International Journal of Cryptology Research 7(1): 16 - 27 (2017)

Algebraic Cryptanalysis on the AA_β Cryptosystem

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

[1]*Al-Kindi Cryptography Research Laboratory, Institute for Mathematical Research, Universiti Putra Malaysia*
[2]*Mathematics Department, Faculty of Science, Universiti Putra Malaysia*

E-mail: ma_asyraf@upm.edu.my, rezal@upm.edu.my
[*]*Corresponding author*

ABSTRACT

AA_β cryptosystem is a factorization based public key encryption that uses the modulus of $N = p^2q$. In this paper, we present three types of algebraic analysis upon the AA_β cryptosystem. We begin with the continued fraction's method, then followed by the Coppersmith's techniques which present several potential ways to retrieve the prime factor of p and q from the AA_β public keys or the plaintext m from the AA_β ciphertext, respectively. For the third analysis, we analyse the congruence relation in order to solve the AA_β equation. Thus, based on such analysis, suggestions are offered as a counter measure on how to secure the AA_β cryptosystem during key generation and encryption process.

Keywords: AA_β cryptosystem, continued fraction, Coppersmiths's theorem, congruence relation

1 INTRODUCTION

In 2013, Ariffin et al. (2013) propose a new public key cryptosystem namely the AA_β cryptosystem, which combines the concept of the Bivariate Function Hard Problem together with the integer factorization problem of the modulus of $N = p^2q$ (Ariffin et al., 2013). The AA_β cryptosystem are able managed to overcome the decryption failure scenario exhibited by the Rabin cryptosystem (Rabin, 1979) and able to decrypt correctly without failure. Thus, it concluded a long journey by various authors in trying to overcome the decryption failure scenario of the Rabin cryptosystem. Among them were nicely surveyed in Asbullah and Ariffin (2016). Furthermore, the AA_β cryptosystem was proven to resilient to the stronger adversarial model, namely the chosen ciphertext attack (Asbullah and Ariffin, 2015b).

The advantages for AA_β cryptosystem is exhibited by its encryption algorithm that does not involve complicated arithmetic operations, for instance, such as division, modular multiplication or exponentiation. Only basic multiplication and addition is required. Moreover, the decryption method is able to produce a unique solution without engaging with any padding or redundancies, while still occupying the Rabin primitive (Asbullah and Ariffin, 2014). In addition, AA_β cryptosystem acquired the quality to secure large data sets.

Our contributions. In this paper, we put forward rigorous mathematical analyses conducted upon the AA_β cryptosystem. First, we showed the algebraic analysis using the continued fraction's method by manipulating the AA_β public keys and recover its prime factor; p and q. Secondly, we present the Coppersmith's theorems upon the AA_β ciphertext that present several possible ways to recover the plaintext m. The third analysis using the congruence relation of the AA_β equation and showing that to solve such congruence relation is currently infeasible. Thus, several suggestions are provided on how to secure the AA_β cryptosystem during its key generation and encryption process.

Paper Organization. The remainder of the paper is structured as follows. In Section 2, we start with the description of the AA_β cryptosystem, followed by the Legendre's theorem and the Coppersmith's technique. In Section 3, we present the algebraic analysis, namely the Legendre's theorem, the Cop-

persmith's method and the congruence relation upon the AA_β cryptosystem. Finally, we conclude in Section 4.

2 PRELIMINARIES

In this section we start with the description of the AA_β cryptosystem. We then introduce the basic facts about the Legendre's theorem and the Coppersmith's method that are used in our analysis.

2.1 AA_β Cryptosystem

First of all, we will review the AA_β cryptosystem which is proposed earlier by Ariffin et al. (2013). We now describe the key generation, encryption and decryption procedure of AA_β cryptosystem as follows.

Algorithm 1 AA_β Key Generation Algorithm

Input: The size k of the security parameter
Output: The public key A_1, A_2 and the private key d, 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 $A_2 = p^2 q$
3. Compute a random integer A_1 such that $2^{3k+4} < A_1 < 2^{3k+6}$ and $\gcd(A_1, A_2) = 1$
4. Compute an integer d such that $A_1 d \equiv 1 \pmod{A_2}$
5. Return the public key A_1, A_2 and the private key d, p, q

2.2 Legendre's theorem

In this section, we show the Legendre's theorem based on continued fractions as follows.

Algorithm 2 AA_β Encryption Algorithm

Input: The plaintext m, t and the public key A_1, A_2
Output: A ciphertext c

1. Choose a plaintext $2^{2k-2} < m < 2^{2k-1}$ such that $\gcd(m, A_2) = 1$
2. Choose a plaintext t such that $2^{4k} < t < 2^{4k+1}$
3. Compute $c = A_1 m^2 + A_2 t$
4. Return the ciphertext c

Algorithm 3 AA_β Decryption Algorithm (Asbullah and Ariffin, 2014)

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

1. Compute $w \equiv cd \pmod{A_2}$
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. Proceed to solve $m_p \pmod{p}$ and $m_q \pmod{q}$ using Garner's algorithm to obtain the list m_i for $i = 1, 2, 3, 4$
5. Compute $t_i = \frac{c - A_1 m_i^2}{A_2}$ for $m_i < 2^{2k-1}$ for $i = 1, 2, 3, 4$
6. Sort the pair (m_i, t_i) for integer t_i, else reject
7. Return the plaintext m, t

Theorem 2.1 (Legendre's Theorem)**.** *(Hardy and Wright, 1965) Let R is a rational number. Let $x, y \in \mathbb{Z}, y \neq 0$ and $\gcd(x, y) = 1$. Suppose $\left|R - \frac{x}{y}\right| < \frac{1}{2y^2}$, then $\frac{x}{y}$ is a convergent of the continued fraction expansion of R.*

The theorem simply says that the unknown integers x and y can be retrieved from the list of continued fraction expansion of a rational number R satisfying the given inequality. We remark that the theory of continued fractions is one of the very important technique used in the analysis upon a public key cryptosystem. For instance, see Nitaj (2011) and Asbullah and Ariffin (2015a).

2.3 Coppersmith's Theorem

In general, finding solutions to modular equations is easy if we know the factorization of the modulus. Else, it can be difficult. Consequently, a significantly powerful method for finding small roots of modular polynomial equations was invented by Coppersmith (1997). When working with modulo of a prime number, there is no reason to use the Coppersmith's theorem since there exist far better root-finding algorithm (for instance, Newton method), yet in cryptography we usually deal with a number of the product of primes (Galbraith, 2012). Moreover, this method has found many different applications in the area of cryptography and a vastly useful tool for cryptanalysis (Nitaj, 2013). We immediately provide the Coppersmith's theorem as follows.

Theorem 2.2. *(Coppersmith, 1997) Let N be an integer of unknown factorization. Let $f_N(x)$ be a univariate, a monic polynomial of degree δ. Then we can find all solutions x_0 for the equation $f_N(x) \equiv 0 \pmod{N}$ with $|x_0| < N^{\frac{1}{\delta}}$ in polynomial time.*

Theorem 2.3. *(May, 2003) Let N be an integer of unknown factorization, which has a divisor $b > N^{\beta}$. Furthermore, let $f_b(x)$ be a univariate, a monic polynomial of degree δ.Then we can find all solutions x_0 for the equation $f_b(x) \equiv 0 \pmod{b}$ with $|x_0| < \frac{1}{2}N^{\frac{\beta^2}{\delta}}$ in polynomial time.*

3 ANALYSIS AND DISCUSSION

In this section, we begin the analysis of the AA_β cryptosystem using the continued fraction's and the Coppersmith method upon the on the AA_β ciphertext equation. We then focuses on the the congruence relation on the AA_β cryptosytem is then given in subsequence subsection.

3.1 Continued Fraction's Method

Suppose A_1 and A_2 are the public parameters from the AA_β cryptosystem. Based on the analysis in this section, we remark that it is important to carefully check for each parameter during the AA_β key generation process.

Theorem 3.1. *Let $A_1 = e_0 + apq$ for some integer e_0 and a. Suppose $\left|\frac{A_1}{A_2} - \frac{a}{p}\right| < \frac{1}{2p^2}$ then $\frac{a}{p}$ is a convergent of the continued fraction expansion of $\frac{A_1}{A_2}$.*

Proof. Consider the value $A_1 = e_0 + apq$ then it can be rewritten as $A_1 \equiv e_0 \pmod{pq}$. Suppose $e_0 \pmod{pq}$ with $e_0 < pq$. If we multiply $A_1 = e_0 + apq$ with p, then we have $A_1 p = e_0 p + ap^2 q = e_0 p + aA_1$. Hence

$$\begin{aligned}\left|\frac{A_1}{A_2} - \frac{a}{p}\right| &= \frac{|A_1 p - aA_2|}{A_2 p} \\ &= \frac{|e_0|}{A_2}\end{aligned}$$

If $\frac{|e_0|}{A_2} < \frac{1}{2p^2}$, that is if $e_0 < \frac{A_2}{2p^2} < \frac{q}{2}$, then by Theorem 2.1, $\frac{a}{p}$ is a convergent of the continued fraction expansion of $\frac{A_1}{A_2}$. This lead to finding p and then q. □

Remark 3.1. *Therefore, we put a remark that $A_1 \equiv e_0 \pmod{pq}$ should be chosen carefully (i.e. $e_0 > \frac{q}{2}$).*

Theorem 3.2. *Let $A_1 = e_1 + bp^2$ for some integer e_1 and b. Suppose $\left|\frac{A_1}{A_2} - \frac{b}{q}\right| < \frac{1}{2q^2}$, then $\frac{b}{q}$ is a convergent of the continued fraction expansion of $\frac{A_1}{A_2}$.*

Proof. Consider the value $A_1 = e_1 + bp^2$ then it can be rewritten as $A_1 \equiv e_1 \pmod{p^2}$. Suppose $e_1 \pmod{p^2}$ with $e_1 < p^2$. If we multiply $A_1 = e_1 + bp^2$ with q, then we have $A_1 q = e_1 q + bp^2 q = e_1 q + bA_1$ Hence

$$\begin{aligned} \left| \frac{A_1}{A_2} - \frac{b}{q} \right| &= \frac{|A_1 q - bA_2|}{A_2 q} \\ &= \frac{|e_1|}{A_2} \end{aligned}$$

If $\frac{|e_1|}{A_2} < \frac{1}{2q^2}$, that is if $e_1 < \frac{A_2}{2q^2} < \frac{p^2}{2q}$, then by Theorem 2.1, $\frac{b}{q}$ is a convergent of the continued fraction expansion of $\frac{A_1}{A_2}$. This lead to finding q and then p. □

Remark 3.2. *Therefore, we put a remark that $A_1 \equiv e_1 \pmod{p^2}$ should be chosen carefully (i.e. $e_1 > \frac{p2}{2q}$).*

3.2 Coppersmith's Method

We now analyze the AA_β cryptosystem based on the Coppersmith's method (i.e.Theorem 2.2 and Theorem 2.3) and obtain the following results.

Proposition 3.1. *Let $c = A_1 m^2 + A_2 t$ be the AA_β ciphertext. Let d such that $A_1 d \equiv 1 \pmod{A_2}$ where $A_2 = p^2 q$. If $m < A_2^{\frac{1}{2}}$, then it can be found in polynomial time.*

Proof. Since there exist an integer d such that $A_1 d \equiv 1 \pmod{A_2}$ where $A_2 = p^2 q$. Compute $w \equiv cd \equiv m^2 \pmod{A_2}$. Consider $f_{A_2}(x) \equiv x^2 - w \equiv 0 \pmod{A_2}$. Consider the Coppersmiths method (i.e. Theorem 2.2) hence $\delta = 2$, the root $x_0 = m$ can be recovered if $m < A_2^{\frac{1}{\delta}} = A_2^{\frac{1}{2}} \approx 2^{\frac{3k}{2}}$. □

Proposition 3.2. *Let $c = A_1 m^2 + A_2 t$ be the AA_β ciphertext. Let $w \equiv m^2 \pmod{p^2}$ such that p^2 is an unknown factor for A_2. If $m < A_2^{\frac{2}{9}}$, then m can be found in polynomial time.*

Proof. Suppose $w \equiv cd \equiv m^2 \pmod{p^2}$ such that p^2 is an unknown factor for A_2. Let $f_{p^2}(x) \equiv x^2 - w \equiv 0 \pmod{p^2}$ with $p^2 \approx 2^{2k} \approx A_2^{\frac{2}{3}}$. Consider the Theorem 2.3. We can find a solution $x_0 = m$ if $m < \frac{1}{2} A_2^{\frac{\beta^2}{\delta}} < A_2^{\frac{(\frac{2}{3})^2}{2}} = A_2^{\frac{2}{9}} \approx 2^{\frac{2k}{3}}$. □

Remark 3.3. *Therefore in order to avoid both attacks, we would set $m > 2^{\frac{3k}{2}}$ in the AA_β encryption algorithm.*

Proposition 3.3. *Let d_0 such that $A_1 d_0 \equiv 1 \pmod{p^2}$ where p^2 is an unknown factor for A_2. If $|d_0| < A_2^{\frac{4}{9}}$ then d_0 can be found in polynomial time.*

Proof. Let d_0 such that $A_1 d_0 \equiv 1 \pmod{p^2}$ where p^2 is an unknown factor for A_2. Consider $f_{p^2}(x) \equiv A_1 x - 1 \equiv 0 \pmod{p^2}$ with $p^2 \approx 2^{2k} \approx A_2^{\frac{2}{3}}$. Thus by applying Theorem 2.3, we can find solution $x_0 = d_0$ if $|d_0| < \frac{1}{2} A_2^{\frac{\beta^2}{\delta}} < A_2^{\frac{(\frac{2}{3})^2}{1}} = A_2^{\frac{4}{9}}$. then d_0 can be found in polynomial time. □

Corollary 3.1. *Let d_1 such that $A_1 d_1 \equiv 1 \pmod{pq}$ where pq is an unknown factor for A_2. If $|d_1| < A_2^{\frac{4}{9}}$ then d_1 can be found in polynomial time.*

Proof. Consider $f_{pq}(x) \equiv A_2 x - 1 \equiv 0 \pmod{pq}$ with $pq > A_2^{\frac{2}{3}}$. Then we reach the same conclusion as the Proposition 3.3. □

The significant of the result from Proposition 3.3 and Corollary 3.1 is that if one is able to compute either d_0 or d_1 then one is able to factor $A_2 = p^2 q$.

Proposition 3.4. *If $d_0 < A_2^{\frac{4}{9}}$ such that $A_1 d_0 \equiv 1 \pmod{p^2}$, then $A_2 = p^2 q$ can be factored in polynomial time.*

Proof. Consider the relation $A_1 d_0 \equiv 1 \pmod{p^2}$. Suppose the integer $d_0 < A_2^{\frac{4}{9}}$ could be computed using Proposition 3.3. Then we have the value $A_1 d_0 - 1 \equiv 0 \pmod{p^2}$ where $A_1 d_0 - 1$ is an integer multiple of p^2. Observe that

if we take the $\gcd(A_1 d_0 - 1, A_2)$ resulting p^2, and then $\frac{A_2}{p^2} = q$. The same argument is applicable for $d_1 < A_2^{\frac{4}{9}}$ such that $A_1 d_1 \equiv 1 \pmod{pq}$. □

Corollary 3.2. *If $d_1 < A_2^{\frac{4}{9}}$ such that $A_1 d_1 \equiv 1 \pmod{pq}$, then $A_2 = p^2 q$ can be factored in polynomial time.*

Proof. Consider Proposition 3.4. The same argument is applicable for $d_1 < A_2^{\frac{4}{9}}$ such that $A_1 d_1 \equiv 1 \pmod{pq}$. □

Remark 3.4. *Consider Propostion 3.4 and Corollary 3.2. In order for the AA_β cryptosystem to be resistant against such methods, it is important to check for each $d_0, d_1 > A_2^{\frac{4}{9}}$ during the AA_β key generation process.*

3.3 Congruence Relation

Consider the Algorithm 1. Observe that the integer d is easily computed, nonetheless without the prime factors of A_2, we only ended up with the congruence relation of $cd \equiv m^2 \pmod{A_2}$ where $A_2 = p^2 q$. Thus to solve the congruence $m^2 \pmod{A_2}$ reduces to solve the integer factorization problem, which is currently infeasible. Now, since the $\gcd(A_1, A_2) = 1$ then exist a unique integer d' such that $A_2 d' \equiv 1 \pmod{A_1}$. In this section, we show that such integer d' can be use to solve the AA_β equation, but it is still far from feasible.

Theorem 3.3. *Suppose $c = A_1 m^2 + A_2 t$ be the AA_β equation. Let d' such that $A_2 d' \equiv 1 \pmod{A_1}$. If at minimum 2^{k-4} is exponentially large, then it is infeasible to determine m^2 or t from its congruence relation.*

Proof. Let $c = A_1 m^2 + A_2 t$ be the AA_β equation. Since the $\gcd(A_1, A_2) = 1$ thus there exist the integer d' such that $A_2 d' \equiv 1 \pmod{A_1}$. Suppose we take $cd' \equiv t \pmod{A_1}$. Set $a \equiv t \pmod{A_1}$. Then there exist for integer j such that

$$t = a + A_1 j \tag{1}$$

Substitute (1) into $c = A_1m^2 + A_2t$, we obtain $c = A_1m^2 + A_2t = A_1m^2 + A_2(a + A_1j)$. Then we have $m^2 = \frac{c-A_2(a+A_1j)}{A_1} = \frac{c-A_2a}{A_1} - A_2j$. Note that $m^2 \in \mathbb{Z}$ also implies $\frac{c-A_2a}{A_1} \in \mathbb{Z}$. Hence setting $b = \frac{c-A_2a}{A_1}$, it follows that we have construct two parametric equation $t = a + A_1j$ and $m^2 = b - A_2j$ for $c = A_1m^2 + A_2t$. However, it is suffice only to find the integer j for $m^2 = b - A_2j$ such that $j = \frac{b-m^2}{A_2}$ satisfying $2^{4k-4} < m^2 < 2^{4k-2}$ and $\sqrt{b - A_2j} \in \mathbb{Z}$. We know that $2^{3k} < A_2 < 2^{3k+3}$. Hence we deduce that j should be in the range of

$$\frac{b - 2^{4k-2}}{2^{3k}} < j < \frac{b - 2^{4k-4}}{2^{3k}}$$

Therefore the difference between the upper and the lower bound of j is

$$\begin{aligned} \frac{b - 2^{4k-4}}{2^{3k}} - \frac{b - 2^{4k-2}}{2^{3k}} &= \frac{-2^{4k-4} + 2^{4k-2}}{2^{3k}} \\ &= \frac{(2^2 - 1) \cdot 2^{4k-4}}{2^{3k}} \\ &= 3 \cdot 2^{k-4} \\ &> 2^{k-4} \end{aligned}$$

The difference is very large and finding the correct j is need to sieve through approximately 2^{k-4} possible integer where 2^{k-4} is exponentially large. Hence finding the correct j using this approach is infeasible. □

4 SUMMARY

We now summarize the paper. In this paper, we put forward rigorous mathematical analyses conducted upon the AA_β cryptosystem. First, we present the congruence relation of the AA_β equation. We showed that to solve such congruence is infeasible. Secondly, we presented the analysis using the continued fraction's method which applies when $e_0 < \frac{q}{2}$ (or $e_1 < \frac{p2}{2q}$) satisfies an equation $A_1 = e_0 + apq$ (or $A_1 = e_1 + bp^2$), hence obtained the primes p and q. The third analysis is using the Coppersmith's theorems upon the AA_β ciphertext to recover the plaintext m. Finally, we provide a suggestion as a countermeasure during the AA_β key generation and encryption process, respectively.

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. (2016). Design of Rabin-like Cryptosystem without Decryption Failure. *Malaysian Journal of Mathematical Sciences*, 10(S):1–18.

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 *In the Proceeding of the* 4^{th} *International Cryptology and Information Security Conference 2014*, pages 86–99.

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

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

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

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

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

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

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

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

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