UNIVERSITI PUTRA MALAYSIA

CRYPTANALYSIS ON THE MODULUS N = p2q AND DESIGN OF RABIN-LIKE CRYPTOSYSTEM WITHOUT DECRYPTION FAILURE

MUHAMMAD ASYRAF BIN ASBULLAH

IPM 2015 9

CRYPTANALYSIS ON THE MODULUS $N = p^2q$ AND DESIGN OF RABIN-LIKE CRYPTOSYSTEM WITHOUT DECRYPTION FAILURE

By

MUHAMMAD ASYRAF BIN ASBULLAH

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

August 2015

DEDICATIONS

To all of my love;
Mak & Abah
Munirah & Wahbah
Atiqah, Atirah, Adibah

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

CRYPTANALYSIS ON THE MODULUS $N = p^2q$ AND DESIGN OF RABIN-LIKE CRYPTOSYSTEM WITHOUT DECRYPTION FAILURE

By

MUHAMMAD ASYRAF BIN ASBULLAH

August 2015

Chairman:Muhammad Rezal bin Kamel Ariffin, PhD
Faculty: Institute For Mathematical Research

Rabin cryptosystem has fast encryption and proven as secure as the integer factorization problem. Nonetheless, its decryption produces four possible correct results with no indicator for choosing the right one is given. Therefore, this scenario leads to a decryption failure. In order to engage with this problem and to refine the existing works, further analysis subjected to mathematical proof are needed.

This thesis concentrates on an investigation into a new method to overcome all the existing drawbacks of the previous effort to refine the Rabin cryptosystem. One of the ways to achieve this is through the utilization of the modulus $N = p^2q$. The first contribution of this thesis deals with the level of security and the difficulty of factoring the modulus $N = p^2q$. As a consequence, we develop four cryptanalysis methods by which to show that $N = p^2q$ can be factored in polynomial time under certain conditions.

The second part of this thesis focuses on revisiting the Rabin encryption scheme; with the goal to overcome all the previous drawbacks of its predecessor, including it's variants. Existing methods exploit some mathematical object or put paddings and redundancies into the message, whilst the new proposed method opens up a refreshing window of research into the problem. The proposed method, called the Rabin-p cryptosystem has recorded an improvement which bears the idea of a failure-free decryption scenario.

In this thesis, we also develop a new cryptographic hard problem based on a special instance of a linear Diophantine equation in two variables, with some provided restrictions and carefully selected parameters. We reason that the proposed cryptographic hard problem can be used for developing practical cryptographic constructions. In parallel, we review the AA_{β} cryptosystem based on the design of Rabin-p function over integers and also as a demonstration of the proposed cryptographic hard problem concept. We then put forward an enhancement of the AA_{β} decryption for better efficiency.

Additionally, we conduct rigorous mathematical analyses on both cryptosystems introduced in this thesis. Moreover, for the purpose of empirical evidences, some parameters are chosen in the course of the process to validate the efficiency in terms of algorithmic running time and memory consumptions. We then conduct a comparative analysis toward estimating the running time during the encryption and decryption process. We also evaluate the memory cost for system parameters and accumulators. Finally, we study the provable security element for both cryptosystems. Emphasis is given to the standard security goal and the strong attack model, namely the indistinguishability and the chosen-ciphertext attack, respectively.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

ANALISISKRIPTO TERHADAP MODULUS $N = p^2q$ DAN REKABENTUK BERASASKAN SISTEMKRIPTO RABIN TANPA KEGAGALAN PENYAHSULITAN

Oleh

MUHAMMAD ASYRAF BIN ASBULLAH

Ogos 2015

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

Sistemkripto Rabin mempunyai penyulitan cepat dan keselamatannya terbukti setara masalah pemfaktoran integer. Bagaimanapun, penyahsulitannya menghasilkan empat kemungkinan jawapan dengan tiada petunjuk yang mengesahkan jawapan yang sebenar, menjurus kepada kegagalan penyahsulitan. Demi memperhalusi permasalahan ini dan menambahbaik kerja yang terdahulu, maka analisis lanjutan secara pembuktian bermatematik adalah diperlukan.

Tesis ini tertumpu kepada penyelidikan suatu kaedah baharu untuk mengatasi kesemua kelemahan sistemkripto Rabin sedia ada. Antara cara mencapai tujuan tersebut ialah memanfaatkan penggunaan modulus $N = p^2q$. Sumbangan pertama tesis adalah membincangkan tahap keselamatan dan kepayahan memfaktorkan modulus $N = p^2q$. Hasilnya, empat kaedah analisiskripto terbina yang menunjukkan bahawa $N = p^2q$ boleh difaktorkan dalam jangkamasa berpolinomial tertakluk kepada syarat tertentu.

Bahagian kedua tesis ini bertumpukan semakan semula keatas skim penyulitan Rabin; bermatlamat untuk mengatasi segala kelemahan sedia ada, termasuklah variasinya. Kaedah sedia ada melibatkan eksploitasi beberapa objek bermatematik atau meletakkan pemadatan dan lebihan terhadap tulisan biasa, manakala kaedah yang dicadangkan membuka lembaran baharu dalam penyelidikan permasalahan tersebut. Kaedah yang dicadangkan, dipanggil sistemkripto Rabin-p didapati mencatatkan peningkatan, yang mana membawa gagasan bebas kegagalan penyahsulitan.

Dalam tesis ini, kami juga membangunkan masalah payah kriptografi baharu berdasarkan kes tertentu bagi persamaan linear Diophantus dua pembolehubah yang memenuhi syarat dan parameter tertentu. Kami berhujah bahawa masalah kriptografi payah yang dicadangkan boleh digunakan untuk membangunkan sistem kriptografi yang praktikal. Disamping itu, kami melihat semula sistemkripto AA_{β} berdasarkan reka bentuk fungsi Rabin-p ke atas nombor bulat beserta konsep masalah kriptografi payah yang dicadangkan. Kami kemudian mengemukakan penambahbaikan terhadap penyahsulitan AA_{β} untuk kecekapan yang lebih baik.

Selain itu, kami menjalankan analisis bermatematik yang rapi terhadap kedua-dua sistemkripto yang diperkenalkan di dalam tesis ini. Selanjutnya, bagi tujuan bukti empirikal, beberapa parameter dipilih untuk proses pengesahkan kecekapan pecutan masa algoritma dan kepenggunaan memori. Kami kemudiannya menjalankan analisis perbandingan anggaran pecutan masa semasa proses penyulitan dan penyahsulitan. Kami juga menilai kos memori untuk sistem parameter dan penumpukkannya. Akhir sekali, kami mengkaji unsur keselamatan terbuktikan bagi kedua-dua sistemkripto tersebut. Penekanan diberikan kepada matlamat piawai keselamatan dan model serangan yang kuat, masing-masing iaitu ketidakbolehbezakan dan serangan ke atas tulisan rahsia terpilih.

ACKNOWLEDGEMENTS

Dengan nama Allah,
Demi zat yang Maha Hidup, yang Maha Berdiri,
yang mengisi dadaku dengan pertunjuk hidayah,
yang mengeluarkan aku dari susah dan payah,
yang menyediakan jalan keluar disetiap masalah,
yang menghilangkan dari jantung hatiku resah dan gundah,
yang meredakan dari perasaanku letih dan lelah,
jika hendakku kira segala pemberianMu, tidak terkira,
jika hendakku hitung segala kasihanMu, tidak kumampu.

All praise and thanks are to Almighty Allah, the most Gracious, the most Merciful. I would like to thank my supervisor Associate Professor Dr. Muhammad Rezal bin Kamel Ariffin, as an excellent researcher to develop and discuss ideas with, who has been a great source of inspiration and also for his continuous guidance. Forever in debt to your priceless advice. Many thanks go to my co-supervisors; Assoc. Prof. Dr. Azmi bin Jaafar and Assoc. Prof. Dr. Siti Hasana binti Sapar for their constant availability to motivate and gives feedbacks on my thesis writing process. I have also received a lot of input and support from my friends in the Al-Kindi Cryptography Research Laboratory Group namely, Zahari bin Mahad, Amir Hamzah bin Abd Ghafar, Tea Boon Chian, and Muhammad Azlan bin Daud. I thank them very much. My warm gratitude goes to all of INSPEM staffs for the administrative matters, for providing facilities that encourage research and for the friendliness services. Last but never least; to my parents, my wife, my son and my family, there is nothing much to say except, I do love all of you. Thanks.

I certify that a Thesis Examination Committee has met on 28 August 2015 to conduct the final examination of Muhammad Asyraf bin Asbullah on his thesis entitled "Cryptanalysis on the Modulus $N = p^2q$ and Design of Rabin-like Cryptosystem without Decryption Failure" 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 Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

Ibragimov Gafurjan, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Chairperson)

Mohamad Rushdan bin Md Said, 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)

Abderrahmane Nitaj, PhD
Professor
Laboratoire de Mathématiques Nicolas Oresme
Université de Caen Basse Normandie
France
(External Examiner)

ZULKARNAIN ZAINAL, 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 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)

Azmi bin Jaafar, PhD
Assosiate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Siti Hasana binti Sapar, 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: Muhammad Asyraf bin Asbullah, GS30299

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: Azmi bin Jaafar

Signature: _____
Name of
Member of
Supervisory
Committee: Siti Hasana binti Sapar

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BFHP	Bivariate Function Hard Problem
CCA	Chosen Ciphertext Attack
CCA1	Non-adaptive CCA
CCA2	Adaptive CCA
CPA	Chosen Plaintext Attack
CRT	Chinese Remainder Theorem
gcd	Greatest Common Divisor
IFP	Integer Factorization Problem
IND	Indistinguishability
IND-CCA2	Indistinguishable against CCA2
LLL	Lenstra-Lenstra-Lovasz
OAEP	Optimal Asymmetric Encryption Padding
ROM	Random Oracle Model
RSA	Rivest-Shamir-Adleman
SET	Secure Electronic Transaction
spm	Single-precision Multiplication

CHAPTER 1

INTRODUCTION

1.1 Cryptography

Post 1990's, the exponentially growing common medium for transporting information is through electronic means. Currently, the internet assumes this role. The internet; is a worldwide network that is being shared amongst the people all around the globe. The internet contains large amount of entities, indistinguishable from countries or nations, with users of varied interests and intentions, in every aspect imaginable. With just simple clicks, we could send emails or communicate with people, do monetary transactions through electronic commerce, and purchase items online.

Nowadays, our daily activities and conversation are dependent on the internet connectivity. Such internet dependencies led us to consider about the security and privacy of communication that occurs in the cyberspace, since it may easily be compromised by the authorities, hackers, or terrorists, of which some consider them as the adversary of the system. Hence, it is necessary and important for establishing a system or environment that guarantee the security of the internet users from any type of adversary.

Out of the wilderness and all the sophistication that we experience within the online world, the field of cryptography turns into a handy tool when security begins to matters. Cryptography provides a mean to ensure that our privacy and confidential information is secured, hence provides confidence for sharing and exchanging such information between other parties (the sender and the intended receiver). It is of a great interest, to be able to analyze the strengths and weaknesses of encryption and decryption processes.

In classical terminology, encryption is defined as a conversion procedure of an information; which changes its readable state into another type of information, yet appearing to be nonsense. When we enter the age of the computer, the technologies evolves at a rapid state, therefore the definition of encryption is also amended. In modern terminology, we may say that encryption is a process of converting an ordinary information (i.e. known as a plaintext) into an unintelligible form (i.e. called as a ciphertext). On the opposite, the decryption is the reverse process of encryption, which functions to recover the intended or actual plaintext from its corresponding ciphertext.

Apparently, both of the encryptor (sender) and the decryptor (receiver) must have '*the key*' in order to successfully performs their operation, respectively. The encryptor uses the key to scramble a plaintext (an ordinary information such as a readable message or any meaningful data) and turns it into a ciphertext. This very same key is also being used by decryptor in order to recover back the original plaintext from its

ciphertext. Consequently, no matter how obscure the algorithm for encryption and decryption is, it could be problematic if the key is not safe in the first place. This is the basic concept that is well known as the Kerckhoffs' principle, that states that the security level of an encrypted information is as strong as the security of its key.

Definition 1.1 (Kerckhoffs' Principle) *(Katz and Lindell, 2008). Security of any cryptosystem should depend only on the secrecy of its key, and not the secrecy of the cryptosystem algorithm itself.*

The reason behind this is because it is much easier to maintain secrecy of a key instead of an algorithm. If the key is exposed then it is easier to change the key instead of replacing the algorithm being used. Accordingly, it is good practice to replace a new key after a certain period. Furthermore, it is much more practical to share the same algorithm publicly between the communicating parties.

As suggested by Kerckhoffs's principle, the details of any cryptographic algorithm need to be public knowledge, which is the contrast to the concept of the 'security by obscurity', except the secrecy for key (Katz and Lindell, 2008). In modern cryptography philosophy, it is natural to assume that the adversary knows everything about the algorithm. Therefore, the only information that needs to be kept secret is the key.

1.2 Asymmetric Encryption

In the classical system, the secret key is supposedly being shared between the sender and the receiver in a symmetrical manner. In order to maintain the secrecy, the key must be shared or distributed securely to both parties. However, the process of exchanging secret keys is problematic when the number of users get larger since more keys are needed to be delivered to various parties. To tackle this problem, Diffie and Hellman (1976) has came up with the notion of *asymmetric encryption*.

Definition 1.2 (Asymmetric Encryption) *(Diffie and Hellman, 1976). Let $\mathscr{M}$ denote the message space, $\mathscr{C}$ denote the ciphertext space, $\mathscr{K}$ denote the key space, m denote the plaintext and c denote the ciphertext. Asymmetric encryption scheme is defined as follows.*

1. *Key generation algorithm K is a probabilistic algorithm that will generate a public key denoted as $e \in \mathscr{K}$ and private key as $d \in \mathscr{K}$ respectively.*
2. *Encryption algorithm E is a probabilistic algorithm that takes a message $m \in \mathscr{M}$ and the public key e, to produce a ciphertext $c \in \mathscr{C}$ as a function of $c = E_e(m)$.*
3. *Decryption algorithm D is a deterministic algorithm which is given the ciphertext c and the private key d, will output m. That is $m = D_d(c)$.*

Basically, a cryptosystem that uses the same secret keys and shared by both; sender and receiver, then it is called as symmetric cryptosystem. If a cryptosystem involves

a private key and public key, then the cryptosystem is known as an asymmetric cryptosystem or commonly referred to as public key cryptosystem.

Definition 1.3 (Proof of Correctness) *(Diffie and Hellman, 1976). For each pairs of key* $(e,d) \in \mathscr{K}$ *output by the algorithm K, and for every message* $m \in \mathscr{M}$ *and ciphertext* $c \in \mathscr{C}$ *then*

$$D_d(c) = D_d(E_e(m)) = m.$$

The *proof of correctness*, as defined by Definition 1.3, suggest that the decryption is the reversal operation of encryption and should be proved to be correct to return back the plaintext from its ciphertext.

Definition 1.4 (One-way Function) *(Menezes et al., 1997). A one-way function is a function that is easily applied in one direction, but very hard to calculate the inverse.*

Let $f : X \longrightarrow Y$ *be an invertible function. For* $x \in X$ *and* $y \in Y$*, then*

1. *it is easy to compute the value of* $y = f(x)$*,*
2. *it is hard to compute the value of* $x = f^{-1}(y)$*.*

Definition 1.5 (Trapdoor One-way Function) *(Menezes et al., 1997). A trapdoor one-way function is a piece of information that allows the inverse for the one-way function to be easily computed (i.e. it is easy to compute the value of* $x = f^{-1}(y)$ *by using trapdoor information).*

The trapdoor information is a piece of auxiliary information that allows the inverse to be easily computed (Hoffstein et al., 2008). For instance, the private key is said to be the trapdoor information to the encryption function. Without the correct private key, one will not be able to do decryption. On the contrary, decryption is an easy task with correct private key.

The design of the encryption and decryption function in public key setting can be realized using the concept of a one-way function and trapdoor one-way function, respectively (Diffie and Hellman, 1976). It is a surprise to learn that despite years of research, it is still not known whether one-way functions exist (Katz and Lindell, 2008). Since we cannot prove the existence of the one-way function, we always can show that a problem is indeed hard corresponding to the concept of the one-way function.

Definition 1.6 (Cryptographic Hard Problem) *(Menezes et al., 1997). A cryptographic hard problem is defined as a concrete mathematical object which is easy to compute in one direction, but very hard to invert.*

Basically, a cryptographic hard problem is widely believed to be hard. Cryptographically speaking, the word *hard* from Definition 1.6 is referring to the difficulty level for solving a certain mathematical problem, including with the help from the state of the art technology. The terminology of cryptographic hard problem provides confidence to the designing process of a cryptosystem, which the security measured is dependent on how difficult its related hard problem could be. If the correct steps are taken and the appropriate parameters are chosen, then to solve hard problems might be infeasible, even via brute force. This is the main ingredient for designing and constructing a public key cryptosystem.

Remark that from the Definition 1.6, it does not necessarily mean that no one has figured out on *how to do the inversion*, but it is rather shown that there exist no efficient algorithm that runs in a reasonable time (i.e. in polynomial time) that can do such operation (Katz and Lindell, 2008). Thus, if the efforts to solve a stated mathematical problem exceeds a certain amount of time (i.e. in exponential time) then we say that such mathematical problem is considered to be intractable, even using the most powerful tools available. On the other hand, suppose the stated mathematical problem can be solved below or within the range of a certain polynomial time, then the cryptosystem that relies upon such problems are considered insecure (Galbraith, 2012).

Definition 1.7 (Prime and Composite) *(Hoffstein et al., 2008). An integer $p \geq 2$ is called a prime if the only positive integers dividing such number are 1 and p itself. If an integer $N > 1$ and not a prime, then we say that such number is composite. The integer 1 is neither prime nor composite. The first few primes are 2, 3, 5, 7, 11, 13,...*

Theorem 1.1 (Fundamental Theorem of Arithmetic) *(Kumanduri and Romero, 1998). Let $N \geq 2$ be an integer. Then N can be factored as a product of prime numbers*

$$N = p_1^{r_1} p_2^{r_2} p_3^{r_3} \dots p_s^{r_s}$$

where p_i are distinct primes and integers $r_i \geq 1$ for $i = 1, 2, \cdots, s$. Moreover,this expression is unique, regardless of its ordering.

Example 1.1 $N = 168 = 2^3 \cdot 3 \cdot 7$

To date, one of the most celebrated problem in mathematics, particularly in number theory is known as the integer factorization problem and exhibits properties of a cryptographic hard problem. It is assumed to be very difficult to solve and is supported by decades of evidence for its hardness. In addition, it is widely believed that the integer factorization problem is a suitable candidate for a one-way function.

Definition 1.8 (Integer Factorization Problem) *(Hoffstein et al., 2008). Let N be a positive integer. Then, the integer factorization problem (IFP) is defined as the problem to find the prime factorization of N such that,* $N = p_1^{r_1} p_2^{r_2} p_3^{r_3} \dots p_s^{r_s}$ *where* p_i *are distinct primes and* $r_i \geq 1$. *For most cases in cryptography, the problem is to find the prime factors p and q from* $N = pq$.

1.3 RSA Cryptosystem

Prior to 1970's, encryption and decryption was done symmetrically. This was the practice until the advent of public key cryptosystem that was introduced by Diffie and Hellman (1976). Yet, at that time the notion of asymmetric cryptosystem is somehow not well realized by many people. In 1978, the RSA cryptosystem that was introduced by Rivest, Shamir and Adlemen went public and it is regarded now by the cryptographic community as the first practical realization of the public key cryptosystem. The security of the RSA cryptosystem is based on the intractability to solve the modular e^{th} root problem coupled with the integer factorization problem (IFP) of the form $N = pq$ and the difficulty to solve key equation $ed + \phi(N)t = 1$ where $\phi(N) = (p-1)(q-1)$ and d the inverse of e modulo $\phi(N)$.

Definition 1.9 (Modular e^{th} Root Problem) *(Menezes et al., 1997). Let* $N = pq$ *and odd integer* $e \geq 3$. *Then the modular* e^{th} *root problem is defined as to find the integer m from c such that* $c \equiv m^e \pmod{N}$.

Definition 1.10 (Euler's ϕ Function) *(Menezes et al., 1997). Let a complete residue system modulo N is a set of elements* $\{0, 1, \cdots, N-1\}$. *The number of invertible elements in a complete residue system modulo N is denoted as* $\phi(N)$ *and is called Euler's* ϕ *Function.*

Theorem 1.2 *(Menezes et al., 1997). If* $N = p_1^{r_1} p_2^{r_2} p_3^{r_3} \dots p_s^{r_s}$ *is the prime factorization of N, then*

$$\phi(N) = \prod_{i=1}^{s} p_i^{r_i - 1} (p_i - 1)$$

Corollary 1.1 *(Menezes et al., 1997). If* $N = pq$, *then*

$$\phi(N) = (p-1)(q-1)$$

The RSA cryptosystem is defined as follows.

Algorithm 1.1 RSA Key Generation Algorithm

Input: The size k of the security parameter
Output: The public key (N,e) and the private key (N,d)
1: Choose two random and distinct primes p and q such that $2^k < p,q < 2^{k+1}$
2: Compute $N = pq$ and $\phi(N) = (p-1)(q-1)$
3: Choose e such that $3 \leq e < \phi(N)$ and $\gcd(e,\phi(N)) = 1$
4: Compute d such that $ed \equiv 1 \pmod{\phi(N)}$
5: Return the public key (N,e) and the private key (N,d)

Algorithm 1.2 RSA Encryption Algorithm

Input: The plaintext m and the public key (N,e)
Output: A ciphertext c
1: Choose integer $0 < m < N$ such that $\gcd(m,N) = 1$
2: Compute $c \equiv m^e \pmod{N}$.
3: Return the ciphertext c

Algorithm 1.3 RSA Decryption Algorithm

Input: A ciphertext c and the private key (N,d)
Output: The plaintext m
1: Compute $m \equiv c^d \pmod{N}$
2: Return the plaintext m

1.3.1 Proof of Correctness for RSA Decryption

Proposition 1.1 *(Rivest et al., 1978). Let $N = pq$ and $\phi(N) = (p-1)(q-1)$. For every integer m such that $\gcd(m,N) = 1$, then $m^{\phi(N)} \equiv 1 \pmod{N}$.*

Proposition 1.2 *(Rivest et al., 1978). Let (N,e) and (N,d) be the public and private key for the RSA cryptosystem, respectively. Suppose $0 < m < N$ such that $\gcd(m,N) = 1$ and $c \equiv m^e \pmod{N}$. Then $m \equiv c^d \pmod{N}$.*

Proof:
Let $N = pq$,$\phi(N) = (p-1)(q-1)$ and $ed \equiv 1 \pmod{\phi(N)}$ be the RSA parameters. Thus there exist an integer t such that $ed = 1 + t\phi(N)$. Hence we have

$$\begin{aligned} c^d &\equiv (m^e)^d \\ &\equiv m^{ed} \\ &\equiv m^{1+t\phi(N)} \\ &\equiv m \cdot m^{t\phi(N)} \pmod{N} \end{aligned}$$

From the Proposition 1.1 it follows that $m \cdot m^{t\phi(N)} \equiv m \pmod{N}$. Since $m < N$, then we have $c^d \equiv m \pmod{N}$. ■

1.4 Rabin Cryptosystem

One year after the invention of the RSA cryptosystem, Rabin (1979) introduced another cryptosystem based on the intractability to solve the square root modulo problem of a composite integer. In fact, this cryptosystem is the first public key cryptosystem of its kind that was proved equivalent to factoring $N = pq$.

Definition 1.11 (Modular Square Root Problem) *(Menezes et al., 1997). The modulo square root problem is defined as to find the integer m from c such that* $c \equiv m^2 \pmod{N}$*, where* $N = pq$.

The Rabin cryptosystem is defined as follows.

Algorithm 1.4 Rabin Key Generation Algorithm

Input: The size k of the security parameter
Output: The public key N and the private key (p,q)

1: Choose two random and distinct primes p and q such that $2^k < p,q < 2^{k+1}$ satisfy $p,q \equiv 3 \pmod{4}$
2: Compute $N = pq$
3: Compute two integers r,s such that $rp + sq = 1$
4: Return the public key N and the private key (p,q)

Algorithm 1.5 Rabin Encryption Algorithm

Input: The plaintext m and the public key N
Output: A ciphertext c

1: Choose integer $0 < m < N$ such that $\gcd(m,N) = 1$
2: Compute $c \equiv m^2 \pmod{N}$.
3: Return the ciphertext c.

At the first glance, we might consider the Rabin cryptosystem as an RSA variant with the use of the public exponent $e = 2$ apart from the RSA with public exponent $e \geq 3$. Interestingly, this claim is not necessarily true since by definition, the value of public key e for the RSA requires $\gcd(e, \phi(N)) = 1$ where $\phi(N) = (p-1)(q-1)$, yet in the case of Rabin cryptosystem is $\gcd(e = 2, \phi(N)) \neq 1$. In addition, the role of the public exponent $e = 2$ of the Rabin encryption gives a computational advantage over the RSA (Williams, 1980).

Algorithm 1.6 Rabin Decryption Algorithm

Input: A ciphertext c and the private key (p,q)
Output: The plaintext m

1: Compute $m_p \equiv c^{\frac{p+1}{4}} \pmod{p}$
2: Compute $m_q \equiv c^{\frac{q+1}{4}} \pmod{q}$
3: Compute $m_1 \equiv rpm_q + sqm_p \pmod{N}$
4: Compute $m_2 \equiv rpm_q - sqm_p \pmod{N}$
5: Compute $m_3 \equiv -m_2 \pmod{N}$
6: Compute $m_4 \equiv -m_1 \pmod{N}$
7: Return the correct plaintext m amongst the four possible candidates

1.4.1 Proof of Correctness for Rabin Decryption

Definition 1.12 (Quadratic Residue) *(Menezes et al., 1997). Let p be an odd prime number. An element $c \in \mathbb{Z}_p$ is said to be a quadratic residue modulo p (i.e. has square roots modulo p) if and only if there exists some $m \in \mathbb{Z}_p$ such that $c \equiv m^2 \pmod{p}$. Otherwise, c is said to be a quadratic nonresidue modulo p.*

Theorem 1.3 (Euler's Criterion) *(Kumanduri and Romero, 1998). If p be an odd prime number and c is an integer coprime to p, then c is a quadratic residue modulo p if and only if $c^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*

Theorem 1.4 (Chinese Remainder Theorem) *(Hoffstein et al., 2008). Suppose that $n_1, n_2, \ldots, n_r$ are pairwise relatively prime positive integers, and let $a_1, a_2, \ldots, a_r$ be integers. Then the systems of congruences, $x \equiv a_i \pmod{n_i}$ for $1 \leq i \leq r$ has a unique solution modulo $N = n_1 n_2 \ldots n_r$, which is given by*

$$x \equiv \sum_{i=1}^{r} a_i N_i y_i \pmod{N}$$

where $N_i = \frac{N}{n_i}$ and $y_i \equiv N_i^{-1} \pmod{n_i}$ for $1 \leq i \leq r$.

Corollary 1.2 *(Hoffstein et al., 2008). Suppose we have a system of congruences $x \equiv a_i \pmod{n_i}$ for $i = 1, 2$, then the solution x to such simultaneous congruences can be written as*

$$x \equiv a_1 N_1 y_1 + a_2 N_2 y_2 \pmod{N}$$

where $N = n_1 n_2$ and y_1, y_2 such that $N_1 y_1 + N_2 y_2 = 1$.

Proposition 1.3 *(Rabin, 1979). Let $N = pq$ with $p, q \equiv 3 \pmod{4}$ be the public and private key for the Rabin cryptosystem, respectively. Suppose $0 < m < N$ such*

that $\gcd(m,N) = 1$ *and* $c \equiv m^2 \pmod{N}$. *Then* m_i *for* $i = 1,2,3,4$ *are the solutions generated from Rabin's decryption procedure.*

Proof:
Firstly, we compute $m_p = c^{\frac{p+1}{4}} \pmod{p}$ and $m_q = c^{\frac{q+1}{4}} \pmod{q}$. By Theorem 1.3, c is a square root modulo p if and only if $c^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ and is a square root modulo q if and only if $c^{\frac{q-1}{2}} \equiv 1 \pmod{q}$. Hence

$$\begin{aligned} \pm m_p^2 &\equiv \left(\pm c^{\frac{p+1}{4}}\right)^2 \\ &\equiv c^{\frac{p+1}{2}} \\ &\equiv c \cdot c^{\frac{p-1}{2}} \\ &\equiv c \pmod{p}. \end{aligned}$$

Thus, $\pm m_p$ are the two square roots of $c \pmod{p}$, and in analogous manner, $\pm m_q$ are the two square roots of $c \pmod{q}$. Then using integers r,s such that $rp + sq = 1$, we combine the congruence $\pm m_p$ and $\pm m_q$ using Corollary 1.2 as follows.

$$\begin{aligned} m_1 &\equiv rpm_q + sqm_p \pmod{N} \\ m_2 &\equiv rpm_q - sqm_p \pmod{N} \\ m_3 &\equiv -rpm_q + sqm_p \pmod{N} \equiv -m_2 \pmod{N} \\ m_4 &\equiv -rpm_q - sqm_p \pmod{N} \equiv -m_1 \pmod{N} \end{aligned}$$

Finally, if return the value m_i for $i = 1,2,3,4$. Remark that, currently at the moment, there are no convincing method on how to choose the correct plaintext m amongst the four possible candidates without any probabilistic error. ■

1.5 Comparison of RSA and Rabin Cryptosystem

The efficiency of the Rabin cryptosystem is at least as good as the RSA. For Rabin cryptosystem, the encryption is computed by performing a single squaring modulo N. This is far more efficient by comparison to the RSA encryption, which requires the calculation of at least a cubic modulo N (Menezes et al., 1997).

Based on some recent results, the public exponent for RSA must be sufficiently large. Values such as $e = 3$ (the smallest possible encryption exponent for RSA) and $e = 17$ can no longer be recommended, but commonly used values such as $e = 2^{16} + 1 = 65537$ still serve to be fine, thus Rabin has some advantage regarding to this matter (Lenstra and Verheul, 2001).

On the other hand, the Rabin decryption algorithm breaks up into two parts. The first

part is the calculation of two modular exponentiations, and the latter part is about the computation using Chinese Remainder Theorem (CRT). Hence, the efficiency of the Rabin decryption is comparable to the decryption of RSA.

The Rabin encryption function is in the form $c \equiv m^2 \pmod{N}$, where $N = pq$ such that p, q are primes congruence $3 \pmod 4$. This modular square roots problem is considered to be as hard as the IFP. In other words, it is mathematically proven that a random plaintext can be recovered completely from the ciphertext, if and only if the adversary is able to efficiently factoring the public key $N = pq$. See Lemma 1.2.

On the contrary, the RSA encryption in the form $c = m^e \pmod{N}$ might be easier than factoring problem. This is the case because the equivalent of RSA encryption function vis-a-vis factoring is not yet proven (Boneh, 1999). Therefore, the process of finding the e^{th} root is might be possible without initially the need to factor $N = pq$. The security of the RSA encryption scheme is merely based on the strong assumption that the modular e^{th} root problem is a one-way function. Up to this very moment, the publicly known methods to find the e^{th} root is only with a machine that is capable to efficiently factor the RSA modulus $N = pq$.

Definition 1.13 (Computational Reduction) *(Galbraith, 2012). Let $\mathscr{A}$ and $\mathscr{B}$ be two different cryptographic hard problems. We say that a problem $\mathscr{A}$ is reducible to a problem $\mathscr{B}$ if by any mean we able to show that for an algorithm that solves problem $\mathscr{B}$ then such algorithm also solves the problem $\mathscr{A}$.*

Definition 1.14 (Computational Equivalent) *(Galbraith, 2012). Let $\mathscr{A}$ and $\mathscr{B}$ be two different cryptographic hard problems. A problem $\mathscr{A}$ is said to be equivalent to problem $\mathscr{B}$ if and only if the problem $\mathscr{A}$ is reducible to problem $\mathscr{B}$ and vice-versa.*

For instance, suppose we have the integer factorization problem (IFP), the modular e^{th} root problem (also known as RSA-problem) and the modular square root problem. Thus, we have the following lemmas.

Lemma 1.1 *(Galbraith, 2012). The modular e^{th} root problem is reducible to factoring the modulus $N = pq$.*

Lemma 1.1 simply says that suppose we are given a randomly generated RSA parameters. Assume there exists an efficient algorithm with the ability to factor $N = pq$. Hence the modular e^{th} root problem is solved as easily as the RSA decryption procedure itself since we already obtain the secret primes p and q.

The converse of the above statement is still left unproven to be true (Boneh, 1999). Thus the question such that *is factoring the modulus $N = pq$ reducible to solving the modular e^{th} root problem* remains open unanswered until today. As a consequence, we cannot simply say that the modular e^{th} root problem is equivalent to factoring the modulus $N = pq$.

Lemma 1.2 *(Galbraith, 2012). The modular square root problem is equivalent to factoring the modulus $N = pq$.*

This lemma is similar to saying that the modular square root problem is reducible to factoring the modulus $N = pq$ and the converse of such assertion is also true. Suppose we are given a modular square root problem with a modulus of $N = pq$. The first statement means that if there exists an algorithm that is capable of factoring $N = pq$ then such algorithm also can be used to solve the given modular square root problem.

Conversely, suppose there exists an algorithm that is capable to solve a modular square root problem (i.e. successfully obtains all the four distinct roots). Hence, if we add any two such roots, out of four, then we have at least an integer such that is a multiple of either p or q. Proceed by computing the greatest common divisor of that integer with the modulus $N = pq$ will output one of its prime factors. The significant of Lemma 1.2 leads to the following theorem.

Theorem 1.5 *(Galbraith, 2012). Breaking the Rabin cryptosystem is equivalent to factoring the modulus $N = pq$.*

From Theorem 1.5, on one side it shows that the Rabin cryptosystem gives confidence for its security, of which breaking the Rabin cryptosystem is as difficult as factoring. On the other side, this equivalence relationship makes the Rabin cryptosystem vulnerable to a realistic attack, namely chosen ciphertext attack (Koblitz and Menezes, 2007). In addition, any cryptosystem that has the property of its security is equivalent to factoring are only of theoretical significance yet not very practicable as of its vulnerability in real attack situation (i.e. chosen ciphertext attack) (Müller and Müller, 1998). The Rabin cryptosystem was prevented for practical use, simply because of these shortcomings.

1.6 Problem Statement

The Rabin encryption scheme is one of an existing workable asymmetric cryptosystem that comes with nice cryptographic properties. For instance, it has low-cost encryption of which the Rabin encryption is relatively fast to encrypt compared to the widely commercialized RSA cryptosystem, and it has been proven to be as difficult as the integer factorization problem. On the other hand, the decryption of Rabin's scheme produces four possible answers, which only one is correct. This four-to-one decryption setting of the Rabin decryption could lead to a decryption failure scenario since no indicator for selecting the correct plaintext is given.

Theoretically speaking, it is such a waste to abandon a cryptosystem that possesses nice features such as the Rabin cryptosystem. Hence attempts were made by numerous researchers (see Section 2.4 of this thesis) with the objective to turn the Rabin cryptosystem to be as practical and implementable as the RSA cryptosystem.

Broadly speaking, all the previous attempts made seem to employ one or more additional features in order to obtain a unique decryption result, but at the same time may have a small probability for decryption failure. One of the ways to accomplish this is through manipulation of some mathematical objects such as the role of the Jacobi symbol or the Dedekind's sums theorem. Also, it can be done by designing an encryption function with a special message structure. Yet, at the same time all the designs lose the computational advantage of the original Rabin's encryption over the RSA cryptosystem.

In order to engage this problem and to overcome all the shortcomings, further theoretical analysis and mathematical proves are needed to refine that existing work.

1.7 Research Objectives and Methodology

In this section, we put forward the research objectives and explanations of the method used towards achieving the stated objectives as follows.

1. *To cryptanalysis the modulus $N = p^2q$.*

   Objective: The modulus of the form $N = p^2q$ is frequently used in cryptography, especially for designing asymmetric cryptosystems. We aim to refine the Rabin cryptosystem and its variations utilizing the modulus $N = p^2q$. On the other hand, several methods have been produced to cryptanalysis the modulus $N = p^2q$. Hence, it is indeed very important to consider the degree of security of such modulus.

   Methodology: In this study, the method to find a good approximation to $\phi(N)$ and the manipulation of generalized key equations was explored to review the difficulty level for factoring the modulus $N = p^2q$. Note that the theory of continued fractions is one of the primary methods employed in the field of mathematical cryptanalysis (Nitaj, 2013). We determined that the best method to take up for this investigation is the Legendre's theorem of the continued fraction.

2. *To refine the Rabin cryptosystem and its existing variants.*

   Objective: This work can be considered as another look at the design of the Rabin cryptosystem, from a different perspective. Our target is to refine the Rabin encryption scheme in order to overcome all the previous drawbacks of its original design and also its variants. We revisit the Rabin cryptosystem and then aspire to furnish a new design aiming for efficient, secure and practical Rabin-like cryptosystem.

   Methodology: In an attempt to refine the original Rabin cryptosystem and its variants, numerous published studies is identified. We then critically reviews all the related previous works to outline all the advantages and drawbacks. In our design, we use the modulus $N = p^2q$ and we restrict the plaintext to be less than p^2. Hence, to decrypt correctly, it suffices to apply an efficient algo-

rithm that solves the square root of quadratic congruence modulo p^2 instead of modulo $N = p^2q$.

3. *To reproduce a new cryptographic hard problem.*

   Objective: Motivated by the work of Herrmann and May (2008), we focus on the study of a particular case of a linear Diophantine equation in only two variables, which discusses the inability to retrieve variables from a given linear Diophantine equation.

   Methodology: An observation made on the work by Herrmann and May (2008) gave rise an intuition for a potentially new cryptographic hard problem that uses a simple mathematical structure. The methodology is to study and analyze deeper on linear Diophantine equations in two variables of a particular setting.

4. *To design a more efficient implementation of the AA_β cryptosystem.*

   Objective: The AA_β cryptosystem that was proposed by Ariffin (2012) is redesigned according to the newly refine Rabin-like cryptosystem (i.e. the result from the second objective) combines with the mathematical structure of the newly proposed hard problem (i.e. the result from the third objective).

   Methodology: We would start out to achieve our intention by observing the relationship between the Rabin encryption function over the integers and the security notion of the newly proposed cryptographic hard problem. We then propose to design a more efficient implementation of the AA_β cryptosystem as mentioned in Ariffin (2012), that manifests such relationship integrated with the new cryptographic hard problem concept, with a few modifications made on the public and private key size.

5. *To give a comparative analysis on the designated Rabin-like cryptosystems.*

   Objective: We would carry out a comparative analysis toward estimating the running time during encryption and decryption processes upon several Rabin-like cryptosystems. We then provide analysis by evaluating the memory cost for system parameters and accumulators during each operation, respectively.

   Methodology: For comparative analysis, besides the designated Rabin-like cryptosystems, we also included other Rabin-like cryptosystems such that utilize the modulus type of $N = p^2q$, does not use the Jacobi symbol, and does not apply any padding method. For comparative purpose, we adopt the methodology presented in Menezes et al. (1997) to estimate the algorithm running times for each cryptosystem in consideration and the methodology presented in Vuillaume (2003) to evaluate their memory cost for system parameters and accumulators, respectively.

6. *To provides elements of provable security.*

   Objective: We would present provable security elements for the designated Rabin-like cryptosystems. The emphasis is given to the standard security goal and the strongest attack model, namely the indistinguishability and the chosen-ciphertext attack, respectively.

Methodology: In this work, we applied the random oracle model to achieve the provable security elements of the designated Rabin-like cryptosystems. For careful analysis, the proof methodology introduced by Cramer and Shoup (2003) and Katz and Lindell (2008) was applied, which is viewed as such a game played between a cryptosystem and an adversary that try to break such cryptosystem.

1.8 Thesis Outline

This thesis is organized as follows.

In Chapter 1, we present an introduction that guide readers to the motivation of this research. We then encapsulate all the introductory materials into the problem statement. We also highlight the objectives of this research.

Chapter 2 provides mathematical backgrounds such as the linear Diophantine equation, Garner's algorithm, continued fractions, and basic description of the lattice and the LLL algorithm. Later on, we review some materials related to the cryptanalysis method for factoring that will be used throughout this thesis. In addition, we provide a survey of Rabin variants.

The work presented in this thesis focuses on using the modulus $N = p^2q$ as a method to refine the Rabin cryptosystem, which will be used in almost all new discoveries in this thesis. In Chapter 3, we investigate the level of security and the difficulty of factoring the modulus $N = p^2q$.

In Chapter 4, we provide a list of drawbacks of previous strategies that need to be avoided for practically implementing the Rabin encryption scheme. In this chapter, we also prove some useful lemmas and then highlight the methodology of the research performed. Afterwards, we present our Rabin-like cryptosystem, namely the Rabin-p cryptosystem. This is followed by rigorous analysis and discussion on the security related to the proposed scheme.

Chapter 5 reproduces a new cryptographic hard problem based on a special instance of a linear Diophantine equation in two variables as mentioned in Ariffin (2012), namely the Bivariate Function Hard Problem. Provided with carefully selected parameters that satisfying the given conditions, we show that the newly introduced cryptographic hard problem is suitable for developing practical cryptographic constructions.

Chapter 6 discusses the relations between the encryption function of the Rabin-p cryptosystem over the integer, coupled with the security notion of the Bivariate Function Hard Problem. Henceforth, we put forward a new and more efficient design of a public key encryption scheme addressed as the AA_β cryptosystem as mentioned in Ariffin (2012). Rigorous mathematical analyses of the design of AA_β cryptosystem are provided in this chapter. Eventually, three other variants of the AA_β cryptosystem will be presented.

In Chapter 7, we conduct a comparative study of the proposed Rabin-like cryptosystems and the other Rabin variants that uses a modulus of type $N = p^2q$ and without using the Jacobi symbol and any padding method in their strategy. In this chapter, we look into the running time estimation for each scheme using the single-precision multiplication measurement. We then evaluate the memory cost for system parameters and accumulators of the encryption and the decryption process for every respective Rabin-like cryptosystems that are chosen in our comparative study.

In Chapter 8, we design two efficient and provably secure cryptosystems. The first design is a hybrid cryptosystem; combining the Rabin-p cryptosystem with an appropriate symmetric encryption scheme. This proposed hybrid construction is proven to be resilient to the stronger attack, namely the chosen ciphertext attack. In the second design, we set a randomized setting to the AA_β cryptosystem from its deterministic form that is preceded earlier in Chapter 6. This randomized AA_β cryptosystem is also shown to be secure against chosen ciphertext attack. Both provably secure cryptosystem in this chapter is projected in the random oracle model.

Finally, we conclusively summarize all the contributions made out in this thesis in Chapter 9, along with some potential future works.

REFERENCES

Abe, M., Gennaro, R., and Kurosawa, K. (2008). Tag-KEM/DEM: A New Framework for Hybrid Encryption. *Journal Of Cryptology*, 21(1):97–130.

Ariffin, M. R. K. (2012). A Proposed IND-CCA2 Scheme for Implementation on an Asymmetric Cryptosystem Based on the Diophantine Equation Hard Problem. In *The* 3^{rd} *International Conference on Cryptology and Computer Security*, pages 193–197.

Bellare, M. and Rogaway, P. (1995). Optimal Asymmetric Encryption. In *Advances In Cryptology - EUROCRYPT'94*, pages 92–111. Springer.

Boneh, D. (1999). Twenty Years of Attacks on the RSA Cryptosystem. *Notices of the AMS*, 46(2):203–213.

Boneh, D. (2001). Simplified OAEP For The RSA And Rabin Functions. In *Advances In Cryptology-Crypto 2001*, pages 275–291. Springer.

Brumley, D. and Boneh, D. (2005). Remote Timing Attacks Are Practical. *Computer Networks*, 48(5):701–716.

Castagnos, G., Joux, A., Laguillaumie, F., and Nguyen, P. Q. (2009). Factoring pq^2 With Quadratic Forms: Nice Cryptanalyses. In *Advances In Cryptology - ASIACRYPT 2009*, pages 469–486. Springer.

Cesáro, E. (1881). Question proposeé 75. *Mathesis*, 1(184).

Coppersmith, D. (1997). Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. *Journal Of Cryptology*, 10(4):233–260.

Coron, J.-S., Patarin, J., and Seurin, Y. (2008). The Random Oracle Model and the Ideal Cipher Model are Equivalent. In *Advances In Cryptology–Crypto 2008*, pages 1–20. Springer.

Cramer, R. and Shoup, V. (2003). Design and Analysis of Practical Public-Key Encryption Schemes Secure Against Adaptive Chosen Ciphertext Attack. *SIAM Journal On Computing*, 33(1):167–226.

CRYPTREC (2002). Evaluation Report of HIME(R). *http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1019_hime.pdf*.

De Weger, B. (2002). Cryptanalysis of RSA with Small Prime Difference. *Applicable Algebra in Engineering, Communication and Computing*, 13(1):17–28.

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

Dolev, D., Dwork, C., and Naor, M. (1998). Non-Malleable Cryptography. In *SIAM Journal On Computing*.

Elia, M., Piva, M., and Schipani, D. (2015). The Rabin Cryptosystem Revisited. *Applicable Algebra in Engineering, Communication and Computing*, 26(3):251–275.

Freeman, D. M., Goldreich, O., Kiltz, E., Rosen, A., and Segev, G. (2013). More Constructions of Lossy and Correlation-Secure Trapdoor Functions. *Journal Of Cryptology*, 26(1):39–74.

Galbraith, S. D. (2012). *Mathematics Of Public Key Cryptography*. Cambridge University Press.

Galindo, D., Martỳn, S., Morillo, P., and Villar, J. L. (2002). A Practical Public Key Cryptosystem from Paillier and Rabin Schemes. In *Public Key Cryptography - PKC 2003*, pages 279–291. Springer.

Goldwasser, S. and Micali, S. (1984). Probabilistic Encryption. *Journal Of Computer And System Sciences*, 28(2):270–299.

Hardy, G. and Wright, E. (1965). *An Introduction to the Theory of Numbers*. Oxford University Press, London.

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.

Hitachi (2002). HIME(R) Public-Key Cryptosystem. *http://www.hitachi.com/rd/yrl/crypto/hime/*.

Hoffstein, J., Pipher, J., and Silverman, J. H. (2008). *An Introduction To Mathematical Cryptography*. Springer.

Katz, J. and Lindell, Y. (2008). *Introduction To Modern Cryptography: Principles And Protocols* . Chapman And Hall/ CRC Press.

Koblitz, N. and Menezes, A. J. (2007). Another Look at Provable Security. *Journal of Cryptology*, 20(1):3–37.

Kocher, P. C. (1996). Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In *Advances In Cryptology - Crypto'96*, pages 104–113. Springer.

Kumanduri, R. and Romero, C. (1998). *Number theory with Computer Applications*. Prentice Hall New Jersey.

Kurosawa, K., Ito, T., and Takeuchi, M. (1988). Public Key Cryptosystem using a Reciprocal Number With the Same Intractability as Factoring a Large Number. *Cryptologia*, 12(4):225–233.

Kurosawa, K., Ogata, W., Matsuo, T., and Makishima, S. (2001). IND-CCA Public Key Schemes Equivalent To Factoring $N = pq$. In *Public Key Cryptography*, pages 36–47. Springer.

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

Lenstra, A. K. and Verheul, E. R. (2001). Selecting Cryptographic Key Sizes. *Journal Of Cryptology*, 14(4):255–293.

Maitra, S. and Sarkar, S. (2008). Revisiting Wiener's Attack - New Weak Keys in RSA. In *Information Security*, pages 228–243. Springer.

May, A. (2003). *New RSA Vulnerabilities Using Lattice Reduction Methods*. PhD thesis, University Of Paderborn.

May, A. (2004). Secret Exponent Attacks on RSA-type Schemes with Moduli $N = p^r q$. In *Public Key Cryptography–PKC 2004*, pages 218–230. Springer.

Menezes, A., Oorschot, P., and Vanstone, S. (1997). *Handbook Of Applied Cryptography*. CRC Press.

Messerges, T. S., Dabbish, E. A., and Sloan, R. H. (1999). Power Analysis Attacks of Modular Exponentiation in Smartcards. In *Cryptographic Hardware And Embedded Systems - CHES'99*, pages 144–157. Springer.

Müller, S. (2001). On the Security of Williams Based Public Key Encryption Scheme. In *Public Key Cryptography*, pages 1–18. Springer.

Müller, S. and Müller, W. B. (1998). The security of public key cryptosystems based on integer factorization. In *Information Security and Privacy*, pages 9–23. Springer.

Naor, M. and Yung, M. (1990). Public-Key Cryptosystems Provably Secure Against Chosen Ciphertext Attacks. In *Proceedings Of The Twenty-Second Annual ACM Symposium On Theory Of Computing*, pages 427–437. ACM.

Nishioka, M., Satoh, H., and Sakurai, K. (2002). Design and Analysis of Fast Provably Secure Public-Key Cryptosystems Based on a Modular Squaring. In *Information Security And Cryptology - ICISC 2001*, pages 81–102. Springer.

Nitaj, A. (2009). Cryptanalysis of RSA Using the Ratio of the Primes. In *Progress in Cryptology - AFRICACRYPT 2009*, pages 98–115. Springer.

Nitaj, A. (2011a). A New Vulnerable Class of Exponents in RSA. *JP Journal of Algebra, Number Theory and Applications*, 21(2):203–220.

Nitaj, A. (2011b). New weak RSA keys . *JP Journal of Algebra, Number Theory and Applications*, 23(2):131–148.

Nitaj, A. (2013). Diophantine and Lattice Cryptanalysis of the RSA Cryptosystem. In *Artificial Intelligence, Evolutionary Computing and Metaheuristics*, pages 139–168. Springer.

Novak, R. (2002). SPA-Based Adaptive Chosen-Ciphertext Attack on RSA Implementation. In *Public Key Cryptography*, pages 252–262. Springer.

Okamoto, T. and Uchiyama, S. (1998). A New Public-Key Cryptosystem as Secure as Factoring. In *Advances In Cryptology - EUROCRYPT'98*, pages 308–318. Springer.

Okeya, K. and Sakurai, K. (2001). Efficient Elliptic Curve Cryptosystems from a Scalar Multiplication Algorithm with Recovery of the *y*-coordinate on a Montgomery-form Elliptic Curve. In *Cryptographic Hardware and Embedded SystemsCHES 2001*, pages 126–141. Springer.

Okeya, K. and Takagi, T. (2006). Security Analysis of CRT-Based Cryptosystems. *International Journal Of Information Security*, 5(3):177–185.

Paillier, P. (1999). Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In *Advances In Cryptology - EUROCRYPT'99*, pages 223–238. Springer.

Rabin, M. O. (1979). Digitalized Signatures and Public-Key Functions as Intractable as Factorization. *MIT Technical Report*, MIT/LCS/TR-212.

Rackoff, C. and Simon, D. R. (1992). Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack. In *Advances In Cryptology - Crypto'91*, pages 433–444. Springer.

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.

Schindler, W. (2000). A Timing Attack Against RSA with the Chinese Remainder Theorem. In *Cryptographic Hardware And Embedded Systems - CHES 2000*, pages 109–124. Springer.

Schmidt-Samoa, K. (2006). A New Rabin-Type Trapdoor Permutation Equivalent To Factoring. *Electronic Notes In Theoretical Computer Science*, 157(3):79–94.

Shannon, C. E. (1949). Communication Theory Of Secrecy Systems. *Bell System Technical Journal*, 28(4):656–715.

Takagi, T. (1997). Fast RSA-Type Cryptosystems using *N*-Adic Expansion. In *Advances In Cryptology - Crypto'97*, pages 372–384. Springer.

Vuillaume, C. (2003). Efficiency Comparison of Several RSA Variants. *Studienarbeit (March 2003) http://www. cdc. informatik. tu-darmstadt. de/reports/reports/studien. pdf*.

Watanabe, Y., Shikata, J., and Imai, H. (2002). Equivalence Between Semantic Security and Indistinguishability Against Chosen Ciphertext Attacks. In *Public Key Cryptography - PKC 2003*, pages 71–84. Springer.

Wiener, M. J. (1990). Cryptanalysis of Short RSA Secret Exponents. *IEEE Transactions on Information Theory*, 36(3):553–558.

Williams, H. (1980). A Modification of the RSA Public-Key Encryption Procedure. *IEEE Transactions On Information Theory*, 26(6):726–729.