problem 28

3.5 DLP Bivariate Function Hard Problem 29

4 A NEW IDENTIFICATION SCHEME BASED ON BIVARIATE FUNCTION HARD PROBLEM 32

4.1 Standard Model of an Identification Scheme 32

4.2 Standard Model Identification Scheme Based on Bivariate Function Hard Problem 32

5 SECURITY ANALYSIS OF IDENTIFICATION SCHEME 38

5.1 Security Model of an Identification Scheme 38

5.2 Security Analysis of Identification Scheme against Impersonation under Passive Attack 39

5.3 Security Analysis of Identification Scheme against Impersonation under Active and Concurrent Attacks 43

6 RESULT DISCUSSIONS 48

6.1 Complexity Analysis of the Identification Scheme 48

6.2 Comparative Analysis against Selected Existing Schemes 49

6.3 Comparative Analysis of Identification Schemes Based on Clock Cycle Performances 50

7 CONCLUSION AND FUTURE WORK 55

REFERENCES 56

BIODATA OF STUDENT 60

LIST OF PUBLICATIONS 61

LIST OF TABLES

Table		Page
6.1	Bit Complexity of basic operation in $\mathbb{Z}$ and $\mathbb{Z}_n$.	48
6.2	Runtime Complexity of ArT Identification Scheme (as proposed in this research)	48
6.3	Runtime Complexity of Fiat-Shamir Identification Scheme.	49
6.4	Runtime Complexity of Guillou-Quisquater Identification Scheme.	49
6.5	Runtime Complexity of Schnorr's Identification Scheme.	49
6.6	Asymptotical Complexity Order of Selected Identification Schemes.	50
6.7	Comparison of Clock Cycle for Bit Length of 32 up to 2048.	51
6.8	Clock Cycles of Fiat-Shamir Identification Scheme.	52
6.9	Clock Cycles of Guillou-Quisquater Identification Scheme.	53
6.10	Clock Cycles of Schnorr's Identification Scheme.	53
6.11	Clock Cycles of Identification Scheme based on BFHP.	53

LIST OF FIGURES

Figure		Page
1.1	Outline of a conventional cryptosystem.	2
1.2	Algorithm of zero knowledge protocol described Quisquater and Guillou in 1990.	4
1.3	Peggy (the Prover) randomly choose her path way.	5
1.4	Victor (the Verifier) chooses an exit path and challenges Peggy.	5
1.5	Peggy reliably appears at the exit Victor names.	5
2.1	Fiat-Shamir (FS) Identification Scheme.	10
2.2	Illustration of FS Identification Scheme.	10
2.3	Guillou-Quisquater (GQ) Identification Scheme.	12
2.4	Illustration of GQ Identification Scheme.	12
2.5	Illustration of Schnorr’s Identification Scheme.	13
2.6	Schnorr’s Identification Scheme.	14
2.7	Identification Scheme based on Permuted Kernel Problem (PKP).	18
2.8	Illustration of Identification Scheme based on Permuted Kernel Problem (PKP).	19
2.9	Identification Scheme based on Syndrome Decoding Problem (SD).	21
2.10	Illustration of Identification Scheme based on Syndrome Decoding Problem (SD).	22
4.1	Illustration of Identification Scheme based on BFHP.	34
5.1	Transcript Queries (Training Phase) of the simulation.	42
5.2	Impersonation Phase (Challenge Phase) of the simulation.	43
5.3	Setup of the simulation of active and concurrent attacks.	46
5.4	Identification Queries (Training Phase) of the simulation.	46
5.5	Impersonation Phase (Challenge Phase) of the simulation.	47

LIST OF ABBREVIATIONS

ATM	-	Auto Transaction Machine
BFHP	-	Bivariate Function Hard Problem
CHA	-	Challenge sent by Verifier
CHAO	-	Challenge Oracle
CLE	-	Constrained Linear Equations
CMT	-	Commitment by Prover
DEHP	-	Diophantine Equation Hard Problem
DLOG	-	Discrete Log Oracle
FS	-	Fiat-Shamir
GQ	-	Guillou-Quisquater
I	-	Impersonator
IBI	-	Identity-Based Identification
KeyGen	-	Key Generator
mpk	-	Master Public Key
MQ	-	Multivariate Quadratic
msk	-	Master Secret Key
OMBFHP	-	One-More Bivariate Function Hard Problem
OMDLP	-	One-More Discrete Logarithm Problem
OMI-RSA	-	One-More RSA Inversion Problem
PIN	-	Personal Identification Number
PKP	-	Permuted Kernel Problem
POK	-	Proof of Knowledge
PP	-	Perceptron Problem
PPP	-	Permuted Perceptron Problem
PPT	-	Probabilistic Polynomial Time
RSP	-	Responses by Prover to Verifier
S	-	Simulator
SD	-	Syndrome Decoding
BFHPO	-	Bivariate Function Hard Problem Oracle
WI	-	Witness Indistinguishability

LIST OF SYMBOLS

$\wedge$	-	Logical conjunction / Logical ‘And’
$\oplus$	-	Exclusive – OR or ‘XOR’
$\parallel$	-	Concatenation
$\overset{R}{\leftarrow}$	-	Random output
$\lfloor x \rfloor$	-	The greatest integer in x
$a\|b$	-	a divides b
G_p	-	Group with prime number of elements
$\mathbb{Z}_{(a,b)}$	-	Integer of interval (a, b)
$\mathbb{Z}^+_{(a,b)}$	-	Postive integer of interval (a, b)
$\mathbb{Z}_N$	-	Group of integer modulo N
$\mathbb{Z}^*_p$	-	Multiplicative group of integer modulo p
$\mathbb{Z}^n$	-	A set of n integers
1^*	-	$(*)$-length string of bits 1
$\mathrm{acc}(\cdot)$	-	Probability that the interaction experiment returns 1
$Adv_A(\cdot)$	-	Success probability of impersonation
$Adv(\cdot)$	-	Probability of winning the game by solving the problem
$A(\cdot)$	-	Addition operation with binary length
d_k	-	Decryption function
e_k	-	Encryption function
$H(\cdot)$	-	Hash function
$\mathcal{IG}(1^k)$	-	Instance generator that on input 1^k output the solution to RSA assumption/Discret Logarithm assumption
$imp - pa$	-	Impersonation under Passive Attack
$imp - aa/ca$	-	Impersonation under Active Attack / Concurrent Attack
$l(\cdot)$	-	Binary length of integer
$M(\cdot)$	-	Multiplication operation with binary length
$Mod(\cdot)$	-	Modular operation with binary length
$MOD_E(\cdot)$	-	Modular exponentiation operation
$\Pr[E]$	-	Probability function of event E
$\mathrm{res}(\cdot)$	-	Probability of the Reset interaction experiment returns 1

CHAPTER 1

INTRODUCTION

1.1 Cryptography

Cryptography is the art and science of secrecy. The application of cryptography in advance technological life has become so common, acknowledgeable and important too. Cryptography's importance especially in encrypting and decrypting the message and information helps to prevent it from being understood by any unauthorized parties. Since ancient times, cryptography has been frequently utilized in military and some secret services to communicate and send the messages secretly. The fundamental and classical task of cryptography is to provide confidentiality by encryption methods (Delfs and Knebl, 2007), that is, the processes of encryption and decryption where it involves the use of secret keys to encipher and decipher the message secretly that are initially agreed by two particular parties.

The following definition indicates all the mathematical notations that are formally used in any cryptosystems (Stinson, 2006).

Definition 1.1
A cryptosystem is a quintuple-(P, C, K, E, D) where the following conditions are satisfied:

1. $P$is a finite set of possible plaintexts.
2. C is a finite set of possible ciphertexts.
3. K, the keyspace, is a finite set of all possible keys.
4. For each $k \in K$, there is an encryption rule $e_k \in E$ and a corresponding decryption rule $d_k \in D$. Each $e_k: P \to C$ and $d_k: C \to P$ are functions such that $d_k(e_k(x)) = x$ for every plaintext element $x \in P$.

The general outline of a conventional cryptosystem is depicted in Figure 1.1 where Alice as the sender, Bob as the receiver, and Eve as the eavesdropper (Van Tilbog, 2000; Stinson, 2006).

The main objective of people studying cryptography and utilize cryptosystems is to provide solutions for some problems (Delfs and Knebl, 2007), that are:

1. **Data Integrity**
   The receiver of a message should be able to check whether the message was modified or not, during transmission, either accidentally or deliberately. No one should be able to substitute a false message for the original message, or for parts of it.

2. **Authentication**
   The receiver of a message should be able to verify its origin. No one should be able to send a message to the receiver and pretend to be the sender (data origin authentication). When initiating a communication, the sender and the receiver should be able to identify each other (entity authentication).

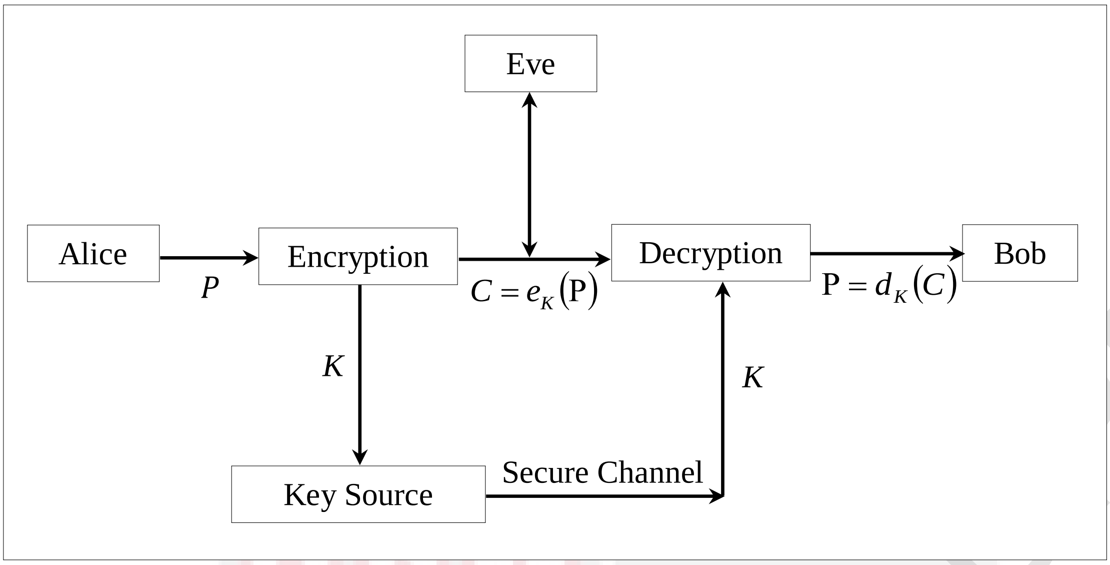

Figure 1.1: Outline of a conventional cryptosystem.

3. **Non-repudiation**
   The sender should not be able to later deny that he sent a message.

4. **Confidentiality**
   When transmitting data, one does not want an eavesdropper to understand the contents of the transmitted messages. The same is true for storing data that should be protected against unauthorized access, for instance by hackers.

Within thousands of years, cryptography has gone through a huge evolution, from the obsolete cryptographic systems such as the Caesar's cipher to the Scytale system and also the Enigma machine until the modern cryptography application such as asymmetric and symmetric cryptography that people fully utilize today. Such evolutions emerged due to the existence of weaknesses in the obsolete cryptographic systems where its security was not guaranteed and would easily be broken by third parties. Since then, many researches have been working on improvising the existing algorithms so as to achieve higher security level.

The idea of modern cryptography especially in mathematical cryptography emphasizes on the utilization of concepts surrounding algebraic number theory, combinatorics, and also group theory. Some mathematical hard problems, such as Integer Factorization Problem, Discrete Logarithm Problem as well as Elliptic Curve which are based on algebraic number theory, are now fully applied especially in asymmetric cryptosystems, such as the RSA Cryptosystem, the El-Gamal Cryptosystem and the Elliptic Curve Cryptosystem. Since then, application such as the internet and banking systems now makes use these cryptosystems.

Besides encrypting and decrypting the message, knowledge of cryptography is also applied in security systems in other aspects. The development of schemes, such as signature schemes and identification schemes allow one to be able to authenticate and verify any users who try to identify themselves. The most common application of such is the Auto Transaction Machine (ATM) in banks, where the user has to input his own Personal Identification Number (PIN) after inserting his ATM card before a further transaction is allowed. Due to the phenomena that the knowledge of cryptography is widely applied in many fields, its security assurance becomes a major concern, that is, how does one be able to verify whether the secret keeper is indeed honest and the secret is secure?

1.2 Provable Security in Cryptography

For so many years, even though more and more cryptographic algorithms and protocols (collectively known as cryptosystems) are being introduced, proposed, improved and modified for practical use, most of the securities of these cryptosystems are yet to be guaranteed due to the lack of provable security analysis. Most of the recent cryptosystems were developed in an ad hoc fashion, which the schemes were attacked, broken, repaired and being attacked again (Dent, 2006).

Since then, cryptologists have tailored research of cryptosystems via providing a formal security proof. Due to this reason, there is heated debate about how cryptologists should formally model the security; the relationship between provable security and complexity theory which is yet to be fully understood; as well as the inconsistency of applying the theory onto the underlying research area and is full of unrealistic simplifying assumptions. A formal security proof or model consists of two definitions (Dent, 2006):

i. It must specify how an arbitrary, probabilistic, polynomial-time attacker can interact with legitimate users of a cryptosystem.

ii. It must state what that attacker should achieve in order to ‘break’ the cryptosystem.

Based on these definitions, there are two general approaches to a formal security proof. The first is the game-based approach, where the attacker interacts with a hypothetical probabilistic algorithm called a challenger. If a cryptosystem is to be proven secure, then one must show that the probability of an arbitrary attacker breaks the cryptosystem is small. Such game-based model has been widely accepted in some cryptosystems including digital signatures (Goldwasser *et al.*, 1998), asymmetric encryption (Rackoff and Simon, 1992), and symmetric encryption (Bellare *et al.*, 1997).

The second approach is to use simulation. In this scenario, one envisages a system in which an arbitrary, probabilistic, polynomial-time attacker can interact with each algorithm of the cryptosystem and also with an arbitrary, probabilistic, polynomial-time environment (Dent, 2006). The strength of this simulation approach is stronger than that of game-based approach in security model, with some examples as suggested by Pfitzmann *et al.* (2000) and Canetti (2001).

Another one most recent discussed topic in the provable security model is the random oracle model. The random oracle model is formalized by introducing and demonstrating the concept of zero knowledge protocols. These entire formal security models suggests that there are deep connections between the computational complexity, security of communication, authentication, randomness and information that challenge cryptologists to elucidate them (Dana and David, 1983) as to ensure provable security has a future in practical cryptography.

1.3 Zero Knowledge Protocol

A zero knowledge protocol is an interactive method for one party to prove to the other that a statement is true, usually mathematical statement, without revealing anything other than the veracity of the statement. Such method plays an important role and has been widely used in cryptography, since it transfers no any knowledge from the sender to the receiver (which “prover” often used to replace sender and “verifier” used to replace receiver in this case) (Delfs and Knebl, 2007).

The concept of zero knowledge was first conceived by Goldwesser *et al.* in 1985. In the paper of Goldwesser *et al.* (1985), the interactive proof systems were not invented, instead the IP (PSPACE) hierarchy of interactive proof systems was invented and the concept of knowledge complexity which includes a measurement of the amount of knowledge about the proof transferred from prover to the verifier was conceived.

The basic zero knowledge protocol was explained by Quisquater and Guillou with a story about a cave (Schneier, 1996; Quisquater and Guillou, 1990). In the explanation, assume that a cave, as illustrated in Figures 1.3, 1.4 and 1.5, has a secret. Someone who knows the magic words can open the secret door in the cave that connects path A and path B. Otherwise, both of the paths lead to dead ends. Peggy (known as the prover) claims that she knows the secret magic words, wants to prove her knowledge to Victor (known as the verifier) without revealing the secret magic words. Figure 1.2 shows the flow of how Peggy convinces Victor about her knowledge.

1. Victor standsoutside the cave (as in Figure 1.3).
2. Peggy walks all the way into the cave and chooses her path, either path A or path B.
3. After Peggy have disappeared into the cave, Victor walks to the point where Peggy was previously (as Figure 1.3).
4. Victor shouts to Peggy, asking her either to:
   a) Come out from path A or
   b) Come out from path B.
5. Peggy complies, using the magic words to open the secret door if she has to.
6. Peggy and Victor repeat the whole procedure for *n* times until Victor satisfies and believes that Peggy is indeed the true prover who knows the true magic words (as Figure 1.4).

Figure 1.2: Algorithm of zero knowledge protocol described by Quisquater and Guillou in 1990.

The illustration of the zero knowledge in the following pages shows that if Peggy is indeed the honest prover, she will always able to open the secret door and appear on the path that Victor named, otherwise, she has only 50% chance of fooling Victor. Hence, as Victor repeatedly tests Peggy for n times, the chance of her being caught lying is at the rate of $1 - \left(\frac{1}{2}\right)^n$.

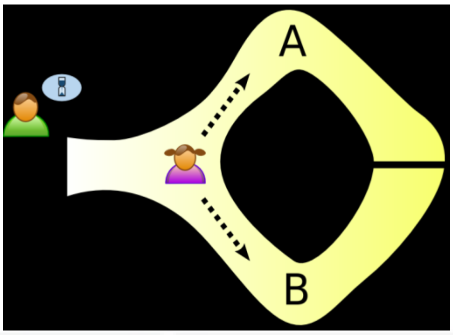

Figure 1.3: Peggy (the Prover) randomly chooses her pathway.

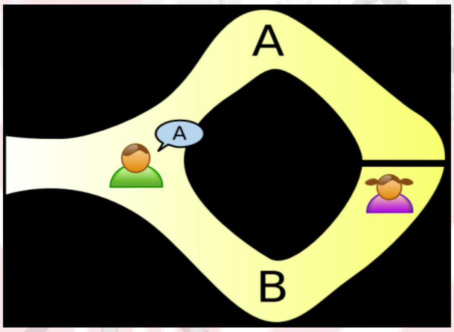

Figure 1.4: Victor (the Verifier) chooses an exit path and challenges Peggy.

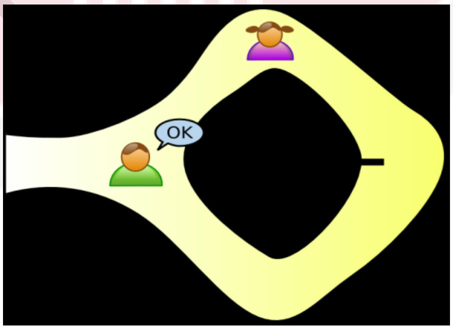

Figure 1.5: Peggy reliably appears at the exit Victor names.

On the other hand, suppose there is an eavesdropper, denoted as Eve recording all the scenes between Peggy and Victor, she will get no information about the truth whether Peggy knows the magic words, since Peggy and Victor can agree beforehand of what they will perform in order to fool Eve. All the above statements proved two problems. Firstly, it is impossible for Victor to convince a third party of the proof's validity. Secondly, it proves that the protocol is zero knowledge, that is no important message is revealed throughout the whole conversation. Generally, a zero knowledge proof must satisfy the following three properties:

i. **Completeness**
If the statement is true, the honest verifier (the one that follows the protocol) will be convinced by an honest prover. That is, the verifier will always able to verify the correctness of the true statement.

ii. **Soundness**
If the statement is false, no cheating prover can convince the honest verifier that it is true, except with some small probability.

iii. **Zero Knowledge**
If the statement is true, no cheating verifier learns anything other than this fact.

Often in zero knowledge protocol, there are two important questions that have always been concerned about. Firstly, how much information does a verifier gain during the interaction or conversation with the prover? Secondly, how much interaction (or what is the least number of interactions) that is needed by the prover to convince the verifier in accepting him? The first question focuses on the property of zero knowledge while the second question deals with the runtime computation. Since these two criteria play important roles in an identification scheme, they should be taken into consideration when setting up or designing a new identification scheme.

1.4 Research Background

The identification scheme in the standard model is a scheme where two entities are trying to prove and identify themselves, respectively in such a way that no secret and private information are revealed throughout the conversation. Also, the impersonation of any adversary contributes to the security problem in the sense that it tries to impersonate in the conversation, hoping that the verifier to accept it as an honest entity. Thus, the provable security of an identification scheme is the most significant criterion in designing new identification schemes against various impersonations.

1.5 Problem Statement

The proposed Diophantine Equation Hard Problem utilizes the simple addition and multiplication processes is embedded within the AA_{β}-Public Key Cryptosystem (Ariffin, 2012). This simple operation computation possesses the potential to be utilized in designing the identification scheme. A proof of security will be provided as to support the newly designed identification scheme in the standard model which is secure against impersonations. The efficiency analysis will then be provided to enhance the desirability in choosing the newly designed identification scheme as a preferable choice compared to some selected existing identification schemes.

1.6 Research Objectives

The objectives of this research are as follows.

1. To propose a new identification scheme in standard model based on Bivariate Function Hard Problem (BFHP).

2. To provide analysis and proofs of security for the new proposed identification scheme based on BFHP against impersonation under passive, active and concurrent attacks.

3. To compare the runtime efficiency and complexity of the new proposed identification scheme based on BFHP with selected existing identification schemes.

1.7 Research Questions

Throughout this research, some questions are proposed as follows.

1. Has the Bivariate Function Hard Problem provided the potential to be utilized in designing a new identification scheme?

2. Is the proposed identification scheme based on Bivariate Function Hard Problem secure against impersonation under passive, active and concurrent attacks?

3. What is the efficiency of the identification scheme based on Bivariate Function Hard Problem compared to the selected existing identification schemes?

4. Is the newly designed identification scheme based on Bivariate Function Hard Problem more desirable compared to the selected existing identification schemes?

1.8 Importance of Research

In this research, a new identification scheme is designed and proposed utilizing a new hard problem which is yet to be found in current cryptology research. Therefore, it is important to prove the security of this new identification scheme in the standard model against various impersonations since provable security remains as the fundamental criterion in providing a secure identification scheme. Also, the runtime computation plays another major role in designing a new identification scheme as time consumption and cost of computation are highly considered when choosing a preferable scheme for practical use.

1.9 Layout of Thesis

In Chapter 2, review of some identification schemes based on existing well known hard problems such as RSA problem and the Discrete Logarithm problem will be given as the initial idea of the research. Some of the famous identification schemes based on the mentioned hard problems and its provable security are reviewed too. This chapter is concluded by reviewing some of the most recent researches in identification schemes, especially in security analysis.

Chapter 3 describes all the definitions and works surrounding the Diophantine Equation Hard Problem and its variants, and how this fundamental primitive was utilized in setting up the AA_{β}-Public Key Cryptosystem. Important definitions and all the necessary conditions which are important to the later part of the thesis are given in this chapter.

In Chapter 4, research and design on the new identification scheme based on the Bivariate Function Hard Problem in the standard model is presented. Chapter 5 describes the formal and complete proof of security of the identification scheme based on the Bivariate Function Hard Problem against impersonation under passive, active and concurrent attacks.

In Chapter 6, discussion about the result of the proposed scheme, its complexity order as well as the efficiency in clock cycle performances of the newly designed identification scheme is given as compared to the selected existing identification schemes. Finally, the conclusion about the results and analysis will be presented in Chapter 7 together with proposition of some future works and researches that can be further considered.

REFERENCES

Ariffin, M.R.K. (2012). A proposed IND-CCA2 Scheme for Implementation on an Asymmetric Cryptosystem Based on the Diophantine Equation Hard Problem. *Proceedings of the 3rd International Conference on Cryptology and Computer Security (ISBN:978-967-394-084-4)* , 193-197.

Ariffin, M.R.K. and Asbullah, M.A., Abu, N.A. and Mahad, Z. (2013). A New Efficient Asymmetric Cryptosystem Based on the Integer Factorization Problem of $N = p^2q$. *Malaysian Journal of Mathematical Sciences* 7(S): 19-37.

Asbullah, M.A. and Ariffin, M.R.K. (2013). A Cost Efficient Decryption Algorithm for the $AA_\beta -$ Cryptosystem. International Arab Journal of Information Technology. (Submitted).

Bellare, M., Desai, A., Jokipii, E. and Rogaway, P. (1997). A Concrete Security Treatment of Symmetric Encryption. *Proc. 38th Annual Symp. Foundation of Computer Science, Washington, DC, USA*: 62-73.

Bellare, M., Namprempre, C., Pointcheval, D. and Semanko, M. (2003). The One-More-RSA Inversion Problems and the Security of Chaum's Blind Signature Scheme. *Journal of Cryptology* 16, 185-215.

Bellare, M. and Palacio, A. (2002). GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks. *Advances in Cryptology - CRYPTOLOGY '02, LNCS* 2442: 162-177.

Beth, T. (1988). A Fiat-Shamir-Like Authentication Protocol for the El Gamal Scheme. *Proceeding of EUROCRYPT '88, LNCS* 330: 77-86.

Canetti, R. (2001). Universally Composable Security: A New Paradigm for Cryptographic Protocols. *Proc. 42nd IEEE Annual Symp. on Foundations of Computer Science, Las Vegas, NV, USA*: 136-145.

Carlson, J, Jaffe, A and Wiles, A. (2006). The Millennium Prize Problems. In S. Cook. *The P versus NP Problem* (pp. 87-106). Clay Mathematics Institute: American Mathematical Society Publisher.

Chaum, D., Evertse, J.H. and van de Graaf, J. (1988). An Improved Protocol for Demonstration Possession of Discrete Logarithm and some Generalizations. *Proceedings of EUROCRYPT '87, LNCS* 304: 127-141.

Chin, J.J. and Heng, S.H. (2012). Security Upgrade for a k-Resilient Identity-Based Identification Scheme In The Standard Model. *The 3rd International Conference on Cryptology and Computer Security 2012 (Cryptology 2012).*

Dana, A. and David, L. (1983). In *Provable Security of Cryptosystem: A Survey*, Yale University, pp. 3.

Delfs, H. and Knebl, H. (2007). In *Introduction to Cryptography: Principles and Applications*, (2nd Ed.). New York: Springer-Verlag Berlin Heidelberg.

Dent, A.W. (2006). Fundamental Problems in Provable Security and Cryptography. *Phil. Trans. R. Soc. A* 364: 3215-3230.

El Gamal, T. (1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithm. *IEEE Transaction on Information Theory* 31:469-472.

Fiat, A. and Shamir, A. (1986). How to Prove Yourself: Practical Solutions to Identification and Signature Problem. *Advances in Cryptology, CRYPTO '86, LNCS* 263: 186-194.

Goldwasser, S., Micali, S. and Rackoff, C., (1985). The Knowledge Complexity of Interactive Proof Systems. *SIAM Journal on Computing (Philadelphia: Society for Industrial and Applied Mathematics)*18 (1): 186-208.

Goldwasser, S., Micali, S. and Rivest, R. (1998). A Digital Signature Scheme Secure against Adaptive Chosen-Message Attack. *SIAM J. Computing* 17: 281-308.

Guillou, L. and Quisquater, J.J. (1988). A "Paradoxical" Identity-Based Signature Scheme Resulting from Zero Knowledge. *Advances in Cryptology – CRTYPTO '88, LNCS* 403: 216-231.

Gunter, C.G. (1989). Diffie-Hellman and El Gamal Protocol with One Single Authentication Key. *Advances in Cryptology, EUROCRYPT '89, LNCS* 434: 29-37.

Herrmann, M. and May, A. (2008). Solving Linear Equations Modulo Divisors: On Factoring Given Any Bits. *ASIACRYPT 2008, LNCS* 5350: 406-424.

Hwang, R.J., Su, F.F., Yeh, Y.S. and Chen, C.Y. (2005). An Efficient Decryption Method for RSA Cryptosystem. *The 19th International Conference on Advanced Information Networking and Applications*, *AINA'05* Taiwan1: 585-590.

Kawachi, A., Tanaka, K. and Xagawa, K. (2008). Concurrently Secure Identification Schemes Based on the Worst-Case Hardness of Lattice Problems. *ASIACRYPT 2008*, *LNCS* 5350: 372-389.

Knudsen, L.R. and Meier, W. (1999). Cryptanalysis of an Identification Scheme Based on the Permuted Perceptron Problem. *EURPCRYPT '99, LNCS* 1592" 363-374.

Mao, W. (2004). In *Modern Cryptography: Theory and Practice*. Prentice Hall PTR.

Michael, R.G. and David, S.J. (1979). In *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W.H. Freeman.

Pfitzmann, B. and Waidner, M. (2000). Composition and Integrity Preservation of Secure Reactive System. *Proc 7th ACM Conf. Computer and Communication Security, Athens, Greece*; 245-254.

Pierce, J.N. (1967). Limit Distribution of The Minimum Distance of Random Linear Codes. *IEEE Trans. Inform Theory* (IT-13): 595-599.

Pointcheval, D. (1995). A New Identification Scheme Based on the Perceptrons Problem. *EUROCRYPT '95, LNCS* 950: 319-328.

Pointcheval, D. and Poupard, G. (2003).A New NP-Complete Problem and Public-key Identification. *Des. Codes Cryptography 28*; 1: 5-31.

Quisquater, J.J. and Guillou, L. (1990). How to Explain Zero Knowledge Protocols to Your Children. *Advances in Cryptology - CRYPTO '89, Proceedings*435: 628-631.

Rivest, R.L., Shamir, A. and Adleman, L. (1978). A Method for Obtaining Digital Signature and Public Key Cryptosystems. *Communication of The ACM '78,* Vol. 21: 120-126.

Sakumoto, K., Shirai, T. and Hiwatari, H. (2011). Public-Key Identification Schemes Based on Multivariate Quadratic Polynomials. *Advances in Cryptology - CRYPTO '11, LNCS* 6841: 703-721.

Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, (2nd Ed.). New York: John Wiley & Sons, Inc.

Schnorr, C.P. (1989). Efficient Identification and Signature for Smart Card. *Advances in Cryptology - CRYPTO '89, LNCS* 435: 239-252.

Shamir, A. (1984a). Identity-based Cryptosystems and Signature Scheme. *Advances in Cryptology - CRYPTO '84, LNCS* 196: 47-53.

Shamir, A. (1984b). A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem. *IEEE Trans. Information Theory*, Vol. IT-30(5), September 1984, pp. 699-704.

Shamir, A. (1990). An Efficient Identification Scheme Based On Permuted Kernels. *Advances in Cryptology – CRYPTO '89, LNCS* 435: 606-609.

Shoup, V. (1997). Lower Bounds for Discrete Logarithm and Related Problems. *Advances in Cryptology – EUROCRYPT '97, LNCS* 1233: 256-266.

Stern, J. (1996). A New Paradigm For Public Key Identification. *IEEE Transaction of Information Theory*; 42(6): 749-765.

Stinson, D.R. (2006). In *Cryptography: Theory and Practice*, ed. K.H. Rosen, pp. 1-2/363-364. Chapman & Hall/CRC.

Van Tilborg, H.C.A. (2000). *Fundamentals of Cryptology: A Professional Reference and Interactive Tutorial*. Boston, Dordrecht, London: Kluwer Academic Publishers.