International Journal of Cryptology Research 5(1): 11-20 (2015)

Rabin-RZ: A New Efficient Method to Overcome Rabin Cryptosystem Decryption Failure Problem

[1]Zahari Mahad and [2]Muhammad Rezal Kamel Ariffin
[1,2]Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Research, Universiti Putra Malaysia
[2]Department of Mathematic, Faculty of Science, Universiti Putra Malaysia
Email: [1]zaharimahad@upm.edu.my, [2]rezal@upm.edu.my

ABSTRACT

We propose a new efficient method to overcome the 4 to 1 decryption failure for the Rabin cryptosystem by reducing the phase space of plaintext from $M \in \mathbb{Z}_{pq}$to $M \in 2^{2n-2}, 2^{2n-1} \subset \mathbb{Z}_{pq}$, where pq is a product of 2 strong primes and $pq \in 2^{2n}, 2^{2n+2}$. Instead of utilizing the pubic modulus $N = pq$, we use $N = p^2q$. Upon decrypting by using the private modulus $d = pq$ via the Chinese Remainder Theorem, we prove that there exists only one plaintext from the 4 roots obtained that will reside within the interval $2^{2n}, 2^{2n+2}$. As a result, the decryption failure is overcome and this technique also enhances the decryption process for the Rabin cryptosystem. Furthermore, we make analytical comparison with other methods designed in previous literature to overcome the Rabin cryptosystem problem.

1. INTRODUCTION

The Rabin cryptosystem which was introduced in 1979 was designed with its cryptographic primitive being the integer factorization problem (IFP) of 2 strong primes. In comparison with the RSA cryptosystem, Rabin's cryptosystem utilizes the public exponent value $e = 2$. Hence, it is implied by the designers to be an optimal/efficient implementation of the RSA cryptosystem (Rabin, 1979). However, the decryption of the Rabin scheme produces four possible distinct outcomes (plaintext). Consequently additional information is required to determine the correct plaintext (Elia *et al.*, 2011). Furthermore, the Rabin cryptosystem has an established security proof that is complete. It can be observed via the following well established propositions.

Proposition 1. *Let $M \in \mathbb{Z}_{pq}$ and $C \equiv M^2 \pmod{pq}$. If the modulus $N = pq$ can be factored, then the square root of C can be obtained and if the square root of C can be obtained then the modulus $N = pq$ can be factored.*

It is well established in the literature that when decrypting the Rabin ciphertext, the receiver of the ciphertext comes upon 4 possible plaintexts.

This scenario is due to the process of solving the square root problem by the Chinese Remainder Theorem (CRT).

Since 1979, much effort has been put into research to find an efficient method to solve the 4 to 1 decryption failure. It is easy to see that if a polynomial time solution is found, then the Rabin cryptosystem has potential to be utilized due to its short public exponent. For example such as Williams technique (Williams, 1980), adding some redundancies in the plaintext (Menezes *et al.*, 1997) or incorporating the Jacobi and the Legendre symbol as extra information (Kurosawa *et al.*, 2001).

In 2013, Ariffin *et al.* designed an asymmetric scheme based on the IFP together with the square root scenario and is analytically proven to have 1 to 1 decryption (Ariffin *et al.*, 2013). Based on work by Ariffin *et al.*, we managed to redesign the Rabin cryptosystem to be more efficient to use. Instead of focusing on the IFP for $N = pq$, we utilized the IFP within $N = p^2q$ as was established earlier within the Okamoto-Uchiyama's scheme in 1998 (Okamoto and Uchiyama, 1998) and Schmidt-Samoa' system in 2006 (Schmidt-Samoa, 2006).

Our paper is structured as following manner. In Section 2, we reproduce the Rabin cryptosystem and discuss in brief the 4 to 1 decryption scenario. We also describe 3 existing strategies to overcome the 4 to 1 decryption failure. In Section 3, we produce our strategy such that Rabin's cryptosystem has an analytically proven unique decryption. In Section 4, a comparison between our new strategies against all existing 3 strategies is presented. We conclude in Section 5.

2. RABIN CRYPTOSYSTEM

The following is an overview of Rabin's cryptosystem (Rabin, 1979).

Key Generation

INPUT: The size n-bit of the prime numbers.
OUTPUT: A public key $N = pq$.

1. Generate two random and distinct n-bit strong primes p and q satisfying
$$p \equiv 3 \mod 4 \ , 2^n < p < 2^{n+1}$$
$$q \equiv 3 \mod 4 \ , 2^n < q < 2^{n+1}$$
2. Set $N = pq$.

Encryption

INPUT: The public key $N = pq$ and the plaintext M.
OUTPUT: The ciphertext C.

1. Plaintext is an integer $M \in \mathbb{Z}_{pq}$.
2. Compute $C \equiv M^2 \pmod{N}$.

Decryption

INPUT: The private key pair (p, q) and the ciphertext C.
OUTPUT: The plaintext M.

1. Solve square root of C via CRT utilizing the private key pair (p, q).
2. Return 4 possible plaintexts M_1, M_2, M_3 and M_4.

Remark 1. The Rabin cryptosystem is known to have decryption failure due to its 4 to 1 mapping. The following is a list of strategies to overcome this feature of the Rabin cryptosystem.

1. **William's technique** (Williams, 1980). The encryption process requires the encrypter to compute a Jacobi symbol. Hence, losing the performance advantage of Rabin over RSA (as in point no. 3).
2. **Redundancy in the message** (Menezes *et al.*, 1996). This scheme has a probability decryption failure of approximately $\frac{1}{2^{k-1}}$ where k is the least significant binary string of the message.
3. **Extra bits** (Kurosawa *et al.*, 2001). One will send 2 extra bits of information to specify the square root. The encryption process requires the computation of the Jacobi symbol. This results in a computational overhead which is much more than just computing a single square modulo N.

3. RABIN-RZ: THE MODIFIED RABIN CRYPTOSYSTEM

We begin by describing our modified version of Rabin's cryptosystem, Rabin-RZ.

Key Generation

INPUT: The size n-bit of the prime numbers.

OUTPUT: A public key $N = p^2q$ and private key $d = pq$.

1. Generate two random and distinct n-bit strong primes p and q satisfying
$$p \equiv 3 \mod 4 \ , 2^n < p < 2^{n+1}$$
$$q \equiv 3 \mod 4 \ , 2^n < q < 2^{n+1}$$
2. Set $= p^2q$.
3. Set $d = pq$.

Encryption

INPUT: The public key $N = p^2q$ and the plaintext M.
OUTPUT: The ciphertext C.

1. Plaintext is an integer $M \in \ 2^{2n-2}, 2^{2n-1} \ \subset \mathbb{Z}_{pq}$.
2. Compute $C \equiv M^2 \pmod N$.

Decryption

INPUT: The private key tuple (d, p, q) and the ciphertext C.
OUTPUT: The plaintext M.

1. Compute $V \equiv C \pmod d$.
2. Solve square root of V via CRT utilizing the private key pair (p, q).
3. Return 4 possible plaintexts M_1, M_2, M_3 and M_4.
4. For $i = 1$ to 4 compute $W_i = \frac{C - {M_i}^2}{N}$.
5. Return the plaintext M_i which produces $W_i \in \mathbb{Z}$.

We now provide the proof of correctness. We begin with the following lemma.

Lemma 1. *Let $N = p^2q$ and $d = pq$. Choose $x \in \mathbb{Z}_d$. If $y \equiv x^2 \ (mod\ N)$ and $V \equiv y \ (mod\ d)$, then $V \equiv x^2 \ (mod\ d)$.*

Proof. We have
$$y = x^2 + Nk_1 \text{ where } k_1 \in \mathbb{Z} \tag{1}$$
and
$$v = y + dk_2 \text{ where } k_2 \in \mathbb{Z} \tag{2}$$

From (1) and (2) we have

$$v = x^2 + Nk_1 + dk_2$$

Finally,

$$v \equiv x^2 \mod d \quad \blacksquare$$

Proposition 2. *Let C be an integer representing a ciphertext encrypted by the Rabin-RZ scheme. 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 $M \in \mathbb{Z}_d$, by solving $V \equiv C \pmod d$ using the CRT we will obtain all 4 roots of V. Also by Lemma 1, indeed $V \equiv M^2 \pmod d$. Furthermore, since $M \in \mathbb{Z}_d$ and $d < N$, 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 as the equation $C \equiv M^2 \pmod N$ as $C = M^2 - Nt$ with $t \in \mathbb{Z}$. Suppose there are two solutions M_1 and M_2 of the equation $C = M^2 - Nt$ with $t \in \mathbb{Z}$, $M_1 \neq M_2$ and for $i = 1, 2$, $M_i < 2^{2n-1}$. Then, ${M_1}^2 - Nt_1 = {M_2}^2 - Nt_2$. Using $N = p^2q$, this leads to

$${M_1}^2 - {M_2}^2 = |t_1 - t_2|\, N.$$

Case 1

$|t_1 - t_2|\,|({M_1}^2 - {M_2}^2)$. The probability that $|t_1 - t_2|\,|({M_1}^2 - {M_2}^2)$ and not equal to zero is 2^{-n}. Conversely, the probability that $|t_1 - t_2|\,|({M_1}^2 - {M_2}^2)$ 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 $M \in [2^{2n-2}, 2^{2n-1}]$, then $M_1 = M_2$. Hence, the equation $C = M^2 - Nt$ 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

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

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. $\blacksquare$

Example

The scenario is A (Along) will send his public key to B (Busu) and Busu will encrypt to Along. Along will choose the primes $p = 100669$, $q = 69859$ and compute $N = 707968400363899$ and $d = 7032635671$. Let says Busu want to sends a message $M = 1439948310$ to Along. Busu will compute

$$519659206359828 \equiv 1439948310^2 \pmod{707968400363899}$$

and sends to Along. To decrypt, Along computes

$$3691358296 \equiv 519659206359828 \mod 7032635671$$

Then, Along uses the CRT and his private keys to compute the four square roots of 3691358296 modulo d, which are

1. $M_1 = 3890433108,$
2. $M_2 = 1439948310,$
3. $M_3 = 5592687361,$
4. $M_4 = 3142202563.$

Then, to determine the correct message Along computes for $i = 1$ to 4:

$$W_i = \frac{C - {M_i}^2}{N}$$

In this example, only M_2 produces $W \in \mathbb{Z}$.

4. COMPARATIVE ANALYSIS BETWEEN RABIN CRYPTOSYSTEM AND ITS IMPROVEMENTS

In this section, we provide comparison via the complexity order of each Rabin improvement with the fundamental Rabin cryptosystem as was disclosed in 1979. We also provide the advantage and disadvantage of each Rabin improvement.

Algorithm	Encryption Speed	Decryption Speed
New Rabin-RZ	$O(4n^2 + 3n)$	$O(2n^3 + 12n^2 + 4n)$
Menezes *et al.*	$O(8n^2 + 3n)$	$O(2n^3 + 16n^2)$
Kurosawa *et al.*	$O(5n^2 + n)$	$O(2n^3 + 4n^2 + 2n)$
Williams	$O(5n^2 + 5n)$	$O(n^3 + n^2 + 9n)$
Rabin (1979)	$O(5n^2 + 2n)$	$O(2n^3 + 12n^2 + 4n)$

Table 1: Complexity time between improvements of Rabin cryptosystems

It is obvious that from Table 1, those improvements of Rabin (1979) – that is with no decryption failure is in the following list in descending effectiveness.

1. New Rabin-RZ
2. Kurosawa
3. Williams

Observe we did not include the method by Menezes in the list because of a possible decryption failure. In Table 2, we also provide comparison advantage and disadvantage between improvements of Rabin cryptosystem.

	Menezes Technique	**Kurosawa Technique**	**Williams Technique**	**Rabin-RZ Technique**
Advantage	Overcome Rabin decryption failure with probability $\frac{1}{2^{l-1}}$ where l is number of bits use as redundancy message.	Decryption never fails.	Decryption never fails. Decryption speed is faster than other methods.	Decryption never fails. No extra computation needed during decryption. Domain for plaintext restricted. Instead for any $M \in \mathbb{Z}_{pq}$, we restrict to the interval

				$2^{2n-2} \leq M \leq 2^{2n-1}$. Encryption speed is faster than other methods. <u>Note:</u> Even though the message domain is restricted to the above-mentioned interval, the interval still contains exponentially many message candidates.
Disadvantage	Probability decryption failure of approximately $\frac{1}{2^{l-1}}$.	Slow in term of performance because of the encryption process requires the computational of the Jacobi symbol, this results in a computational overhead, which is much more than just computing a	Slow in term of performance because of the encryption process requires the computational of the Jacobi symbol, this results in a computational overhead, which is much more than just computing a	Domain for plaintext is restricted to the interval $2^{2n-2} \leq M \leq 2^{2n-1}$.

		single square modulo N.	single square modulo N.	

Table 2: Comparison advantage and disadvantage between enhancement methods of Rabin cryptosystem

5. CONCLUSION

Through the presentation of this work, we have provided an efficient mechanism to utilize the IFP couple with the square root problem which initially had difficulties to be executed under the circumstances of a 4 to 1 decryption scenario like Rabin cryptosystem.

Extending the results through complexity order analysis, it could be seen that with an encryption and decryption speed of $O(n^2)$ for encryption and $O(n^3)$ for decryption, the Rabin-RZ is able to provide an ideal platform for application that rely on fast encryption and decryption masses. In concluding, we have overcome decryption failure of the Rabin cryptosystem in the most effective manner as opposed to existing methods.

REFERENCES

Rabin, M. O. 1979. Digitalized Signatures and Public-Key Functions as Intractable as Factorization. *Tech. Report MIT/LCS/TR-212, MIT Laboratory for Computer Science*.

Menezes, R. L., van Oorschot, P. C. and Vanstone, S. A. 1996. *Handbook of Applied Cryptography.* CRC Press.

Kurosawa, K., Ogata, W., Matsuo, T. and Makishima, S. 2001. IND-CCA Public Key Schemes Equivalent to Factoring $N = pq$. *Public Key Cryptography 2001*: 36-47.

Williams, H. C. 1980. A Modification of the RSA Public Key Encryption Procedure. *IEEE Trans. Inf. Theory.* 26(6): 726-729.

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 Mathematical Sciences.* 7(S): 19-37.

Okamoto, T. and Uchiyama, S. 1998. A New Public-Key Cryptosystem as Secure as Factoring. *EUROCRYPT-98, Lecture Notes in Computer Science*. 1430: 308-318.

Schmidt-Samoa, K. 2006. A New Rabin-type Trapdoor Permutation Equivalent to factoring. *Electronic Notes in Theoretical Computer Science (ENTCS).* 157(3): 79-94.

Elia, M., Piva, M. and Schipani, D. 2011. *The Rabin Cryptosystem revisited*. Accessed 19th February 2014. Sourced from *www.arxiv.org*