Malaysian Journal of Mathematical Sciences 11(S) April : 9–20 (2017)
Special Issue: The 2nd International Conference and Workshop on Mathematical Analysis (ICWOMA 2016)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

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

Efficient Methods to Overcome Rabin Cryptosystem Decryption Failure

Mahad, Z. *[1], Asbullah, M. A.[1,2], and Ariffin, M. R. K.[1,3]

[1] *Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia*
[2] *Centre of Foundation Studies for Agriculture Sciences, Universiti Putra Malaysia, Malaysia*
[3] *Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, Malaysia*

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

ABSTRACT

Rabin cryptosystem is an efficient factoring-based scheme, however, its decryption produces 4-to-1 output, which leads to decryption failure. In this work, in order to overcome the 4-to-1 decryption problem for the Rabin cryptosystem, we propose two distinct methods using the modulus of the type $N = p^2q$ coupled with the restriction on the plaintext space M. In the first method, the plaintext space is limited to $M \in \mathbb{Z}_{pq}$. For the second method, we restrict the plaintext in the range of $M \in (0, 2^{2n-2})$. Importantly, we prove that the decryption output of the proposed methods is unique and without decryption failure. The results in this work indicate that the decryption problem of Rabin cryptosystem is overcome.

Keywords: Rabin cryptosystem, unique decryption, equivalent to factorization.

1. Introduction

In 1979, the Rabin cryptosystem was introduced based on the intractability to solve the square root modulo problem of a composite integer, $N = pq$ Rabin (1979). This cryptosystem is the public key system that was proven equivalent of factoring $N = pq$. The Rabin cryptosystem also might be considered as a variant of the RSA cryptosystem with utilizing of the public exponent $e = 2$ compared to the RSA with public exponent $e \geq 3$. By utilizing the public exponent $e = 2$, the Rabin encryption gives a computational advantage over the RSA cryptosystem.

In the Rabin encryption procedure, a single execution of the squaring modulo N is computed with complexity order $O(n^2)$. This is far more efficient and faster by comparison to the RSA encryption procedure. The RSA encryption procedure requires the calculation of at least cubic modulo N with complexity order $O(n^3)$. 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). In the Rabin decryption procedure, it requires computation of two modular exponentiations and computation of the Chinese Remainder Theorem (CRT). This makes the Rabin decryption process to be slightly faster than the RSA.

The Rabin encryption in the form $C \equiv M^2 \pmod{N}$, where $N = pq$ with p and q are primes congruence $3 \pmod{4}$ is considered to be as hard as factoring problem. It is mathematically proven that the adversary is able to efficiently factor the modulus $N = pq$ then the plaintext can be recovered. It is well established in the literature Rabin decryption process will produce four possible plaintexts, thus introduces ambiguity to decide the correct plaintext. This scenario is due to the process of solving the square root problem by the Chinese Remainder Theorem (CRT).

Hence, several attempts were made by researchers with the objectives to turn the Rabin cryptosystem to be as practical and implementable as the RSA cryptosystem. All the previous attempts made seem to utilize one or more additional techniques in order to obtain a unique decryption result, at the same time resulting in a free decryption failure Rabin-like cryptosystem. Some of the techniques to accomplish this are through manipulation of the Jacobi symbol during the key generation process, provide extra information and also use the concept of message padding during the encryption process. Also, it can be accomplish by designing an encryption function with a special message structure. However, at the same time all of 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, we revisit Rabin cryptosystem and its variants. In this paper, our objective is to refine the Rabin encryption scheme in order to defeat all the previous drawbacks of its original design and its variants. We present efficient and practical methods to overcome Rabin cryptosystem decryption failure without using the Jacobi symbol, message redundancy technique or sending extra information in order to specify the correct plaintext. In addition, our proposed methods produce a unique decryption result without decryption failure and are indeed as intractable as the integer factorization problem.

Paper Organization. Section II introduces the description of the original Rabin cryptosystem. This section also provides a survey for Rabin's variants and then provides a list of drawbacks from previous strategies that need to be avoided. Section III highlights our proposed methods, along with its proof of correctness and examples. We put a conclusion in the final section.

2. Preliminaries

2.1 Rabin Cryptosystem

The Rabin cryptosystem is defined as follow.

Algorithm 1 Rabin Key Generation Algorithm

```
Require: The size $n$ of the security parameter
Ensure: The public key $N$ and the private key $(p, q)$.
Choose two random and distinct primes $p$ and $q$ such that $2^n < p, q < 2^{n+1}$ satisfying $p, q \equiv 3 \pmod 4$.
Compute $N = pq$.
Return the public key $N$ and the private key $(p, q)$.
```

Algorithm 2 Rabin Encryption Algorithm

```
Require: The public key $N$ and the plaintext $M$.
Ensure: The ciphertext $C$.
Choose any integer $M \in \mathbb{Z}_N$
Compute $C \equiv M^2 \pmod N$.
Return the ciphertext $C$.
```

Algorithm 3 Rabin Decryption Algorithm

```
Require: The private key $(p, q)$ and the ciphertext $C$.
Ensure: The plaintext $M$.
Compute $m_p \equiv C^{\frac{p+1}{4}} \pmod{p}$.
Compute $m_q \equiv C^{\frac{q+1}{4}} \pmod{q}$.
Compute two integers $r$ and $s$ such that $rp + sq = 1$.
Compute $M_1 \equiv rpm_q + sqm_p \pmod{N}$.
Compute $M_2 \equiv rpm_q - sqm_p \pmod{N}$.
Compute $M_3 \equiv -M_2 \pmod{N}$.
Compute $M_4 \equiv -M_1 \pmod{N}$.
Return the correct plaintext $M$ amongst the four possible candidates.
```

2.2 Rabin's Variants

Since 1979, many efforts have been put into research in searching for practical and optimal Rabin cryptosystem by numerous scholars. We put forward the summary for Rabin's variants as follows.

In 1980, Williams Williams (1991) made an attempt to solve 4-to-1 situation of the Rabin decryption problem by incorporating the Jacobi symbol. This scheme also known as Rabin-Williams cryptosystem. Through this technique, Rabin-Williams scheme manage to solve 4-to-1 situation of the Rabin decryption problem with unique decryption while maintaining the property of breaking such scheme is equivalence to factoring.

In 1988, Kurosawa *et al.* Kurosawa et al. (1991) use the same technique of using the Jacobi symbol couple with the concept of extra information (two extra bits) to solve 4-to-1 situation of the Rabin decryption problem. In the proposed scheme, two extra bits as extra information will be computed and send along with its ciphertext purposely to specify the correct square root. However, due to computation of the Jacobi symbol, its result in turn leads to additional computational cost.

In 1997, Menezes *et al.* Menezes et al. (1997) proposed a technique of redundancy in the messages, which is a technique to append the plaintext with repeating of least significant bits of the message with a pre-defined length l before encryption process. By using this technique, the decryption process is likely will give a unique output. However, this scheme has a probability $\frac{1}{2^{l-1}}$ of decryption failure Menezes et al. (1997).

Also in 1997, Takagi Takagi (1997) proposed a Rabin-type cryptosystem also known as Rabin-Takagi with an alternative modulus choice of $N = p^2q$. In 2001, Boneh Boneh (2001) proposed a scheme that does not use the Jacobi symbol and padding or redundancy to a plaintext but the message output of the decryption process is unique with high probability. Next, in 2002, Nishioka *et al.* Nishioka et al. (2002) also made a contribution regarding the use of modulus $N = p^2q$ as depicted earlier by Rabin-Takagi cryptosystem called HIME(R). Basically, HIME(R) and Rabin-Takagi are quite similar in term of performing the encryption process 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.

3. Our Propose Methods

In this section, we provide the details of the proposed methods. In designing the proposed methods, we will not use the Jacobi symbol, extra information concept and and padding or redundancy to a plaintext. The proposed methods are defined as follows.

3.1 Method I: $M \in \mathbb{Z}_{pq}$ and $N = p^2q$

In the first method, we use an alternative modulus choice of $N = p^2q$ as previously proposed by Takagi. We then impose restriction on the plaintext M space as $M \in \mathbb{Z}_{pq}$.

Algorithm 4 Method I Key Generation Algorithm

```
Require: The size $n$ of the security parameter
Ensure: The public key $N$ and the private key $(p, q)$.
1: Choose two random and distinct primes $p$ and $q$ such that $2^n < p, q < 2^{n+1}$
   satisfying $p, q \equiv 3 \pmod 4$.
2: Compute $N = pq$.
3: Return the public key $N$ and the private key $(p, q)$.
```

Algorithm 5 Method I Encryption Algorithm

```
Require: The public key $N$ and the plaintext $M$.
Ensure: The ciphertext $C$.
1: Choose any integer $M \in \mathbb{Z}_{pq}$
2: Compute $C \equiv M^2 \pmod{N}$.
3: Return the ciphertext $C$.
```

Algorithm 6 Method I Decryption Algorithm

```
Require: The private key $(p, q)$ and the ciphertext $C$.
Ensure: 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 two integers $r$ and $s$ such that $rp + sq = 1$.
4: Compute $M_1 \equiv rpm_q + sqm_p \pmod{pq}$.
5: Compute $M_2 \equiv rpm_q - sqm_p \pmod{pq}$.
6: Compute $M_3 \equiv -M_2 \pmod{pq}$.
7: Compute $M_4 \equiv -M_1 \pmod{pq}$.
8: For $i = 1$ to 4 compute $W_i = \frac{C - M_i^2}{N}$.
9: Return the correct plaintext $M = M_i$ which produces $W_i \in \mathbb{Z}$.
```

Remark 3.1. *Let p and q be two distinct primes such that p, $q \equiv 3 \pmod{4}$. Suppose M_i for $1 \leq i \leq 4$ be the four distinct solutions of modular square roots of $M^2 \pmod{N}$ using Chinese Remainder Theorem (CRT) as depicted in the step 4 - 7 in Algorithm 6. Then we have the congruence relation of M_i for $i = 1$ to 4 such that $M_4 \equiv -M_1 \pmod{N}$ and $M_3 \equiv -M_2 \pmod{N}$.*

Remark 3.2. *The correct plaintext M can be determined when the value of W_i is a perfect integer. Thus, one proceed computing the $W_i = \frac{C - M_i^2}{N}$ for maximum four times to determine the correct M.*

3.2 Method II: $M \in (0, 2^{2n-2})$ and $N = p^2q$

In the second method, we still use an alternative modulus choice of $N = p^2q$ as previously proposed by Takagi. However, for the plaintext M space is restricted to $M \in (0, 2^{2n-2})$.

Algorithm 7 Method II Key Generation Algorithm

```
Require: The size $n$ of the security parameter
Ensure: The public key $N$ and the private key $(p, q)$.
Choose two random and distinct primes $p$ and $q$ such that $2^n < p, q < 2^{n+1}$ satisfying $p, q \equiv 3 \pmod 4$.
Compute $N = pq$.
Return the public key $N$ and the private key $(p, q)$.
```

Algorithm 8 Method II Encryption Algorithm

```
Require: The public key $N$ and the plaintext $M$.
Ensure: The ciphertext $C$.
Choose any integer $M \in (0, 2^{2n-2})$
Compute $C \equiv M^2 \pmod N$.
Return the ciphertext $C$.
```

Algorithm 9 Method II Decryption Algorithm

```
Require: The private key $(p, q)$ and the ciphertext $C$.
Ensure: The plaintext $M$.
Compute $m_p \equiv C^{\frac{p+1}{4}} \pmod p$.
Compute $m_q \equiv C^{\frac{q+1}{4}} \pmod q$.
Compute two integers $r$ and $s$ such that $rp + sq = 1$.
Compute $M_1 \equiv rpm_q + sqm_p \pmod{pq}$.
Compute $M_2 \equiv rpm_q - sqm_p \pmod{pq}$.
Compute $M_3 \equiv -M_2 \pmod{pq}$.
Compute $M_4 \equiv -M_1 \pmod{pq}$.
For $i = 1$ to 4 compute $W_i = \frac{C - M_i^2}{N}$ for $M_i < 2^{2n-1}$, else reject.
Return the correct plaintext $M = M_i$ which produces $W_i \in \mathbb{Z}$.
```

Proposition 3.1. *Suppose p and q such that $2^{n-1} \leq p, q \leq 2^n - 1$ and M_i for $i = 1$ to 4 as previously defined. Then there exist at exactly two integers of M_i such that smaller than 2^{2n-1}.*

Proof. Let p and q such that $2^{n-1} \leq p, q \leq 2^n - 1$ thus we will have $pq \in (2^{2n-1}, 2^{2n} - 1)$. This condition implies that $\frac{pq}{2} \geq 2^{2n-2}$. Since we have set $M < 2^{2n-2}$, hence we will get $M < 2^{2n-2} \leq \frac{pq}{2} < pq$. Suppose we have four distinct solutions M_i for $i = 1$ to 4. Assume that amongst the four solutions, we have $M_a \in (0, 2^{2n-2})$. From Remark 3.1, we also need to compute

$-M_a \pmod{pq}$ as can be easily computed as $pq - M_a$. Observe that since $M_a \in (0, 2^{2n-2})$ therefore we confirm that $pq - M_a > 2^{2n-1}$. For now, we need to settle with the two other solutions. Let M_a is the other solution such that is not equal to either M_a or $pq - M_a$. We need to consider two cases as follows.

Case 1: If $M_b \in (0, 2^{2n-2})$, then it follows the above explanation.

Case 2: If $M_b > 2^{2n-2}$, then $pq - M_b < 2^{2n-1} - 2^{2n-2} = 2^{2n-2}$, thus would be greater or equal than 2^{2n-2}. ■

Corollary 3.1. *Suppose p and q such that $2^{n-1} \leq p, q \leq 2^n - 1$ and M_i for $i = 1$ to 4 as previously defined. Then there exist exactly two integers of M_i discarded during decryption.*

Proof. As provided by Proposition 3.1, we extend the result such that exactly two integers of M_i for $i = 1$ to 4 that are greater or equal than 2^{2n-2}, in which those elements does not fall on the range of M. Hence, these two integers are directly discarded during the decryption process. ■

3.3 Proof of Correctness

The proposed methods above have produces the correct and unique solution output M during their decryption process. The proof of correctness and uniqueness are described as follows. We will begin with the proof of correctness followed by the proof of uniqueness.

Lemma 3.1. *Let $N = p^2q$. Choose $M \in Z_{pq}$. If $C \equiv M^2 \pmod N$ and $V \equiv C \pmod{pq}$, then $V \equiv M^2 \pmod{pq}$.*

Proof. We have

$$C = M^2 + Nk_1 \text{ where } k_1 \in Z \tag{1}$$

and

$$V = C + pqk_2 \text{ where } k_2 \in Z \tag{2}$$

From (1) and (2) we have

$$V = M^2 + Nk_1 + pqk_2$$

Finally,

$$V \equiv M^2 \pmod{pq}$$

■

Proposition 3.2. *Let C be an integer representing a ciphertext encrypted using the proposed methods. Then, $C \equiv M^2 \pmod N$ has a unique solution for M.*

Proof. We begin with the proof of correctness of the decryption procedure. Since $M \in Z_{pq}$, by solving $V \equiv C \pmod{pq}$ using the Chinese Remainder Theorem (CRT), we will obtain all 4 roots of V. Also by Lemma 3.1, indeed $V \equiv M^2 \pmod{pq}$. Furthermore, since $M \in Z_{pq}$ and $pq < N$, certainly one of the roots is a solution for $C \equiv M^2 \pmod N$.

We now proceed to prove uniqueness. We re-write the congruence relation for the equation $C \equiv M^2 \pmod N$ as $C = M^2 - Nk$ with $k \in Z$. Suppose there are two solutions M_1 and M_2 of the equation $C = M^2 - Nk$ with $k \in Z$, $M_1 \neq M_2$ and for $i = 1, 2$ and $M_i < 2^{2n-1}$. Then, $M_1^2 - Nk_1 = M_2^2 - Nk_2$. Using $N = p^2q$, this leads to $M_1^2 - M_2^2 = (k_1 - k_2)N$.

Case 1: $(k_1 - k_2)|(M_1^2 - M_2^2)$. The probability that $(k_1 - k_2)|(M_1^2 - M_2^2)$ and not equal to zero is 2^{-n}. Conversely, the probability that $(k_1 - k_2)|(M_1^2 - M_2^2)$ and equal to zero is $1 - \frac{1}{2^n}$. Thus, $M_1^2 = M_2^2$ is with probability $1 - \frac{1}{2^n}$ and since $M \in Z_{pq}$, then $M_1 = M_2$. Hence, the equation $C = M^2 - Nk$ has only one solution.

Case 2: $N|(M_1 + M_2)(M_1 - M_2)$. The conditions that should be satisfied is either one of the following.

$$\begin{cases} pq|(M_1 \pm M_2) \\ p|(M_1 \mp M_2 \end{cases} \text{or} \begin{cases} p^2|(M_1 \pm M_2) \\ q|(M_1 \mp M_2 \end{cases}$$

Observe that pq, $p^2 > 2^{2n}$ while $|M_1 \pm M_2| < 2 \cdot 2^{2n-1} = 2^{2n}$. This implies that either condition is not possible. Hence, the equation $C = M^2 - Nk$ has only one solution. ■

Example 3.1. *Suppose we have two communicating parties, namely Bob as the sender of a message and Alice as its corresponding receiver. Let the security parameter $n = 16$.*

Key generation: *Alice generate two distinct primes $p = 52163$ and $q = 52183$.*

1. *Compute $N = p^2q = 141988824666127$.*
2. *Alice keeps her private key p and q.*
3. *Alice publishes her public key N.*

Encryption: *Bob receives Alice's public key. He would like to send a message* $M = 1323567403$.

1. *Compute* $C \equiv M^2 \pmod N = 114540378155610$.
2. *Bob sends* C *to Alice as his ciphertext.*

Decryption: *Alice receives a ciphertext* $C = 114540378155610$ *from Bob. To decrypt* C*, Alice then executes:*

1. *Compute* $m_p \equiv C^{\frac{p+1}{4}} \pmod p = 16559$.
2. *Compute* $m_q \equiv C^{\frac{q+1}{4}} \pmod q = 2209$.
3. *Compute two integers* r *and* s *such that* $rp + sq = 1$ *where* $r = 18264$ *and* $s = -18257$.
4. *Compute* $M_1 \equiv rpm_q + sqm_p \pmod{pq} = 1398454426$.
5. *Compute* $M_2 \equiv rpm_q - sqm_p \pmod{pq} = 2128651145$.
6. *Compute* $M_3 \equiv -M_2 \pmod{pq} = 593370684$.
7. *Compute* $M_4 \equiv -M_1 \pmod{pq} = 1323567403$.
8. *Compute* $W_i = \frac{C - M_i^2}{N}$ *where* $W_1 = -\frac{718421954}{52163}$, $W_2 = -\frac{1664586635}{52163}$, $W_3 = -\frac{129306174}{52163}$ *and* $W_4 = -12337$.
9. *Since* W_4 *is a integer, then return the plaintext* $M = M_4$.

Example 3.2. *Suppose we have two communicating parties, namely Bob as the sender of a message and Alice as its corresponding receiver. Let the security parameter* $n = 16$.

Key generation: *Alice generate two distinct primes* $p = 47087$ *and* $q = 47111$.

1. *Compute* $N = p^2q = 104453829341159$.
2. *Alice keeps her private key* p *and* q.
3. *Alice publishes her public key* N.

Encryption: *Bob receives Alice's public key. He would like to send a message* $M = 949333985 < 2^{2n-2}$ *where* $2^{2n-2} = 1073741824$.

1. *Compute* $C \equiv M^2 \pmod{N} = 7375520460373$.
2. *Bob sends* C *to Alice as his ciphertext.*

Decryption: *Alice receives a ciphertext* $C = 7375520460373$ *from Bob. To decrypt* C*, Alice then executes:*

1. *Compute* $m_p \equiv C^{\frac{p+1}{4}} \pmod{p} = 34109$.
2. *Compute* $m_q \equiv C^{\frac{q+1}{4}} \pmod{q} = 46887$.
3. *Compute two integers* r *and* s *such that* $rp + sq = 1$ *where* $r = -1963$ *and* $s = 1962$.
4. *Compute* $M_1 \equiv rpm_q + sqm_p \pmod{pq} = 1268981672$. *Ignore because* $M_1 > 1073741824$.
5. *Compute* $M_2 \equiv rpm_q - sqm_p \pmod{pq} = 210774390$.
6. *Compute* $M_3 \equiv -M_2 \pmod{pq} = 2007541267$. *Ignore because* $M_3 > 1073741824$.
7. *Compute* $M_4 \equiv -M_1 \pmod{pq} = 949333985$.
8. *Compute* $W_i = \frac{C - M_i^2}{N}$ *where* $W_2 = -\frac{20023511}{47087}$ *and* $W_4 = -8628$.
9. *Since* W_4 *is a integer, then return the plaintext* $M = M_4$.

4. Conclusion

Through the presentation of this work, we have proposed two efficient methods to overcome the Rabin cryptosystem decryption failure. In the proposed methods, we managed to not using the Jacobi symbol, message redundancy technique or sending extra information in order to specify the correct plaintext. Also, in the proposed methods we managed to maintain the use of integer factorization problem as a source of security. In addition, the proposed methods producing a unique decryption result without decryption failure are not like the methods proposed previously. In concluding, we have overcome decryption failure of the Rabin cryptosystem in the most effective manner as opposed to existing methods.

Acknowledgement

The authors would like to thanks the Institute for Mathematical Research, Universiti Putra Malaysia for research funding.

References

Boneh, D. (2001). Simplified oaep for the rsa and rabin functions. In *In Advances in Cryptology-Crypto 2001*, pages 275–291. Springer.

Kurosawa, K., Ito, T., and Takeuchi, M. (1991). Public key cryptosystem using a reciprocal number with the same intractability as factoring a large number. *Cryptologia*, 12(4):225–233.

Lenstra, A. and Verheul, E. R. (2001). Selecting ccryptographic key sizes. *Journal of Cryptology*, 14(4):255–293.

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

Nishioka, M., Satoh, H., and Sakurai, K. (2002). Design and analysis of fast provably secure public-key cryptosystems based on a modular squaring. In *In Information Security and Cryptology-ICISC 2001*, pages 81–102. Springer.

Rabin, M. O. (1979). Digitalized signatures and public-key functions as intractable as factorization. Technical report.

Takagi, T. (1997). Fast rsa-type cryptosystems using n-adic expansion. In *In Advances in Cryptology-Crypto97*, pages 372–384. Springer.

Williams, H. (1991). A modification of the rsa public-key encryption procedure. *IEEE Transactions On Information Theory*, 26(6):726–729.