Malaysian Journal of Mathematical Sciences 10(S) August: 1–18 (2016)
Special Issue: The 7^{th} International Conference on Research and Education in Mathematics (ICREM7)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

Design of Rabin-Like Cryptosystem without Decryption Failure

Muhammad Asyraf Asbullah *[1] and Muhammad Rezal Kamel Ariffin[1,2]

[1]*Laboratory of Cryptology, Analysis and Structure, Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia*
[2]*Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, Malaysia*

*E-mail: *ma_ asyraf@upm.edu.my*
**Corresponding author*

ABSTRACT

In this work, we design a new, efficient and practical Rabin-like cryptosystem without using the Jacobi symbol, redundancy in the message and avoiding the demands of extra information for finding the correct plaintext. Decryption outputs a unique plaintext without any decryption failure. In addition, decryption only requires a single prime. Furthermore, the decryption procedure only computes a single modular exponentiation instead of two modular exponentiation executed by other Rabin variants. As a result, this reduces the computational effort during the decryption process. Moreover the Novak's side channel attack is impractical over the proposed Rabin-like cryptosystem. In parallel, we prove that the Rabin-p cryptosystem is indeed as intractable as the integer factorization problem.

Keywords: Rabin cryptosystem, modulus $N = p^2q$, unique decryption, equivalent to factorization, Chinese remainder theorem.

1. Introduction

Prior to 1970's, encryption and decryption were done only in symmetrically, until the advent of public key cryptosystem that was introduced by Diffie and Hellman (1976). At that time, the notion of asymmetric cryptosystem is somehow not well understood by many people. In 1978, the RSA cryptosystem (Rivest et al., 1978) went public and it is regarded now by the cryptographic community as the first practical realization of the asymmetric cryptosystem. The security of the RSA was based on the intractability to solve the modular e^{th}-root problem coupled with the integer factorization problem (IFP) of the form $N = pq$, where p and q are distinct and equal bit-size primes.

In 1979, another cryptosystem was introduced which is based on the intractability to solve the modular square root problem of a composite integer, namely the Rabin cryptosystem (Rabin, 1979). In fact, this cryptosystem is the first public key system of its kind that was proven equivalent to factoring $N = pq$. 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 $e = 2$ from the Rabin encryption gives a computational advantage over the RSA cryptosystem.

The encryption of Rabin (1979) is computed by executing a single squaring modulo N. This is far more efficient by comparison to RSA encryption, which requires the calculation of at least a cubic modulo $N = pq$ (Menezes et al., 1997). Based on recent results in this area the public exponent for RSA must be sufficiently large, thus Rabin has some advantage regarding this matter (Lenstra and Verheul, 2001). On the other hand, the process for Rabin's decryption breaks up into two parts. First is the calculation of two modular exponentiations, and secondly the computation of the Chinese Remainder Theorem (CRT) for recombination of the congruence's. Here the efficiency of the Rabin decryption is slightly faster than the 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 (mod 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 $N = pq$. 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 $N = pq$.

Motivation. In principle, the Rabin cryptosystem is very efficient because only a modular squaring operation is required for encryption; furthermore, it is proven to be as difficult as the IFP. Unfortunately, the Rabin cryptosystem suffers from two major drawbacks; the foremost one is because the Rabin's decryption produces four possible candidates, thus introduces ambiguity to decide the correct message out of four possible values. Another drawback is from the fact that its equivalence relation to factorization. These two disadvantages of the Rabin encryption scheme prevented it from widespread practical use.

Hence, attempts were made by numerous researchers with the objective to turn the Rabin cryptosystem to be as practical and implementable as the RSA cryptosystem. See Section 2.3 of this paper. Broadly speaking, all the previous attempts made seem to employ one or more additional features in order to obtain a unique decryption result, at the same time resulting in a free decryption failure Rabin-like cryptosystem. One of the ways to accomplish this is through manipulation of some mathematical objects such as the role of the Jacobi symbol. Also, it can be done by designing an encryption function with a special message structure. Yet, at the same time all the designs are losing the computational advantage of the original Rabin's encryption over the RSA cryptosystem.

Our Contributions. In order to engage this problem and to overcome all the shortcomings, further theoretical analysis and mathematical proves are needed. In this paper, our objective is to refine the Rabin cryptosystem in order to overcome all the previous drawbacks of its original design and its variants. We present an efficient and practical Rabin-like cryptosystem without using the Jacobi symbol, message redundancy technique or sending extra information in order to specify the correct plaintext. In addition, decryption only requires a single prime. Furthermore, the decryption procedure only computes a single modular exponentiation instead of two modular exponentiation executed by other Rabin variants. As a consequence, this brings down the computational effort during the decryption operation and most importantly, decryption outputs a unique plaintext without any decryption failure and resilient to Novak's

side channel analysis. In parallel, we prove that the Rabin-p cryptosystem is indeed as intractable as the IFP.

Paper Organization. Section 2 introduces the notion of public key encryption and the description of the original Rabin cryptosystem. This section also provides a survey for Rabin's variants and then provide a list of drawbacks from previous strategies that need to be avoided. Section 3 highlight the methodology of the research performed. Later in this section we also give a list of useful lemmas. We end this section with the description of our proposal, namely the Rabin-p cryptosystem, along with its proof of correctness. This is followed by proving that Rabin-p cryptosystem is indeed as intractable as the IFP and its related computational reducibility in Section 4 and Section 5, respectively. We put a conclusion in the final section.

2. Preliminaries

2.1 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 gets 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 2.1. *(Diffie and Hellman, 1976). Let $\mathcal{M}$ denote the message space, $\mathcal{C}$ denote the ciphertext space, $\mathcal{K}$ denote the key space, m denote the plaintext and c denote the ciphertext. The asymmetric encryption scheme is defined as follows.*

1. *Key generation algorithm K is a probabilistic algorithm that will generate a public key denoted as $e \in \mathcal{K}$ and private key as $d \in \mathcal{K}$ respectively.*
2. *Encryption algorithm E is a probabilistic algorithm that takes a message $m \in \mathcal{M}$ and the public key e, to produce a ciphertext $c \in \mathcal{C}$ 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, if 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 2.2. *(Proof of Correctness). For each pairs of key* $(e, d) \in \mathcal{K}$ *output by the algorithm* K*, and for every message* $m \in \mathcal{M}$ *and ciphertext* $c \in \mathcal{C}$ *then*

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

2.2 Rabin Cryptosystem

In this section, we present the Rabin cryptosystem. We begin with a description for the key generation as the following procedure. The private key consists of two random and distinct primes p and q, each satisfies 3 (mod 4) and the public key is the product $N = pq$.

Algorithm 1 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)

To encrypt a plaintext m, the Rabin encryption algorithm does the following.

Algorithm 2 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.

To decrypt a ciphertext with the private key p and q, the Rabin cryptosystem does the following.

Algorithm 3 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

2.3 A Survey for Rabin variants

It is very interesting to witness continuous efforts in searching for practical and optimal Rabin cryptosystem by numerous scholars. We put forward a survey for Rabin's variants as follows.

Williams (1980) makes an attempt to solve the 4-to-1 situation by incorporating the Jacobi symbol. Through this approach, Rabin-Williams scheme successfully provided unique decryption while maintaining the property of breaking such scheme is equivalence to factoring.

Subsequently, the same approach of using the Jacobi symbol with Rabin cryptosystem was proposed by Kurosawa et al. (1988). In the Kurosawa et al. (1988) scheme, the encryptor will compute and send two extra bits of information along with its ciphertext purposely to specify the correct square root (i.e the intended message). However, both encrypt-decrypt processes require the Jacobi symbol computation. This result in turn leads to additional computational cost.

Menezes et al. (1997) proposed a redundancy to the message, which is a technique to append the plaintext with repeating l least significant bits of the message before applying Rabin function upon it. With the help of adding some redundancies onto the message, the decryption process then is likely will give a unique output. This scheme has a probability $\frac{1}{2^{l-1}}$ of decryption failure, where l is the length of the least significant bits of the message.

Takagi (1997) proposed a Rabin-type cryptosystem with an alternative modulus choice of $N = p^2q$. Boneh (2001) suggest an elegant strategy; imposing some special properties to the plaintext (i.e. padding scheme and mes-

sage restriction) before encryption of which contribute to produce a unique message with high probability. Rabin-Boneh cryptosystem is considered as an optimal Rabin-type encryption in term of efficiency since it does not use the Jacobi symbol while the message output of the decryption process is unique with high probability. Notice that, the problem with introducing a padding or redundancy to a plaintext is the decryption may fail with a small probability.

Industrial giants, Hitachi (2002) also made a contribution regarding the use of modulus $N = p^2q$ as depicted earlier by Takagi (1997) (i.e.Rabin-Takagi cryptosystem). Basically, HIME(R) and Rabin-Takagi are quite similar in term of performing the Rabin function for encryption and solving modular square root with modulus $N = p^2q$ as parts of their decryption process. However, the method used by the HIME(R) decryption to solve the square roots modulo $N = p^2q$ is significantly different from the Rabin-Takagi.

Schmidt-Samoa (2006) introduced a new Rabin-type trapdoor permutation which is proven as difficult as factoring $N = p^2q$. Even though it is indeed a Rabin variant, however, we will not consider it in this paper. The reason is because one of our objectives is actually to find a better answer to solving the Rabin's $4-$to-1 decryption problem, whilst the decryption of Schmidt-Samoa cryptosystem produces a $p-$to-1 mapping.

Freeman et al. (2013) propose a design of Rabin-like cryptosystem which require to sends extra bits and relies extensively on the Jacobi symbol. However, the entire computed Jacobi symbol in this scheme is embedded implicitly in the ciphertext. This is in contrast to the design of Kurosawa et al. (2001), which does clearly expose such information as a part of the ciphertext. We observe that the usage of the Jacobi symbol during key generation, the encryption and decryption procedure implies extra computations. Furthermore, this cryptosystem still leaks the most significant bit of the plaintext m (Galbraith, 2012).

Recently, a new Rabin variant proposed by Elia et al. (2015). The design of this newly Rabin-like cryptosystem exploiting the Dedekind's sums theorem for the identification processes amongst the four possible roots.

2.4 Pre-Conditions

In this section, we initiate a list that describes the drawback of the previous strategies to overcome the Rabin weaknesses. This list provides conditions that needed to be avoided in any attempt to refine the Rabin scheme.

2.4.1 The Use of Jacobi Symbol

The requirement to compute Jacobi symbol possibly during the key generation, encryption or decryption makes the system less efficient (Boneh, 2001). In terms of computational performance, a Rabin-like cryptosystem is extremely fast as long as this process does not require for computing a Jacobi symbol (Galbraith, 2012).

2.4.2 Message Redundancy and Padding Mechanism

Some schemes introduce redundancy upon the message or design padding mechanism aiming to achieve an efficient way to determine the correct plaintext from its four possible candidates. For instance, as for the HIME(R) cryptosystem that applies the OAEP scheme (Hitachi, 2002) and the Rabin-Boneh with a padding mechanism that designated to be simpler than OAEP (Boneh, 2001). However, both methods still have a small probability for decryption failure.

2.4.3 Novak's Side Channel Analysis

In general, the decryption algorithm of a Rabin-like cryptosystem consists of two parts. The first part is for the modular exponentiation operation of which in order to obtain the message in the form of m modulo p and m modulo q from its corresponding ciphertext c. The second part then would be the recombination process using the Chinese Remainder Theorem (CRT) algorithm to recover the proper message m. Most side channel attacks deal with the first part. For instance, from the work by Kocher (1996), Schindler (2000) and Brumley and Boneh (2005) which uses the timing analysis approach or the result in Messerges et al. (1999) enables side channel analysis using the power analysis approach. Alternatively, Novak (2002) proposed a very efficient side channel analysis upon the CRT computation (i.e. the second part of the Rabin-like decryption).

From the survey done in Section 2.3, we observe that all variants of the Rabin-like cryptosystem (except Rabin-Williams scheme) involves a process that depends heavily on the CRT or Garner's algorithm (i.e. the process to recover all the modulo square roots). Therefore, Novak's analysis is indeed applicable for such computation, of which can result in the insecurity of the cryptosystems (Okeya and Takagi, 2006).

3. Our Propose Scheme

3.1 Methodology

In this section, we outline the methodology to overcome the drawbacks of the Rabin cryptosystem. Firstly, we assign the condition on the modulus to be used is of the type $N = p^2q$. We observed that such modulus claimed to be no easier as to factoring the standard $N = pq$ (Castagnos et al., 2009). This statement is supported by the fact that many RSA-like cryptosystems are designed using such modulus (Asbullah and Ariffin, 2015). We then impose restriction on the plaintext m and ciphertext c space as $m \in \mathbb{Z}_{p^2}$ and $c \in \mathbb{Z}_{p^2q}$, respectively. From the plaintext-ciphertext expansion, such restriction leads to a system that is not a length-preserving for the message.

Let m and c be the plaintext and ciphertext and $c(m)$ be the function of c taking m as its input. Suppose, for example, the plaintext spaces and the ciphertext spaces in the RSA cryptosystem are the same. Thus we denote the function for the RSA cryptosystem as $c(m) : \mathbb{Z}_{pq} \longrightarrow \mathbb{Z}_{pq}$. Note that this situation could be an advantage for the RSA scheme since RSA encryption has no message expansion. However, this is not true for all cryptosystems. For example, the plaintext-ciphertext mapping for Okamoto-Uchiyama cryptosystem (Okamoto and Uchiyama, 1998) is $c(m) : \mathbb{Z}_p \longrightarrow \mathbb{Z}_{p^2}$, Pailier cryptosystem (Paillier, 1999) and the cryptosystem proposed by Galindo et al. (2002) is $c(m) : \mathbb{Z}_{pq} \longrightarrow \mathbb{Z}_{(pq)^2}$, Rabin-Boneh (Boneh, 2001) mapping is $c(m) : \mathbb{Z}_{\frac{pq}{2}} \longrightarrow \mathbb{Z}_{pq}$ and the Rabin variant introduced by Ariffin et al. (2013) and Schmidt-Samoa (2006) is $c(m) : \mathbb{Z}_{pq} \longrightarrow \mathbb{Z}_{p^2q}$.

The maximum size for the message is defined by the plaintext space. One way to do it would be to tell the user a maximum number of bits for the plaintext messages. If we view the message as merely the keys for a symmetric encryption scheme, meaning that the message is indeed a short message, then this is not a big issue since many other schemes also implemented such approach. Therefore, we contend that the restriction of message space would turn a restriction is not an issue.

3.2 Useful Lemmas

Lemma 3.1. *(Kumanduri and Romero, 1998). Let p be a prime number such that $p \equiv 3 \pmod 4$ and c an integer such that $\gcd(c, p) = 1$. The congruence $c \equiv m^2 \pmod p$ has either no solutions or exactly two solutions. If m_1 is a solution, then $-m_1 \pmod p$ is the other solution.*

Lemma 3.2. *(Kumanduri and Romero, 1998). Let p be a prime number such that $p \equiv 3 \pmod 4$ and c an integer such that $\gcd(c, p) = 1$. The congruence $c \equiv m^2 \pmod{p^2}$ has exactly two solutions if $c \equiv m^2 \pmod p$ has exactly two solutions.*

Lemma 3.3. *Consider Lemma 3.2. Let $c \equiv m^2 \pmod{p^2}$. Then $m_1 = m_p + jp$ is a solution to $c \equiv m^2 \pmod{p^2}$ where $m_p \equiv c^{\frac{p+1}{4}} \pmod p$, $j \equiv \frac{i}{2m_p} \pmod p$ such that $i = \frac{c - {m_p}^2}{p}$. Furthermore $m_2 \equiv -m_1 \pmod{p^2}$ is the other solution.*

Proof. Suppose we consider $c \equiv m^2 \pmod{p^2}$ as in Lemma 3.2. Let $m_p \equiv c^{\frac{p+1}{4}} \pmod p$ such that ${m_p}^2 \equiv c \pmod p$. Suppose that $m_1 = m_p + jp$ is a solution for $c \equiv m^2 \pmod{p^2}$, then we have

$$\begin{aligned} c &\equiv m_1^2 \\ &\equiv (m_p + jp)^2 \\ &\equiv {m_p}^2 + 2m_p jp \pmod{p^2} \end{aligned} \tag{1}$$

Then, rearrange (1) as

$$2m_p jp \equiv c - {m_p}^2 \pmod{p^2} \tag{2}$$

Note that from ${m_p}^2 \equiv c \pmod p$, we have $c - {m_p}^2 \equiv 0 \pmod p$ which means that $c - {m_p}^2$ is a multiple of p. Let $ip = c - {m_p}^2$ for some integer i, then we obtain $i = \frac{c - {m_p}^2}{p}$. We then rewrite (2) as

$$2m_p jp \equiv ip \pmod{p^2},$$

of which such congruence implies that $2m_p j \equiv i \pmod p$. Hence, we obtain $j \equiv \frac{i}{2m_p} \pmod p$. To conclude, we have the solution $m_1 = m_p + jp$ such that $c \equiv {m_1}^2 \pmod{p^2}$. Furthermore, we observe that $m_2 \equiv -m_1 \pmod{p^2}$ is the other solution as in Lemma 3.2. □

Lemma 3.4. *Consider Lemma 3.3. If m_1 and m_2 are the two distinct integers solution for $c \equiv m^2 \pmod{p^2}$, then $m_1 + m_2 = p^2$.*

Proof. Suppose $m_1 \not\equiv m_2 \pmod{p^2}$ such that ${m_1}^2 \equiv {m_2}^2 \equiv c \pmod{p^2}$. Observe that, from Lemma 3.3 if m_1 is a solution for $c \equiv m^2 \pmod{p^2}$, then $m_2 \equiv -m_1 \pmod{p^2}$ is also a solution. Thus, $m_2 \equiv -m_1 \pmod{p^2}$ can be reinterpreted as $m_2 = p^2 - m_1$. Hence $m_1 + m_2 = p^2$. □

Lemma 3.5. *Let m_1 and m_2 be integers such that $m_1 + m_2 = p^2$ with p^2 is an odd integer. Then either m_1 or m_2 is less than $\frac{p^2}{2}$.*

Proof. Suppose p^2 is an odd integer, then by definition $\frac{p^2}{2}$ must not be an integer. Let $m_1 + m_2 = p^2$. Since that m_1 and m_2 are integers, therefore m_1 and m_2 must not be equal to $\frac{p^2}{2}$.

Suppose we consider the following cases. If for both m_1 and m_2 are less than $\frac{p^2}{2}$, then we should have $m_1 + m_2 < p^2$. Therefore this case contradicts with the fact that $m_1 + m_2 = p^2$. On the other hand, if m_1 and m_2 are greater than $\frac{p^2}{2}$, then we should have $m_1 + m_2 > p^2$, which also contradicts with the fact that $m_1 + m_2 = p^2$. Hence, we consider the case where either m_1 or m_2 is less than $\frac{p^2}{2}$. Let $m_1 < \frac{p^2}{2}$, then there exists a real number ϵ_1 such that $m_1 + \epsilon_1 = \frac{p^2}{2}$. On the other hand, since $m_1 < \frac{p^2}{2}$, then m_2 must be greater than $\frac{p^2}{2}$. Therefore there exists a real number ϵ_2 such that $m_2 - \epsilon_2 = \frac{p^2}{2}$. If we add up these equations, we have

$$(m_1 + \epsilon_1) + (m_2 - \epsilon_2) = \frac{p^2}{2} + \frac{p^2}{2} = p^2$$

Since $m_1 + m_2 = p^2$, thus $\epsilon_1 - \epsilon_2$ should be equal to zero, meaning that $\epsilon_1 = \epsilon_2$. We conclude that only one of m_1 or m_2 is less than $\frac{p^2}{2}$. □

3.3 The Rabin-p Cryptosystem

In this section, we provide the details of the proposed cryptosystem namely Rabin-p Cryptosystem. Rabin-p is named after the Rabin cryptosystem with the additional p symbolizing that the proposed scheme only uses a single prime p as the decryption key. This section is structured as follows. We first describe the Rabin-p key generation, encryption and decryption procedures. We then provide the explanation of the Rabin-p decryption process.

The key generation algorithm of the Rabin-p cryptosystem (Algorithm 4) produces two random and distinct primes p and q of the same length such that $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$. The key generation algorithm then produces an integer N as a product $N = p^2q$, which is denoted as the public key. The private key is the prime p.

Algorithm 4 Rabin-p Key Generation Algorithm

Input: The size k of the security parameter
Output: The public key $N = p^2q$ and the private key p
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 $N = p^2q$
3: Return the public key N and the private key p

The encryption algorithm (Algorithm 5) takes the plaintext $m < 2^{2k-1}$ and compute $c \equiv m^2 \pmod N$. We observe that the message m is restricted to the range of $m < 2^{2k-1} = \frac{2^{2k}}{2} < \frac{p^2}{2} < p^2$. The output is the ciphertext c.

Algorithm 5 Rabin-p Encryption Algorithm

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

To decrypt a ciphertext, the Rabin-p decryption algorithm with the private key p does the following.

Algorithm 6 Rabin-p Decryption Algorithm

Input: A ciphertext c and the private key p
Output: The plaintext m
1: Compute $w \equiv c \pmod p$
2: Compute $m_p \equiv w^{\frac{p+1}{4}} \pmod p$
3: Compute $i = \frac{c - {m_p}^2}{p}$
4: Compute $j \equiv \frac{i}{2m_p} \pmod p$
5: Compute $m_1 = m_p + jp$
6: If $m_1 < 2^{2k-1}$, then return $m = m_1$. Else, return $m = p^2 - m_1$

We observe that the decryption algorithm needs only a single prime number as its key. In addition, only one modular exponentiation is taking place during the decryption process. Such computational advantage would positively affect the overall operations.

Remark 3.1. *We reason that since our proposed scheme does not need to carry out any CRT computation, thus the Novak's attack is not applicable on the Rabin-p cryptosystem (i.e. resilient against Novak's attack).*

3.4 Proof of Correctness for Rabin-p Decryption

Proposition 3.1. *Let* $c \equiv m^2 \pmod{N}$ *be the Rabin-p ciphertext. Then Algorithm 6 is correct.*

Proof. Suppose $c \equiv m^2 \pmod{N}$ be the Rabin-p ciphertext where $N = p^2q$, thus we have $c - m^2 \equiv 0 \pmod{N}$. Since $p^2 \mid N$, then $p^2 \mid c - m^2$. Since $m < p^2$, therefore it is sufficient just solving for $c \equiv m^2 \pmod{p^2}$ which is efficiently be solved using Lemma 3.3. In addition, according to Lemma 3.2, there are exactly two distinct solution m_1 and m_2 satisfies $c \equiv m^2 \pmod{p^2}$. From Lemma 3.4 we have $m_1 + m_2 = p^2$. We now show that the Algorithm 6 only produce a unique solution for $m < 2^{2k-1}$. Observe that the upper bound for $m < \frac{p^2}{2}$. Consider Lemma 3.5, then we have either m_1 or m_2 is less than $\frac{p^2}{2}$ such that $m_1 + m_2 = p^2$ satisfy $m < 2^{2k-1}$. Finally, we conclude that only one of m_1 or m_2 are less than $\frac{p^2}{2}$ and will be outputted by Algorithm 6 as the unique $m < 2^{2k-1}$. □

4. Equivalent to Factoring $N = p^2q$

In this section, we show that if there exists someone or an algorithm can anyhow decrypt the message m from the Rabin-p's ciphertext, then that someone must be also able to factor $N = p^2q$. Observe the following.

Proposition 4.1. *Let* $N = p^2q$, $m < 2^{2k-1}$ *and* $2^{2k-1} < \hat{m} < p^2$ *such that* $m + \hat{m} = p^2$. *Then* $\gcd(m + \hat{m}, N) = p^2$.

Proof. Suppose $2^k < p < 2^{k+1}$, then $2^{2k} < p^2 < 2^{2k+2}$, and $2^{2k-1} < \frac{p^2}{2} < 2^{2k+1}$. Suppose $m < 2^{2k-1}$, then from Lemma 3.5 there exists another integer $\hat{m} > 2^{2k-1}$ such that $m + \hat{m} = p^2$. Thus this implies $p^2 - \hat{m} = m < 2^{2k-1}$.

Now, we determine the range of the $\hat{m}$ such that $p^2 - \hat{m} < 2^{2k-1}$. Then we obtain the lower bound for $\hat{m}$, of which

$$\hat{m} > p^2 - 2^{2k-1} > 2^{2k} - 2^{2k-1} = 2^{2k-1}$$

and upper bounded by $\hat{m} < p^2$. Take the $\gcd(m + \hat{m}, N)$, then we obtain p^2. Hence $q = \frac{N}{p^2}$. □

From here, with the help from the Algorithm 6, we can build a factoring algorithm for N. The factoring algorithm is defined as follows.

Algorithm 7 Algorithm for Factoring $N = p^2q$

Input: A ciphertext c and the modulus N
Output: The prime factors p,q
1: Choose an integer $2^{2k-1} < \hat{m} < 2^{2k}$
2: Compute $\hat{c} \equiv \hat{m}^2 \pmod{N}$
3: Ask the decryption of $\hat{c}$ from Algorithm 6
4: Algorithm 6 output $m < 2^{2k-1}$, else reject
5: Compute $\gcd(\hat{m} + m, N)$
6: If $\gcd(\hat{m} + m, N) = 1$, then reject
7: If $\gcd(\hat{m} + m, N) \neq 1$, then return p^2
8: Compute $\frac{N}{p^2} = q$
9: Return the prime factors p, q

5. Computational Reducibility

If a new cryptosystem is designed, we are expected to provide a comparison of the relative difficulty of breaking the scheme to the solving any existing hard problems. We begin with the following definitions.

Definition 5.1 (Computational Reduction)**.** *Let $\mathcal{A}$ and $\mathcal{B}$ be two different cryptographic hard problems. We say that a problem $\mathcal{A}$ is reducible to a problem $\mathcal{B}$ if by any mean we able to show that for an algorithm that solves problem $\mathcal{B}$ then such algorithm also solves the problem $\mathcal{A}$.*

Definition 5.2 (Computational Equivalent)**.** *Let $\mathcal{A}$ and $\mathcal{B}$ be two different cryptographic hard problems. A problem $\mathcal{A}$ is said to be equivalent to problem $\mathcal{B}$ if and only if the problem $\mathcal{A}$ is reducible to problem $\mathcal{B}$ and vice-versa.*

Now, we show that breaking the Rabin-p cryptosystem is indeed reducible to factoring the modulus $N = p^2q$. Furthermore, the converse of such statement is also true.

Lemma 5.1. *Breaking the Rabin-p cryptosystem is reducible to factoring $N = p^2q$.*

Proof. Suppose there exists an algorithm $\mathcal{A}_1$ with the ability to factor the modulus $N = p^2q$, then we obtain the primes p and q. Thus, we can solve the Rabin-p's ciphertext $c \equiv m^2 \pmod{N}$ directly by using the Algorithm 6. □

Lemma 5.2. *Factoring $N = p^2q$ is reducible to breaking the Rabin-p cryptosystem.*

Proof. Conversely, suppose there exists an algorithm $\mathcal{A}_2$ that breaks the Rabin-p cryptosystem. Then such algorithm is able to find the message m from the ciphertext $c \equiv m^2 \pmod{N}$. By using the same approach as Proposition 4.1, hence $\mathcal{A}_2$ can proceed to compute $\hat{m}$. Finally, with the help of Algorithm 7, $\mathcal{A}_2$ can easily factor the modulus $N = p^2q$. □

Proposition 5.1. *Breaking the Rabin-p cryptosystem is equivalence to factoring the modulus $N = p^2q$.*

Proof. This assertion is a consequence from Lemma 5.1 and Lemma 5.2. □

Remark 5.1. *In other words, it is mathematically proven that a random plaintext can be recovered completely from the ciphertext, if and only if we are able to efficiently factoring the public key $N = p^2q$.*

6. Conclusion

This study can be viewed as another look at the design of the Rabin cryptosystem, from a different view. Our proposed cryptosystem namely the Rabin-p cryptosystem is purposely designed with the objective to avoid the Jacobi symbol, redundancy in the message and the demands of extra information for finding the correct plaintext. We observe that the decryption process outputs a unique plaintext without any decryption failure while requires only a single prime number. We further show that the decryption procedure only computes a single modular exponentiation instead of two modular exponentiation executed by other Rabin variants. As a result, this reduces the computational effort during the decryption process. Finally, we show that Rabin-p cryptosystem is indeed as intractable as the integer factorization problem.

Acknowledgment

The authors would like to thank the Ministry of Education, Malaysia and Institute for Mathematical Research, Universiti Putra Malaysia for research

funding. The authors also would like to thank Prof. Dr. Abderrahmane Nitaj from the Laboratoire de Mathématiques, Université de Caen, France, for valuable comments and discussion.

References

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

Asbullah, M. A. and Ariffin, M. R. K. (2015). New Attacks on RSA with Modulus $N = p^2q$ Using Continued Fractions. *Journal of Physics: Conference Series*, 622(1):012019.

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.

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

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.

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

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

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.

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 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.

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.

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

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