UNIVERSITI PUTRA MALAYSIA

SIDE CHANNEL ANALYSIS ON AA$^{\beta}$ CRYPTOSYSTEM AND A SIGNING SCHEME BASED ON BIVARIATE FUNCTION HARD PROBLEM AND DISCRETE LOGARITHM PROBLEM

AMIR HAMZAH BIN ABD GHAFAR

IPM 2015 4

SIDE CHANNEL ANALYSIS ON AA_β CRYPTOSYSTEM AND A SIGNING SCHEME BASED ON BIVARIATE FUNCTION HARD PROBLEM AND DISCRETE LOGARITHM PROBLEM

By

AMIR HAMZAH BIN ABD GHAFAR

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

September 2015

DEDICATIONS

Bismillah ir-Rahman ir-Rahim

To NS and AH,
Ayah and Emak,
Alice, Bob and Eve:

`All’s fair in love, war, and crypto.`

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

SIDE CHANNEL ANALYSIS ON AA_β CRYPTOSYSTEM AND A SIGNING SCHEME BASED ON BIVARIATE FUNCTION HARD PROBLEM AND DISCRETE LOGARITHM PROBLEM

By

AMIR HAMZAH BIN ABD GHAFAR

Sepetember 2015

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

This study has two main parts. The first part discusses side-channel attack on the AA_β cryptosystem. The encryption scheme was introduced in 2012. Hence this attack is aimed to address new rooms for improvements for AA_β. Side-channel attack is an attack on the implementation of a cryptosystem by collecting physical data that are leaked by the machines which execute the cryptosystem. The components of side-channel attacks that are used in this study are timing attack and power attack. We mathematically model the attacks and prove the viability of such attacks. Then we provide solutions on how to overcome.

The second part of this thesis presents a new digital signing scheme that utilizes the Bivariate Function hard Problem (BFHP) and Discrete Logarithm Problem (DLP) as its underlying mathematical hard problems. BFHP is the same problem used by AA_β while DLP is the established hard problem used by one of the first public-key cryptosystem, Diffie-Hellman cryptosystem. We study and analyze this new scheme with respect to its security and performance when compared to other widely-used digital signing schemes.

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

ANALISIS SALURAN SISI TERHADAP SISTEMKRIPTO AA_β DAN SKIM TANDATANGAN BERASASKAN MASALAH SUKAR FUNGSI DUA PEMBOLEHUBAH DAN MASALAH LOGARITMA DISKRIT

Oleh

AMIR HAMZAH BIN ABD GHAFAR

September 2015

Pengerusi : Muhammad Rezal Bin Kamel Ariffin, PhD
Fakulti : Institut Penyelidikan Matematik

Kajian ini mempunyai dua bahagian penting. Pertama, ia membincangkan mengenai analisis/serangan saluran sisi terhadap sistemkripto AA_β. Skim penyulitan ini baru sahaja diperkenalkan pada tahun 2012. Justeru, serangan seperti ini bertujuan bagi mencari ruang penambahbaikan pada sistemkripto ini. Serangan saluran sisi secara amnya bermaksud serangan terhadap implementasi suatu sistemkripto dengan mengumpul data fizikal yang akan dihasilkan oleh mesin yang mengendalikan sistemkripto itu. Komponen serangan ini yang diguna pakai dalam kajian ini ialah serangan melalui masa dan serangan melalui kuasa. Kami membentuk model matematik serangan ini dan membuktikan kejayaan serangan tersebut. Kemudian kami memberi penyelesaian untuk mengatasi serangan.

Bahagian kedua tesis ini pula membentangkan suatu skim tandatangan digital baru yang menggunakan Masalah Sukar Fungsi Dua Pembolehubah serta Masalah Logaritma Diskrit sebagai masalah sukar matematiknya. MSFDP ialah masalah yang sama digunakan oleh AA_β manakala MLD pernah digunakan sebelumnya oleh salah satu sistemkripto kekunci-awam yang pertama; sistemkripto Diffie-Hellman. Kajian ini juga mengetengahkan analisis keselamatan serta analisis prestasi terhadap skim baru ini berbanding dengan skim tandatangan digital sedia ada.

ACKNOWLEDGEMENTS

Bismillah ir-Rahman ir-Rahim.

To Allah the creator of all the creations, all praise be to Him who is eternal and exists without a place, the Most Beneficent and the Most Merciful, the Lord of the Worlds.

High gratitude and respect to my supervisor, Associate Professor Dr Muhammad Rezal bin Kamel Ariffin for his never ending guidance and patience pushes me forward throughout this journey. Sincere appreciation goes to my co-supervisor, Associate Professor Dr Mat Rofa bin Ismail for giving me spiritual motivation in completing this thesis.

As to my wife, Nurul Syarina bt Shaharuddin, thank you for your never ending love and understanding of my lifelong passion - cryptography.

Nothing can replicate the care and support from my parents, Abd Ghafar bin Md Din and Kamaliah binti Abd Rahman as they are my inspiration to make this life better everyday .

Kind regards to my friends who row in the same ship of cryptography; Muhammad Asyraf, Zahari Mahad, Tea Boon Chian, Azlan Daud and many other whose names shall never be forgotten because without their contributions and teachings, this thesis will never be completed.

See you all again in the next adventure!

I certify that a Thesis Examination Committee has met on September 18th 2015 to conduct the final examination of Amir Hamzah bin Abd Ghafar on his thesis entitled ”Side Channel Analysis on AA_β Cryptosystem and A Signing Scheme Based on BFHP and DLP” in accordance with the 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:

Zanariah binti Abdul Majid, PhD
Professor
Faculty of Science
Universiti Putra Malaysia
(Chairperson)

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

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

Hailiza binti Kamarulhaili, PhD
Professor
School of Mathematical Sciences
Universiti Sains Malaysia
(External Examiner)

ZULKARNAIN ZAINAL, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 27 October 2015

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy.

The members of the Supervisory Committee were as follows:

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

Mat Rofa bin Ismail, PhD
Assosiate 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: Amir Hamzah bin Abd Ghafar, GS33770

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: Muhammad Rezal bin Kamel Ariffin

Signature: ______________________________
Name of
Member of
Supervisory
Committee: Mat Rofa bin Ismail

TABLE OF CONTENTS

	Page
ABSTRACT	i
ABSTRAK	ii
ACKNOWLEDGEMENTS	iii
APPROVAL	iv
LIST OF TABLES	xi
LIST OF FIGURES	xii
LIST OF ALGORITHMS	xiii
LIST OF ABBREVIATIONS	xiii

CHAPTER

1 **INTRODUCTION** 1
- 1.1 Cryptography 1
- 1.2 Asymmetric Key Cryptography 3
  - 1.2.1 Encryption Algorithm 3
  - 1.2.2 Digital Signature 4
- 1.3 Attacks in Cryptography 5
- 1.4 Research Motivation 7
- 1.5 Problem Statement 7
- 1.6 Research Objective 7
- 1.7 Research Methodology 7
- 1.8 Contribution of Research 8
- 1.9 Scope and Limitation of the Study 8
- 1.10 Overview of the Thesis 9

2 **MATHEMATICAL AND CRYPTOGRAPHIC BACKGROUND** 10
- 2.1 Introduction 10
- 2.2 Hard Mathematical Problems in Cryptography 10
  - 2.2.1 Integer Factorization Problem 10
  - 2.2.2 Discrete Logarithm 11
  - 2.2.3 Linear Diophantine Equations with Infinitely Many Solutions 12
  - 2.2.4 Bivariate Function Hard Problem 13
- 2.3 Continued Fraction 15
  - 2.3.1 Legendre's Theorem (1798) 16

3 **AA_β CRYPTOSYSTEM** 17
- 3.1 Introduction 17
- 3.2 Hard Mathematical Problem 17
- 3.3 AA_β Algorithm 17

3.4 Implementation of AA_β 19
3.4.1 Multiple-Precision Modular Arithmetic 20
3.4.2 Attacking the Implementation of AA_β 20

4 **SIDE CHANNEL ANALYSIS** 22
4.1 Introduction 22
4.2 Modular Exponentiation 23
4.2.1 Repeated Squaring Algorithm 24
4.2.2 Montgomery Algorithm 25
4.2.3 Karatsuba Algorithm 28
4.3 Timing Analysis 30
4.3.1 Kotcher's Attack 30
4.3.2 Schindler's Attack 31
4.3.3 Brumley and Boneh's Attack 33
4.4 Power Analysis 34
4.4.1 Simple Power Analysis 35
4.4.2 Differential Power Analysis 36
4.5 Prevention of Side Channel Analysis 36
4.5.1 RSA Blinding (Yan, 2007) 37
4.5.2 Time Delay 37
4.5.3 Secure Programming (Witteman and Oostdijk, 2008) 37
4.5.4 Anti-Tampering Devices 37

5 **TIMING ATTACK ON AA_β** 38
5.1 Introduction 38
5.2 The Attack Model 38
5.3 Attacking AA_β Cryptosystem using Timing Attack 39

6 **POWER ANALYSIS** ON AA_β 47
6.1 Introduction 47
6.2 The Attack Model 49
6.3 Trace Pair Analysis using λ and $\lambda+1$ 54
6.3.1 If $\lambda < \lambda+1 < \frac{pq}{d}$ 54
6.3.2 If $\lambda < \frac{pq}{d} < \lambda+1$ 55
6.4 Finding the Value of λ 56
6.5 Retrieving λ_{approx} to find p 60

7 **COUNTERMEASURES AGAINST SIDE CHANNEL ATTACK ON AA_β** 65
7.1 Introduction 65
7.2 AA_β Blinding 65
7.2.1 Discussion 67
7.3 Time Delay 67
7.3.1 Randomized Time Delay 67
7.3.2 Standardized Time Delay 68

8 **SIGNING SCHEME BASED ON BFHP AND DLP** 69
8.1 Introduction 69
8.2 Hard Mathematical Problem and The Structure of The Scheme 69
8.3 Working Algorithms 69
8.4 Security Analysis 71
8.5 Performance Analysis 73

9 **CONCLUSION AND FUTURE WORK** 75
9.1 Conclusion 75
9.2 Future Work 75

REFERENCES 76
APPENDICES 79
BIODATA OF STUDENT 79
LIST OF PUBLICATIONS 80

LIST OF TABLES

Table **Page**

1.1 Important Jargons in Cryptography 1

1.2 Difference between Symmetric Key and Asymmetric Key Cryptography 3

5.1 The execution time using the combination of MSB 4-bits 42

5.2 The execution time of W_1, W_2 and W_3 (a) 45

5.3 The execution time of W_1, W_2 and W_3 (b) 45

6.1 Finding the full bits of λ 59

6.2 The value of intermediates, i_t and k_t corresponding with their t-th iteration. 63

8.1 Operations in signature schemes 73

LIST OF FIGURES

Figure **Page**

4.1 The full setup of side channel attack (Petric, 2011). 23

4.2 The number of extra reductions falls significantly at the integer multiple of p 32

4.3 SPA leaks from Repeated Squaring Algorithm used in implementation of RSA (Kocher et al., 2011) 35

4.4 Two traces and their difference that shows their point of divergence (Kocher et al., 2011) 36

5.1 The execution time using the combination of MSB 4-bits 43

6.1 Pattern of power traces for $\left|\Delta_{\gamma 1} - \Delta_{\gamma 2}\right| < \varepsilon$. 48

6.2 Pattern of power traces for $\left|\Delta_{\gamma 1} - \Delta_{\gamma 2}\right| < \varepsilon$. 48

6.3 The expected power trace for $\lambda < \lambda + 1 < \frac{pq}{d}$. 54

6.4 The expected power traces for $\lambda < \frac{pq}{d} < \lambda + 1$. 55

LIST OF ALGORITHMS

Algorithm **Page**

3.1a AA_β Key Generation algorithm 18

3.1b AA_β Encryption algorithm 18

3.1c AA_β Decryption algorithm 19

3.2 Multi-Precision Division Algorithm 21

4.1 Left-to-right algorithm 25

4.2 Right-to-left algorithm 25

4.3a Left-to-right with Montgomery Algorithm 27

4.3b Montgomery Algorithm 28

5.1 Timing Attack AA_β 46

6.1 λ Retrieval Algorithm 57

7.1 AA_β Decryption Algorithm (with blinding) 67

8.1a Key Generation algorithm 70

8.1b Signing algorithm 70

8.1c Verification algorithm 70

LIST OF ABBREVIATIONS

DES	Data Encryption Standard
DHKE	Diffie-Hellman Key Exchange
DLP	Discrete Logarithm Problem
DPA	Differential Power Analysis
GNFS	General Number Field Sieve
IFP	Integer Factorization Problem
LSB	least significant bit
MPA	Multiple-Precision Arithmetic
MSB	most significant bit
SPA	Simple Power Analysis

CHAPTER 1

INTRODUCTION

1.1 Cryptography

Cryptography is derived from two Greek words, *kryptos* and *graphein* which means “hidden” and “writing” respectively. The meaning of these words literally become the main aim of cryptography. The art and science of securing writings or messages begun since early civilization when human started to communicate and need to hide their communication. Every encryption or ‘securing’ of the messages using a secret key, there must be an attempt to retrieve the secrets - either the secrete messages or the secret keys - by the adversary. The attempt or attack in most cases are rogue and fraudulent. It is a product of a process called *cryptanalysis*.

Before we delve further into the topic, it is important to know first some jargon in Table 1.1 that are widely used in cryptography.

Table 1.1: Important Jargons in Cryptography

Jargon	Meaning
Plaintext	Original message that needs to be secured.
Ciphertext	Plaintext that has been encrypted and should be impossible to read.
Encryption	A process to transform plaintext to ciphertext using a key.
Decryption	A process to transform back the ciphertext to plaintext using a key.

For a classic example of cryptography, a sender of a plaintext, known as Alice will encrypt her plaintext then send them to her friend, Bob in the form of ciphertext. Bob then needs to decrypt the ciphertext to read the original plaintext. The goals of this process can be categorized into four main points:

i. **Confidentiality.** Nobody except Alice and Bob should know the content of the plaintext.

ii. **Authentication.** Bob should be able to know that the ciphertext is truly coming from Alice, not anybody else.

iii. **Integrity.** Bob should be able to detect if the ciphertext has been altered during transmission.

iv. **Non-Repudiation.** Alice cannot deny her involvement in sending the plaintext should any future dispute occurs.

To achieve all these goals, a proper system to conduct the process should be put into order. This system is called *cryptosystem*. Definition 1.1 gives you the insight of a cryptosystem.

Definition 1.1 (Katz and Lindell, 2007) *Let m denotes the plaintext, c denotes the ciphertext and k denotes the key. A cryptosystem is defined by three algorithms:*

1. *Key Generation algorithm, Gen is a probabilistic algorithm to derive keys used in the cryptosystem. In most cases, this algorithm uses pseudorandom number generator (PRNG) to output k.*
2. *Encryption algorithm, Enc is a deterministic or probabilistic algorithm that takes plaintext, m as its input and produces ciphertext, c using key, k.*

$$Enc_k(m) = c$$

3. *Decryption algorithm, Dec is a deterministic algorithm that takes ciphertext, c as its input and gives back original plaintext, m using key, k.*

$$Dec_k(Enc_k(m)) = m$$

or

$$Dec_k(c) = m$$

Early cryptographic applications were mostly used by governments or military to deceive their enemies. However, in the modern cryptography world, cryptography is used everywhere and everyday. To achieve secure electronic communication or transaction, there must be either one or both **symmetric** and **asymmetric key cryptography** involved.

Symmetric key cryptography uses a component of secret keys which has to be shared between Alice and Bob. Since ancient times, cryptosystems such as Caesar Cipher, Playfair cipher, Vigenere cipher and many more uses this fundamental concept of key sharing to achieve confidentiality. But, towards the digital age, key sharing can be cumbersome especially if the communication involves more than two parties and must be done in relatively short time. Government sectors and industrialists found that private key cryptography used to communicate securely is ineffective. They have to distribute all the shared keys manually and this increases the risk for the keys to be exposed to the enemy.

Therefore, circa 1970s, asymmetric key cryptography was introduced. Unlike symmetric cryptography, asymmetric key cryptography uses two different keys which are called public and private keys. The public key is accessible by anyone while the private key is kept by the key's owner only. Table 1.2 shows the difference between symmetric and asymmetric key cryptography.

Table 1.2: Difference between Symmetric Key and Asymmetric Key Cryptography

Differences	Symmetric Key Cryptography	Asymmetric Key Cryptography
Encryption key	Shared secret key, k_{shared}	Public key, k_{pub}
Decryption key	Shared secret key, k_{shared}	Private key, k_{priv}
Modes of Operation	1. Substitution 2. Transposition	1. Modular arithmetic 2. Exponentiation 3. Elliptic curve etc.

1.2 Asymmetric Key Cryptography

In 1976, Whitfield Diffie and Martin Hellman began the revolution of asymmetric key cryptography by introducing Diffie-Hellman Key Exchange (DHKE) (Diffie and Hellman, 1976). The significant importance possessed by DHKE is to share a secret key without the involved parties to meet each other. The parties only need to give their public keys to extract the shared secret key.

This solves the key management problem that has been a disadvantage of using symmetric key cryptography. In the case of DHKE, both the keys; private and public keys are related using a mathematical relation called modular arithmetic.

Asymmetric key cryptography have two main functions. The first is to act as an encryption algorithm to encrypt information so it cannot be seen by the enemy. The other one is to act as an authentication means called digital signing algorithm.

1.2.1 Encryption Algorithm

A year after DHKE was introduced, the first asymmetric key encryption scheme called RSA was introduced (Rivest et al., 1978). RSA utilizes Integer Factorization Problem (IFP) and the e-th root problem as its hard mathematical problem. After that, many other asymmetric encryption schemes such as the ElGamal encryption scheme (ElGamal, 1985), the Elliptic Curve encryption scheme and its variants (Koblitz, 1987) and the NTRU encryption scheme (Hoffstein et al., 1998). All the mentioned schemes are practical and their implementations are used widely in today's digital applications.

Since this thesis mostly covers on asymmetric key, Definition 1.2 slightly modifies Definition 1.1 to define asymmetric key encryption scheme.

Definition 1.2 (Katz and Lindell, 2007) *Let m denotes the plaintext, c denotes the ciphertext, k_{pub} denotes the public key and k_{priv} denotes the private key. An encryption scheme, Π_{enc} is defined by three algorithms:*

1. *Key Generation algorithm, Gen is a probabilistic algorithm to derive both k_{pub} and k_{priv}.*
2. *Encryption algorithm, Enc is a deterministic or probabilistic algorithm that takes plaintext, m as its input and produces ciphertext, c using public key, k_{pub}.*
$$Enc(k_{pub}, m) = c$$
3. *Decryption algorithm, Dec is a deterministic algorithm that takes ciphertext, c as its input and gives back original plaintext, m using private key, k_{priv}.*
$$Dec(Enc(k_{pub}, m), k_{priv}) = m$$
or
$$Dec(c, k_{priv}) = m$$

Next we will move to digital signature.

1.2.2 Digital Signature

Digital signature has a very important role in the digital world today. It gives the notion of *authentication, integrity* and *non-repudiation* in every message or data sent. Some signature schemes are derived from its encryption scheme. For example, the RSA digital signing scheme uses its private key to generate a signature of a message or data while its public key to verify the signature. In general most schemes use the same hard mathematical problem from their encryption scheme to be embedded into its corresponding digital signature scheme.

Some of digital signature schemes that are being used today are RSA's Public-Key Cryptography Standards (PCKS) (Jonsson and Kaliski, 2003), DSA (Digital Signature Algorithm) and its elliptic curve variants which was endorsed by American's National Institute of Standards and Technology (Kravitz, 1993) and Schnorr signature (Schnorr and Jakobsson, 2000).

As with the encryption algorithm, we will now produce a definition with regards to the Digital Signature Scheme.

Definition 1.3 (Katz and Lindell, 2007) *Let m denotes the plaintext, s denotes the signature, k_{pub} denotes the public key and k_{priv} denotes the private key. A signature scheme, Π_{sig} is defined by three algorithms:*

1. *Key Generation algorithm, Gen is a probabilistic algorithm to derive both k_{pub} and k_{priv}.*
2. *Signing algorithm, Sig is a deterministic or probabilistic algorithm that takes plaintext, m as its input and produces a signature, s using public key, k_{priv}.*

$$Sig(k_{priv}, m) = s$$

3. *Verifying algorithm, Ver is a deterministic algorithm that takes ciphertext, s as its input and gives back original plaintext, m using private key, k_{pub}.*

$$Ver(Sig(k_{priv}, m), k_{pub}) = m$$

or

$$Ver(s, k_{pub}) = m$$

1.3 Attacks in Cryptography

While cryptography deals with building a cryptosystem, cryptanalysis tackles the method of breaking the cryptosystem. Analysis or 'attack' is a very important step not only in the academic world, but more importantly in real world application because every successful attack will be used as a benchmark to strengthen the security of a target cryptosystem.

Attackers or adversaries in cryptography can be classified into two (Martin, 2012):

1. *Passive Attacker* is an attacker who only watches, hears or monitors the communication without doing any attempt to alter the communicated data. The attacker only tries to disrupt the confidentiality of the communication.
2. *Active Attacker* is an attacker who actively intercepts the communicated data and modifies it. The attacker tries to disrupt the confidentiality, authenticity and data integrity of the communication.

Now we will look at categories of attacks that can be launched on encryption scheme:

1. *Ciphertext only attack* is where the adversary tries to deduce the plaintext or decryption key by only having ciphertext during a passive attack. If a cryptosystem is vulnerable to this kind of attack, it is completely insecure cryptosystem.

2. *Known plaintext attack* is where the adversary know some of the plaintexts with their respective ciphertexts and tries to deduce the secret part of the cryptosystem.

3. *Chosen plaintext attack* is where the adversary has access to the encryption oracle and can choose plaintext to be encrypted. The ciphertexts produced and the chosen plaintext are used to deduce any previous unknown plaintexts encrypted using the same encryption oracle. If a cryptosystem is secure against this attack, we called it CPA-secure cryptosystem.

4. *Adaptive chosen plaintext attack* is similar to chosen plaintext attack but the choices of plaintext may rely on ciphertext encrypted from the previous requests to the encryption oracle.

5. *Chosen ciphertext attack* is where the adversary has access to the decryption oracle thus can choose any ciphertext to be decrypted. While the adversary has access to the decryption oracle, but it does not means the adversary has the decryption key because the key may be stored securely in the oracle. The main aim of this attack is to gain knowledge of plaintext of non-chosen ciphertext and ultimately the decryption key. Side channel attack which is the focus of this thesis falls under this category.

6. *Adaptive chosen cipherext attack* is similar to chosen ciphertext attack but the choices of ciphertext may rely on plaintext decrypted from previous requests to the encryption oracle.

We now provide the reader with fundamental categories of attack upon digital signature scheme:

1. *Key-only attack* is when the adversary only knows the signer's public key or signing key.

2. *Known message attack* is the same like known plaintext attack in encryption scheme plus the adversary knows the signature generated from the messages.

3. *Adaptive chosen message attack* is the most severe that any adversary can mount onto the signer. In this attack, the adversary has access to random oracle which will sign any message passed through it. Thus, the adversary not only can obtain signatures, $s_1, s_2, \cdots s_i$ from the messages, $m_1, m_2, \cdots m_i$, the adversary chooses, but also request signatures, $s_{i+1}, s_{i+2}, \cdots$ from the messages, $m_{i+1}, m_{i+2}, \cdots$ which depend on $m_1, m_2, \cdots m_i$.

For more explanation regarding attacks on signatures, we can refer to (Goldwasser et al., 1988). All of the stated attacks are realistically can be done in real world implementation. Therefore, to show its security level, it is very important to provide analysis of these attacks onto a cryptosystem.

Next, introductory details of this thesis will be given.

1.4 Research Motivation

AA_β cryptosystem is a new encryption scheme. To use it without any doubt, the cryptosytem must first be tested by several self-simulated attacks. Side channel analysis or attack is a practical method that can be used by attackers in real-world scenarios because it attacks the implementation of the cryptosystem. After the analysis, if there is no successful side-channel attack that could be launched upon the implementation of the cryptosystem, it gives a higher sense of security for cryptosystem. However, if there is an attack that successfully retrieve the secret key from the cryptosystem, it means the implementation should be strengthened before the cryptosystem can be used by the public.

Another motivation is to build a signing scheme that uses BFHP as its underlying security strength. Being a newly introduced hard mathematical problem, there is no signing scheme that utilizes BFHP as its security strength. The advantage of using BFHP is due to its simplicity which increases the efficiency of the signing scheme significantly. More details about BFHP is discussed in Subsection 2.2.4.

1.5 Problem Statement

1. Is AA_β cryptsystem susceptible from any side channel attack?
2. If there is a side-channel attack against AA_β, what is the best preventive measure that can be conducted?
3. Can we build a new digital signing scheme based on Bivariate Function Hard Problem (BFHP) and Discrete Logarithm Problem (DLP)?

1.6 Research Objective

1. To conduct side-channel attacks on AA_β cryptosystem via timing and power analysis.
2. To present countermeasures that can be used if the side-channel attack against AA_β exists.
3. To develop a new digital signing scheme that uses BFHP and DLP.

1.7 Research Methodology

Side channel attack is categorized as chosen ciphertext attack. It focuses on the decryption algorithm of a cryptosystem. Its first strategy is to collect the external data that has been released by the software or hardware that compute the decryption algorithm. Then, proper analysis can be conducted on the data to check whether it can inadvertently expose the secret keys that embedded in the algorithm. The analysis can be mathematical, observational and/or practically invasive. If any leakage of the secret keys happen, the countermeasures to overcome the attack can be introduced by inserting random parameter into the decryption algorithm or transform the operation of the algorithm to make it only releases the uniform pattern of the external data.

In this study also we choose BFHP and DLP as the hard mathematical problems to introduce a new signing scheme. The problems act as the security strength for the scheme. To manipulate the problem into a working algorithm, a study is held on the established cryptosystems that utilize the same hard mathematical problem. The new scheme then should be tested against several ad-hoc attacks and a performance analysis to compare it with the other scheme.

1.8 Contribution of Research

- An analysis in terms of side channel attacks on AA_β cryptosystem will strengthen the security of it with respect to practical implementation.
- A new digital signing scheme that uses BFHP and DLP.

1.9 Scope and Limitation of the Study

The scope to conduct a side-channel attack against AA_β focuses on the timing attack and power attack. We will present the attack model and the assumptions used in the model. Then we will go further into the attack itself and to find the causes of the attack. We discuss the power attack by using figures of power traces to explain the concept of the power analysis before the attack itself is presented. After both attacks has been presented, the countermeasures against them will be shown.

The limitation in the study of the attack is the non-existing fully operational implementation of AA_β in any real-world cryptographic machines. This means all the attacks that are launched are purely theoretical and simulative. That is why the assumptions that have been made prior to the attack are important to visualize the real attack if there exists implementation of AA_β in the future.

Another scope in the study is in designing a new signing scheme. Both hard problems (i.e BFHP and DLP) of the scheme are introduced in the early chapters. After the scheme has been presented, we will forward security and performance analysis of the scheme.

1.10 Overview of the Thesis

In Chapter 2, the mathematical and cryptographic concepts that are used throughout the study will be explained. The relevant details about AA_β which is the target cryptosystem in this thesis will be presented in Chapter 3 before the methodology of the attack will be shown in the next chapter, Chapter 4. Next, the attack itself are divided into two chapters which are Chapter 5 and Chapter 6 for timing attack and power attack respectively. The countermeasures against both attacks are in Chapter 7. After that, the new digital signing scheme is detailed in Chapter 8 before the conclusion of this thesis.

REFERENCES

Anderson, R. and Kuhn, M. (1996). Tamper resistance-a cautionary note. In *Proceedings of the second Usenix workshop on electronic commerce*, volume 2, pages 1–11.

Ariffin, M., Asbullah, M., Abu, N., and Mahad, Z. (2013). A new efficient asymmetric cryptosystem based on the integer factorization problem. *Malaysian Journal of Mathematical Sciences*, 7(S):19–37.

Ariffin, M. and Mahad, Z. (2013). AA_β public-key cryptosystem - a practical comparative analysis against RSA and ECC. *International Journal of Digital Content Technology and its Applications*, 7(7):174–182.

Boneh, D., Durfee, G., and Howgrave-Graham, N. (1999). Factoring $N = p^r q$ for large r. In *Advances in CryptologyCrypto99*, pages 326–337. Springer.

Brent, R. P. and Zimmermann, P. (2011). *Modern computer arithmetic*. Number 18 in 0.5.1. Cambridge University Press.

Brumley, D. and Boneh, D. (2005). Remote timing attacks are practical. *Computer Networks*, 48(5):701–716.

Coppersmith, D., Odlzyko, A. M., and Schroeppel, R. (1986). Discrete logarithms in $GF(p)$. *Algorithmica*, 1(1-4):1–15.

Diffie, W. and Hellman, M. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in Cryptology*, pages 10–18. Springer.

Gandolfi, K., Mourtel, C., and Olivier, F. (2001). Electromagnetic analysis: Concrete results. In *Cryptographic Hardware and Embedded SystemsCHES 2001*, pages 251–261. Springer.

Genkin, D., Shamir, A., and Tromer, E. (2013). RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. *IACR Cryptology ePrint Archive*, 2013:857.

Goldwasser, S., Micali, S., and Rivest, R. L. (1988). A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2):281–308.

Hartmanis, J. and Stearns, R. E. (1965). On the computational complexity of algorithms. *Transactions of the American Mathematical Society*, pages 285–306.

Herrmann, M. and May, A. (2008). Solving linear equations modulo divisors: On factoring given any bits. In *Advances in Cryptology-ASIACRYPT 2008*, pages 406–424. Springer.

Hoffstein, J., Pipher, J., and Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. In *Algorithmic number theory*, pages 267–288. Springer.

Jonsson, J. and Kaliski, B. (2003). Public-key cryptography standards (PKCS)# 1: RSA cryptography specifications version 2.1. https://tools.ietf.org/html/rfc3447. Accessed: 2014-03-07.

Kaliski, B. and Staddon, J. (1998). PKCS # 1: RSA cryptography specifications version 2.0. Technical report, RFC 2437, October.

Karatsuba, A. and Ofman, Y. (1963). Multiplication of multidigit numbers on automata. In *Soviet physics doklady*, volume 7, page 595.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209.

Koç, C. K. (2009). *About Cryptographic Engineering*. Springer.

Kocher, P., Jaffe, J., and Jun, B. (1999). Differential power analysis. In *Advances in CryptologyCRYPTO99*, pages 388–397. Springer.

Kocher, P., Jaffe, J., Jun, B., and Rohatgi, P. (2011). Introduction to differential power analysis. *Journal of Cryptographic Engineering*, 1(1):5–27.

Kocher, P. C. (1996). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Advances in CryptologyCRYPTO96*, pages 104–113. Springer.

Kravitz, D. W. (1993). Digital signature algorithm. US Patent 5,231,668.

Lenstra, A. K., Lenstra, H. W., and Lovász, L. (1982). Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534.

Lenstra, A. K., Lenstra Jr, H. W., Manasse, M. S., and Pollard, J. M. (1993). *The number field sieve*. Springer.

Martin, K. M. (2012). *Everyday Cryptography: Fundamental Principles and Applications*. Oxford University Press.

Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A. (2010). *Handbook of applied cryptography*. CRC press.

Montgomery, P. L. (1985). Modular multiplication without trial division. *Mathematics of computation*, 44(170):519–521.

OpenSSL Security Advisory (2003). Timing-based attacks on RSA keys. https://www.openssl.org/news/secadv_20030317.txt. Retrieved July 25th, 2014.

Osvik, D. A., Shamir, A., and Tromer, E. (2006). Cache attacks and countermeasures: the case of AES. In *Topics in Cryptology–CT-RSA 2006*, pages 1–20. Springer.

Petric, A. (2011). Side Channel Attack Measurement Setup. http://www.alexander-petric.com/2011/08/side-channel-attack-measurement-setup-2.html. Accessed: 2015-04-14.

Quisquater, J.-J. and Couvreur, C. (1982). Fast decipherment algorithm for RSA public-key cryptosystem. *Electronics letters*, 18(21):905–907.

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.

Rudich, S. and Wigderson, A. (2004). *Computational complexity theory*. American Mathematical Soc.

Schindler, W. (2000). A timing attack against RSA with the chinese remainder theorem. In *Cryptographic Hardware and Embedded SystemsCHES 2000*, pages 109–124. Springer.

Schirokauer, O., Weber, D., and Denny, T. (1996). Discrete logarithms: the effectiveness of the index calculus method. In *Algorithmic number theory*, pages 337–361. Springer.

Schmidt, W. M. (1996). *Diophantine approximation*, volume 785. Springer.

Schnorr, C.-P. (1991). Efficient signature generation by smart cards. *Journal of cryptology*, 4(3):161–174.

Schnorr, C. P. and Jakobsson, M. (2000). Security of signed ElGamal encryption. In *Advances in Cryptology–ASIACRYPT 2000*, pages 73–89. Springer.

Seurin, Y. (2012). On the exact security of schnorr-type signatures in the random oracle model. In *Advances in Cryptology–EUROCRYPT 2012*, pages 554–571. Springer.

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM journal on computing*, 26(5):1484–1509.

Stamp, M. and Low, R. M. (2007). *Applied cryptanalysis: breaking ciphers in the real world*. John Wiley & Sons.

Vacca, J. R. (2012). *Computer and information security handbook*. Newnes.

Witteman, M. and Oostdijk, M. (2008). Secure application programming in the presence of side channel attacks. In *RSA conference*, volume 2008.

Yan, S. Y. (2007). *Cryptanalytic attacks on RSA*. Springer.