International Journal of Cryptology Research 8(1): 1 - 16 (2018)

A Fast and Efficient Design for AA_β Cryptosystem

Muhammad Asyraf Asbullah *1, **Muhammad Rezal Kamel Ariffin**1,2, and **Zahari Mahad**2

1*Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Research (INSPEM), 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

This paper presents an upgrade of the AA_β cryptosystem of any forms preceding this work. The principal idea in this work is to utilize the Rabin-p decryption strategy upon the original AA_β design. As a result, this approach leads to a fast and efficient decryption procedure for the AA_β cryptosystem, along with economical key parameters due to its significantly smaller size. Next, we demonstrate that breaking the AA_β function (cryptosystem) is reducible to breaking the Rabin-p cryptosystem, and partially the other way around. Finally, we present another AA_β-variant with the public key $A_2 = pqr$.

Keywords: AA_β Cryptosystem, Rabin-p Cryptosystem, Internet of Things, integer factorization problem, embedded system

1 INTRODUCTION

The AA_β cryptosystem is a public key cryptosystem that was designed at first in earlier 2012, targeted to visualize an asymmetric encryption that utilized the security instances by a so-called Bivariate Function Hard Problem (Mahad and Ariffin, 2012). The earlier design also ready to highlight an answer for the decryption failure state of affairs of Rabin encryption. A full-fledged version of the AA_β cryptosystem was introduced later in Ariffin et al. (2013). Since then, the AA_β cryptosystem received a substantial attention from interested researchers.

Asbullah and Ariffin (2014) suggested using the Garner's algorithm, which replaces the computation of Chinese Remaindering Theorem (CRT) during the AA_β decryption procedure. Consequently, the modification makes the decryption become very fast and reduces the required computational process. A comparative analysis was also provided, against Rabin-Takagi (Takagi, 1998) and HIME(R) cryptosystem (Nishioka et al., 2002). Asbullah and Ariffin (2015) come up with a provably secure design of AA_β cryptosystem in order to achieve a security level of indistinguishability against chosen cipher attack.

Adnan et al. (2016a) present a practical implementation of the AA_β as a lightweight asymmetric encryption scheme on an embedded system device. On the other hand, Adnan et al. (2016b) focused on a timing analysis of the AA_β encryption on embedded Linux for the Internet of Things (IoT). Meanwhile, Adnan et al. (2017) provides a result for energy analysis of the AA_β cryptosystem. Their results absolutely indicate that a prospect for the AA_β cryptosystem is implemented for a lightweight public key encryption on an embedded device, therefore appropriate additionally for IoT.

A number of cryptanalyses were conducted upon the AA_β cryptosystem. For instance, we will survey many results on algebraic cryptanalysis and conjointly side-channel cryptanalysis upon the same cryptosystem. The work in Ghafar and Ariffin (2014) shows that the AA_β cryptosystem is at risk of a timing attack (i.e. a class of side channel attack). Fortuitously, their result solely discusses within the theoretical sense of timing attack with the assumption that the attacker ready to collect some leaked values of a particular parameter throughout the decryption process. Moreover, Asbullah and Ariffin (2016a) shows that there exist inappropriate keys selection that can be manipulated to break the cryptosystem (as analogous as to their prior work in Asbullah and Ariffin (2016b)). These observations due to the algebraic nature implicitly reside within the public and private keys. Hence, they recommend that the parameters chosen during key generation for AA_β cryptosystem must be scrutinized and selected wisely before implementation. Later on, Ghafar and Ariffin (2016) designed a straightforward power analysis and show that the secret keys of the AA_β cryptosystem can be retrieved by using such a method. We tend to highlight that of all the above cryptanalytical results nevertheless are removed from practical to breaks the cryptosystem, yet the results so useful as security measures of the AA_β cryptosystem.

In this work, we proposed a design that enhances the AA_β cryptosystem (of any version prior to this work). Our methodology is to adjust the key generation algorithm and incorporate the Rabin-p decryption techniques upon the AA_β decryption procedure. The reason (rationale) by doing so is that our enhanced AA_β cryptosystem will be as efficient as the Rabin-p cryptosystem. Furthermore, we provide the computational reducibility to Rabin-p cryptosystem, and vice versa (partially), in addition to the ones that explained in the original work of Ariffin et al. (2013).

This paper has been divided into five sections, begins with a brief overview of the AA_β cryptosystem in Section 1. Section 2 laying out the background and important materials for this research. Section 3 describes the design of our enhanced AA_β cryptosystem. In Section 4, we explain the design rationale for the enhanced version. In addition, we put forward the relation between our proposed cryptosystem with the security of the Rabin-p cryptosystem. Finally, we present another AA_β-variant with the public key $A_2 = pqr$. Section 5 concludes the work.

2 PRELIMINARIES

2.1 AA_β Function

First of all, we will review the AA_β function which is proposed earlier by Ariffin et al. (2013). Consider the following definition.

Definition 2.1. *(Ariffin et al., 2013). Suppose* p, q *be two distinct primes satisfies* $3 \pmod 4$ *where* $2^k < p, q < 2^{k+1}$*. Let* $A_1 \in \mathbb{Z}^+_{(2^{3k+4}, 2^{3k+6})}$ *and* $A_2 = p^2 q$ *such that* $\gcd(A_1, A_2) = 1$*. Suppose* $m^2 \in \mathbb{Z}^+_{(2^{2k-2}, 2^{2k-1})}$ *and* $t \in \mathbb{Z}^+_{(2^{4k}, 2^{4k+1})}$*. Then we define the following equation (1) as the* AA_β *function.*

$$c = A_1 m^2 + A_2 t \tag{1}$$

Note that the integers (A_1, A_2) *are known parameters and* (m, t) *be unknown integers to be solved.*

Theorem 2.1. *(Ariffin et al., 2013). Let* $c = A_1 m^2 + A_2 t$ *be* AA_β *function, then it has a unique solution for* m *and* t*, respectively.*

The above theorem show that the AA_β function once solved will have a unique integers m and t, respectively.

2.2 The AA_β Cryptosystem

The details of the original design of the AA_β cryptosystem is given here, following the description in Ariffin et al. (2013). However, we only give a simplified version of the AA_β decryption algorithm due to Asbullah and Ariffin (2014). We now describe the key generation, encryption and decryption procedure of the original AA_β cryptosystem as follows.

Algorithm 2.1 Key Generation

1. Generate two primes $2^k < p, q < 2^{k+1}$ such that $p, q \equiv 3 \pmod 4$
2. Set $A_2 = p^2 q$
3. Randomly select $A_1 \in \{(2^{3k+4}, 2^{3k+6})\}$ where $\gcd(A_1, A_2) = 1$
4. Compute the integer d' satisfying $A_1 d' \equiv 1 \pmod{pq}$
5. Output a tuple (A_1, A_2) as the public key and a tuple (d', p, q) as the private key.

Algorithm 2.2 Algorithm for Encryption

1. Generate a plaintext $m \in \{(2^{2k-2}, 2^{2k-1})\}$
2. Generate a plaintext $t \in \{(2^{4k}, 2^{4k+1})\}$
3. Set the ciphertext $c = A_1 m^2 + A_2 t$

Remark 2.1. *Assume the AA_β decryption algorithm as depicted in Ariffin et al. (2013) the utilization of the Chinese Remaindering Theorem (CRT) is needed to solve simultaneous congruence equations. Be that as it may, there exists an alternative method, which is faster and more efficient method known as the Garner's algorithm (Asbullah and Ariffin, 2014). Consequently, we remark that the AA_β decryption algorithm used in this section taken from Asbullah and Ariffin (2014) since it is more effective than its prior original version as follows.*

Algorithm 2.3 Algorithm for Decryption

```
1. Determine $w \equiv cd' \pmod{pq}$
2. Compute $m_p \equiv w^{\frac{p+1}{4}} \pmod{p}$
3. Compute $m_q \equiv w^{\frac{q+1}{4}} \pmod{q}$
4. Compute $j \equiv p^{-1} \pmod{q}$
5. Calculate $h_1 \equiv (m_q - m_p)j \pmod{q}$
6. Calculate $h_2 \equiv (-m_q - m_p)j \pmod{q}$
7. Calculate $m_1 = m_p + h_1 p$
8. Calculate $m_2 = m_p + h_2 p$
9. Calculate $m_3 = pq - m_2$
10. Calculate $m_4 = pq - m_1$
11. For $m_i < 2^{2k-1}$, determine $t_i = \frac{c - A_1 m_i^2}{A_2}$ where $i = 1, 2, 3, 4$
12. Sort the pair $(m_i, t_i)$ for integer $t_i$, else reject
13. Output the plaintext tuple $(m, t)$
```

2.3 Useful Lemmas

In this section we provides two important lemmas that will be useful later for our work in this paper.

Lemma 2.1. *(Asbullah and Ariffin, 2016c). Let* $p \equiv 3 \pmod{4}$ *be a prime number. Let* $c \equiv m^2 \pmod{p^2}$ *where* m *is an unknown integer such that* $m < p^2$ *and* $\gcd(m, p) = 1$. *Then a solution to* $c \equiv m^2 \pmod{p^2}$ *can be determine by* $m_1 = m_p + jp$ *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* $m_2 = p^2 - m_1$ *is the another solution.*

Lemma 2.2. *(Asbullah and Ariffin, 2016c). Let m_1 and m_2 be the two solutions from Lemma 2.1. Then one of the two solutions less than $\frac{p^2}{2}$.*

3 AA_β CRYPTOSYSTEM: ENHANCED VERSION

This section is dedicated to describe the new design for enhanced version of the AA_β-cryptosystem. Then, we provide the proof of correctness.

3.1 The Proposed Cryptosystem

Algorithm 3.1 Key Generation of The Proposed Cryptosystem

```
1. Generate primes $2^k < p, q < 2^{k+1}$ where $p, q \equiv 3 \pmod 4$
2. Set $A_2 = p^2 q$
3. Generate random integer $A_1 \in \{(2^{3k+4}, 2^{3k+6})\}$ satisfying $\gcd(A_1, A_2) = 1$
4. Compute $d$ such that $A_1 d \equiv 1 \pmod{p^2}$
5. Output a tuple $(A_1, A_2)$ as the public key and a tuple $(d, p)$ as the private key.
```

Remark 3.1. *Note that the following encryption algorithm (Algorithm 3.2) is identical to the original encryption algorithm (Algorithm 2.2).*

Algorithm 3.2 Encryption Algorithm of The Proposed Cryptosystem

```
1. Generate a plaintext $m \in \{(2^{2k-2}, 2^{2k-1})\}$
2. Generate a plaintext $t \in \{(2^{4k}, 2^{4k+1})\}$
3. Set the ciphertext $c = A_1 m^2 + A_2 t$
```

Algorithm 3.3 Decryption Algorithm for The Proposed Cryptosystem

```
1. Set $w \equiv dc \pmod{p^2}$
2. Determine $m_p \equiv w^{\frac{p+1}{4}} \pmod{p}$
3. Determine $i = \frac{w - {m_p}^2}{p}$
4. Determine $j \equiv \frac{i}{2m_p} \pmod{p}$
5. Set $m_1 = m_p + jp$
6. Output $m = m_1$ if $m_1 < 2^{2k-1}$. Else output $m = p^2 - m_1$
7. Compute $t = \frac{c - A_1 m^2}{A_2}$
8. Output the plaintext tuple $(m, t)$
```

3.2 Proof of Correctness

Theorem 3.1. *Let $c = A_1 m^2 + A_2 t$ be the ciphertext output by Algorithm 3.2. Then such ciphertext will correctly decrypted by the Algorithm 3.3 and retrived the plaintext tuple (m, t).*

Proof. Suppose c be the ciphertext with parameters dictated in the Algorithm 3.2. The ciphertext c then can be decrypted efficiently as follows. Since d such that $dA_1 \equiv 1 \pmod{p^2}$, we proceed to determine w as follows.

$$w \equiv dc \equiv d(A_1 m^2 + A_2 t) \equiv dA_1 m^2 \equiv m^2 \pmod{p^2} \tag{2}$$

Then, by using Lemma 2.1, the equation (2) efficiently solved, which produces two distinct solution m_1 and m_2. From Lemma 2.2, only one of m_1 and m_2 satisfies an integer less than $\frac{p^2}{2}$. Since we have $m < 2^{2k-1} < \frac{p^2}{2}$, thus we get the unique m. We further to compute $t = \frac{c - A_1 m^2}{A_2}$. Hence, analytically the ciphertext c correctly decrypted by the Algorithm 3.3 and output the unique solution of the tuple (m, t). ■

3.3 A Toy Example

Suppose we have two communicating parties, namely Bob as the sender of a message and Alice as its corresponding receiver. Let the security parameter $k = 31$.

Key generation:
Alice generate two distinct primes $p = 2300864171, q = 3699229571$.

1. Choose $A_1 = 571387513048875070687101686822$
2. Compute $d \equiv {A_1}^{-1} \pmod{p^2} = 4439689156782303504$
3. Alice publish her public key's A_1, A_2

Encryption:
Bob receive Alice's public key. He would like to send a message $m = 1470703929037549618$ and $t = 182851268416957848864398027264367694 85$.

1. Compute $c = A_1 m^2 + A_2 t = 159398327689964192613291765110823977233 5$ $5034294738731988152 04073863$
2. Bob send c to Alice as his ciphertext.

Decryption:
Alice receives a ciphertext $c = 609516451157084983009264189549286$ from Bob. To decrypt c, Alice then

1. Compute $w \equiv cd \pmod{p^2} = 1171061998070371913$
2. Compute $m_p \equiv c^{\frac{p+1}{4}} \pmod{p} = 2008449701$
3. Compute $i = \frac{w - m_p^2}{p} = -1244231728$
4. Compute $j \equiv \frac{i}{2m_p} \pmod{p} = 639196327$
5. Compute $m_1 = m_p + jp = 1470703929037549618$
6. Since $m_1 < 2^{2k-1}$, set $m = m_1$
7. Compute $t = \frac{c - A_1 m^2}{A_2} = 18285126841695784886439802726436769485.$
8. Return the plaintext m and t

4 DISCUSSIONS

4.1 Enhancement from the Original Version

Table 1 illustrates the comparison between the original AA_β (Ariffin et al., 2013), the fast variant AA_β (Asbullah and Ariffin, 2014) and the proposed enhanced variant.

	Original AA_β	Fast AA_β	Enhanced Version
Public keys	$\lvert A_1\rvert, \lvert A_2\rvert = 3k$	$\lvert A_1\rvert, \lvert A_2\rvert = 3k$	$\lvert A_1\rvert, \lvert A_2\rvert = 3k$
Private keys	$\lvert d'\rvert = 2k, \lvert p\rvert, \lvert q\rvert = k$	$\lvert d'\rvert = 2k, \lvert p\rvert, \lvert q\rvert = k$	$\lvert d\rvert = 2k, \lvert p\rvert = k$
Mod Exponent	2	2	1
Mod Inverse	2	1	1
Mod Reduction	5	3	2
Division	4	4	2
Novak's attack	Yes	Yes	No

Table 1: Comparison between three versions of AA_β Cryptosystem in consideration.

1. Note that the improved version solely use d, p as the private keys throughout key generation method whereas within the original version, additionally to the private keys d', p is another large prime q. That means that smaller key size thus ends up for less storage and quicker computational operations. Furthermore, this step emphasizes that we tend to solely need to find q for creating the public key $A_2 = p^2 q$, then the large prime q may be discarded later on.

2. Our proposed decryption method in this work takes advantage from the efficiency of the Rabin-p decryption algorithm, that solely needed one prime p coupled with a private integer d rather than two primes p, q as within the original version, with additional private key d'. Such necessities would have an effect on the general operations in term of computational advantages. For example, as shown in Table 1, the modular operations that iare required for the proposed upgraded version are minimal as compared to the first version and the another variant in consideration.

3. Furthermore, the decryption process in our proposed work takes advantage from the security feature provided within the Rabin-p cryptosystem in term of resistant against the Novak's attack; since the upgraded version of the proposed algorithm (i.e.Algorithm 3.3) does not execute the computation of the CRT or the Garner's algorithm. Therefore, we have a tendency to claimed that the upgraded version provides a further security feature. Refer to (Asbullah and Ariffin, 2016c) for details.

4.2 Computational Reducibility

In the original version, Ariffin et al. (2013) show that for any efficient algorithm able to factor the modulus $A_2 = p^2q$, then such algorithm also able to solve the AA_β function. Furthermore, they also prove that the AA_β function can be solved if there exists algorithm that can solve the Bivariate Function Hard Problem (BFHP). This section will provide another cases regarding breaking the AA_β function (cryptosystem) with respect to the computational reducibility as follows.

Theorem 4.1. *Breaking the AA_β function (cryptosystem) is reducible to solving the Rabin-p cryptosystem.*

Proof. Suppose we are given a problem satisfies Definition 2.1, i.e. the AA_β function. Notice that there exists an integer x such that $A_1x \equiv 1 \pmod{A_2}$. Thus, we can compute $w' \equiv cx \equiv m^2 \pmod{A_2}$. Suppose there exists an algorithm able to solve the Rabin-p cryptosystem, then the same algorithm eventually able to solve $w' \equiv m^2 \pmod{A_2}$. Since the AA_β function (cryptosystem) has a unique solution for the integer m, hence we proceed to obtained the unique integer t such that $t = \frac{c-A_1m^2}{A_2}$. ■

Theorem 4.2. *Solving the Rabin-p cryptosystem is partially reduce to breaking the AA_β function (cryptosystem) .*

Proof. Let $c \equiv m^2 \pmod{p^2q}$ be a ciphertext output by Rabin-p cryptoysystem. Suppose there exists an algorithm able to solve the AA_β function, therefore the same algorithm can be used to solve the Rabin-p cryptosystem whenever m satisfies $2^{2k-2} < m < 2^{2k-1}$. Since the integer m from the Rabin-p cryptosystem is taken from $m \in \{(0, 2^{2k-1})\}$, yet such algorithm only efficiently solve for the set of integers in the range $(2^{2k-2}, 2^{2k-1})$. ■

4.3 AA_β-variant with the public key $A_2 = pqr$

In this section, we might consider using the modulus $A_2 = pqr$ where p, q and r are three distinct large primes and incorporated within the AA_β cryptosystem. All the other parameters are the same as the proposed enhanced version (see Section 3). We show the conception of solving the solutions of the equation $w \equiv cd \pmod{pq}$ during decryption algorithm as follows.

Algorithm 4.1 AA_β Decryption with the public key $A_2 = pqr$

```
Input: A ciphertext $c$ and the private key $(d, p, q)$
Output: The plaintext $m, t$
Compute $w \equiv cd \pmod{pq}$
Compute $m_p \equiv w^{\frac{p+1}{4}} \pmod{p}$
Compute $m_q \equiv w^{\frac{q+1}{4}} \pmod{q}$
Compute $j \equiv p^{-1} \pmod{q}$
Compute $h_1 \equiv (m_q - m_p)j \pmod{q}$
Compute $h_2 \equiv (-m_q - m_p)j \pmod{q}$
Compute $m_1 = m_p + h_1 p$
Compute $m_2 = m_p + h_2 p$
Compute $m_3 = pq - m_2$
Compute $m_4 = pq - m_1$
Compute $t_i = \frac{c - A_1 m_i^2}{A_2}$ such that $m_i < 2^{2k-1}$ for $i = 1, 2, 3, 4$
Sort the pair $(m_i, t_i)$ for integer $t_i$, else reject
Return the plaintext $m, t$
```

4.3.1 Proof of Correctness for Algorithm 4.1

It is obvious that the decryption works and the uniqueness of the solution is preserved (see Theorem 4.3).

Theorem 4.3. *Let $c = A_1 m^2 + A_2 t$ be the AA_β ciphertext with $A_2 = pqr$ ciphertext. Then the Algorithm 4.1 will output the unique $m < 2^{2k-1}$.*

Proof. Suppose $c = A_1 m^2 + A_2 t$ be the ciphertext output by Algorithm 3.2 with parameters as described in its procedure except with $A_2 = pqr$.

From $c \equiv m^2 \pmod{pq}$, we have $c - m^2 \equiv 0 \pmod{pq}$. Thus, $pq \mid c - m^2$. Since $2^{2k-2} < m < 2^{2k-1}$, therefore it is sufficient just solving for

$c \equiv m^2 \pmod{pq}$ using Chinese Remainder Theorem or Garner's method of which give exactly four distinct solution m_1, m_2, m_3 and m_4 satisfies $c \equiv m^2 \pmod{pq}$. In addition, Theorem 2.1 analytically prove that such ciphertext c has unique solution for m and t. Therefore the Algorithm 4.1 will provide a 1-to-1 decryption. ■

4.3.2 Demerit of AA_β-variant with the public key $A_2 = pqr$

Observed that, the decryption performs by Algorithm 4.1 deemed as less efficient in comparison with Algorithm 3.3. The first reason is because we need to generate another distinct prime r for the public key $A_2 = pqr$, thus increase the cost of generating additional random prime numbers for every modulus generated.

Secondly, note that the decryption performs by Algorithm 4.1 need to solve the congruence $w \equiv c \pmod{pq}$. Therefore, this computational procedure involves the same operational cost as the decryption algorithm in the original Rabin cryptosystem. We recall that this operation execute two modular exponentiation of modulo p and of modulo q. It then further with recombination process using the Garner's algorithm. As stated in Theorem 4.3, the result of such procedure will produce four different integers compared to Algorithm 3.3 which only produces the unique solution m. Hence, it obviously increases the running time in this matter.

To make it worst, this AA_β-variant with the public key $A_2 = pqr$ involves Garner's algorithm of which susceptible to the Novak's attack thus can affect the security.

5 CONCLUSION

Taking everything into account, this paper introduces an upgrade of the AA_β cryptosystem of any forms preceding this work. The principal idea in this work utilizes the Rabin-p decryption strategy upon the original AA_β design. Thusly, this approach leads to a fast and efficient decryption procedure for the AA_β

cryptosystem, along with economical key parameters due to its significantly smaller size. Besides, we demonstrate that breaking the AA_β function (cryptosystem) is reducible to breaking the Rabin-p cryptosystem, and partially the other way around. Finally, we present another AA_β-variant with the public key $A_2 = pqr$, with a (negative) discussion surround the said variant. In any case, we intend to analyze the upgraded AA_β cryptosystem and the majority of its forerunner form as a future work; for instances, the rigor analysis on running time, memory consumption, hardware and software implementations, etc.

REFERENCES

Adnan, S., Isa, M., and Hashim, H. (2016a). Implementation of the AA_β lightweight asymmetric encryption scheme on an embedded system device. *Advanced Science Letters*, 22(10):2910–2913.

Adnan, S., Isa, M., and Hashim, H. (2016b). Timing analysis of the lightweight AA_β encryption scheme on embedded Linux for Internet of Things. In *ISCAIE 2016 - 2016 IEEE Symposium on Computer Applications and Industrial Electronics*, pages 113–116. IEEE.

Adnan, S., Isa, M., and Hashim, H. (2017). Energy analysis of the AA_β lightweight asymmetric encryption scheme on an embedded device. In *IEACon 2016 - 2016 IEEE Industrial Electronics and Applications Conference*, pages 116–122. IEEE.

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. (2014). Comparative Analysis of Three Asymmetric Encryption Schemes Based Upon the Intractability of Square Roots Modulo $N = p^2q$. In *The 4th International Cryptology and Information Security Conference 2014 (Cryptology2014)*, pages 86–99.

Asbullah, M. A. and Ariffin, M. R. K. (2015). Provably Secure Randomized AAβ Cryptosystem. *International Journal of Cryptology Research*, 5(2):1–14.

Asbullah, M. A. and Ariffin, M. R. K. (2016a). Analysis on the AA$_\beta$ Cryptosystem. In *The 5th International Cryptology and Information Security Conference 2016 (Cryptology2016)*, pages 41–48.

Asbullah, M. A. and Ariffin, M. R. K. (2016b). Analysis on the Rabin-p cryptosystem. In *The 4th International Conference on Fundamental and Applied Sciences (ICFAS2016)*, pages 080012–1–080012–8. AIP Conf. Proc. 1787.

Asbullah, M. A. and Ariffin, M. R. K. (2016c). Design of Rabin-like Cryptosystem without Decryption Failure. *Malaysian Journal of Mathematical Sciences*, 10(S):1–18.

Ghafar, A. H. A. and Ariffin, M. R. K. (2014). Timing Attack Analysis on AA_β Cryptosystem. *Journal of Computer and Communication*, 2:1–9.

Ghafar, A. H. A. and Ariffin, M. R. K. (2016). SPA on Rabin variant with public key $N = p^2q$. *Journal of Cryptographic Engineering*, 6(4):339–346.

Mahad, Z. and Ariffin, M. R. K. (2012). AA_β public key cryptosystem - A new practical asymmetric implementation based on the square root problem. In *Proceedings - 2012 7th International Conference on Computing and Convergence Technology (ICCIT, ICEI and ICACT), ICCCT 2012*, pages 584–588. Cited By :1.

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.

Takagi, T. (1998). Fast RSA-Type Cryptosystem Modulo p^kq. *Advances in Cryptology-CRYPTO'98*, 1462:318–326.