ASM Sc. J., 12, Special Issue 1, 2019 for IQRAC2018, 191-202

Successful Cryptanalysis upon a Generalized RSA Key Equation

Normahirah Nek Abd Rahman*[1], Muhammad Rezal Kamel Ariffin[2,3], and Muhammad Asyraf Asbullah[2]

[1]*Pusat PERMATApintar Negara, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia*

[2]*Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia*

[3]*Department of Mathematics, Faculty of Science, Universiti Putra Malaysia,43400 UPM Serdang, Selangor, Malaysia*

**Corresponding author: normahirah@ukm.edu.my*

This work presents three distinct attacks on the modulus of type $N = p^2q$. The first attack focused on the generalized key equation $eX - NY = (ap^2 + bq^2)Z$. Under certain conditions, the modulus $N = p^2q$ can be factored in polynomial time by using continued fraction expansion together with some restrictions on some parameters. The existence of probabilistic polynomial time algorithm which output the factor p and q is also presented. Hence, one can run the proposed algorithm to test whether the key belongs to the corresponding weak class or not to ensure that one does not accidentally create a weak key. Consequently, the next two attacks focus on multivariable case for system of generalized key equations utilize the combination of simultaneous Diophantine approximation and the LLL algorithm which enables one to factor the k moduli $N_i = p_i^2q_i$ simultaneously in polynomial time.

Keywords: Continued fraction, Lattice basis reduction, Public key Cryptosystem, Post-Quantum, Multivariate

I. Introduction

The idea to utilize key e to encrypt and key d to decrypt came from the seminal work by Diffie and Hellman, 1976 where $e \neq d$. This idea radicalized the secure communication concept. Invented in 1978, named after its inventors Rivest, Shamir and Adleman, RSA cryptosystem is one of the well-known public key cryptosystem that played a very important role in providing privacy and ensuring data authenticity.

The mathematical operations in RSA depend on three parameters, the modulus $N = pq$ which is the product of prime numbers p and q, a congruence relation of $ed \equiv 1 (\text{mod } \phi(N))$ where e, d be the public exponent and the private exponent, respectively and $\phi(N)$ is the Euler's totient function. Hence, the difficulty of breaking the RSA cryptosystem is based on three hard mathematical problems, namely the integer factorization problem of $N = pq$, finding the e-th root of $x \equiv y^e (\text{mod } N)$ and solving the linear equation $ed - k\phi(N) = 1$ which contains three variables namely $(d, \phi(N), k)$ (Rivest, Shamir, and Adleman, 1978).

There are many practical issues that have been considered when implementing RSA cryptosystem to reduce the encryption process or the execution decryption time. If the secret exponent d is relatively small, then the RSA cryptosystem seems to have faster decryption process. Therefore, knowing the value of d will lead to factoring the modulus N.

In 1990, Wiener proved that, if the secret exponent $d < \frac{1}{3}N^{1/4}$ which lead to RSA to be totally insecure. Wiener, 1990 was able to obtain the integer solutions through the continued fractions of $\frac{e}{N}$ and eventually factor-

ing N. Recently, Muhammad Asyraf Asbullah and Muhammad Rezal Kamel Ariffin, 2019 show that the Wiener's bound can be improved to $d < \frac{1}{2}N^{1/4}$. Furthering this, by using lattice basis reduction technique D. Boneh and G. Durfee, 1999 proposed an extension of Wiener's work which RSA insecure when the secret exponent $d < N^{0.292}$. Blömer and May, 2004 combine lattice basis reduction techniques with continued fractions algorithm which later leads to the factorization of RSA.

J. Hinek, 2007 presented another attack for a single user generate k instances of RSA (N_i, e_i), each with the same small private exponent d using k equations $e_i d - k_i\phi(N_i) = 1$ and showed that the k modulus N_i are easily factorable if $d < N^{\delta}$ with $\delta = \frac{k}{2(k+1)} - \varepsilon$ which ε is a small constant relying upon the size of max N_i.

Sarkar and Maitra, 2010 proposed a generalized attack when $n \geq 2$ many decryption key d used with the common RSA modulus N and $d_i < N^{\frac{3n-1}{4n-4}}$ for each i, $1 \leq i \leq n$. Later, Nitaj et al., 2014 proposed new strategy based on the a lattice basis reduction technique to factor all the RSA moduli $N_1, ..., N_k$. The result consider the situation such that the RSA moduli satisfy k equations respectively to the generalized key equation $e_i x - y_i\phi(N_i) = z_i$ or $e_i x_i - y\phi(N_i) = z_i$, where x_i, y_i, z_i, x, y are appropriately small parameters and $\phi(N_i) = (p_i - 1)(q_i - 1)$.

Variant designs of the RSA utilizing $N = p^2q$ exist because of various reasons to achieve better throughput. This is to be able to send large data sets and to obtain better computation time while maintaining the level of security. For example the HIME(R) design became a standard in Japan because it was able to "carry" more data securely than the existing RSA.

On the other hand, Takagi, 1998 showed that the decryption process is about three times faster than RSA cryptosystem using Chinese Remainder Theorem if they choose the 768-bit modulus p^2q for 256-bit primes p and q. Additionally, AA_β Cryptosystem that has been proposed by Muhammad Rezal Kamel Ariffin et al., 2013 overcome Rabin's cryptosystem decryption failure which was due to a 4-to-1 mapping by incorporating the hardness of factoring integer $N = p^2q$ coupled with the square root problem as its cryptographic primitive. The design for encryption does not involve "expensive" mathematical operation.

Throughout many years, the use of modulus $N = p^2q$ has found in many applications in cryptography. For example, Fujioka, Tatsuaki Okamoto, and Miyaguchi, 1991 used a modulus of the form $N = p^2q$ in an electronic cash scheme. Due to Peralta and E. Okamoto, 1996, a factoring method specifically for $N = p^2q$ has been proposed which this method is a variation of Ellicptic Curve Method (ECM) and was suggested to be slightly faster than ECM (M. J. Hinek, 2009). Then, T. Okamoto and Uchiyama, 1998 proposed a public key cryptosystem which can be proven to be as secure as the intractability of factoring $N = p^2q$ against passive adversaries (Dan Boneh, Glenn Durfee, and Howgrave-Graham, 1999).

According to May, 2004 the modulus of the form $N = p^2q$ was frequently used in designing efficient public key cryptosystems, thus such modulus is considered an important case in cryptography and cryptanalysis. Instances of schemes that utilize the modulus $N = p^2q$ are Multi-power RSA Cryptosystem (Takagi, 1998), T. Okamoto and Uchiyama, 1998, HIME(R) Cryptosystem (Nishioka, Satoh, and Sakurai, 2001), the AA_β Cryptosystem (M. Asbullah and M. Ariffin, 2014) and Rabin-p Cryptosystem (M. A. Asbullah and M. R. K. Ariffin, 2016b).

In 2014, Sarkar proved that the modulus $N = p^2q$ can be factored if $d < N^{0.395}$ using lattice reduction techniques (Sarkar, 2014). Recently, M. A. Asbullah and M. R. K. Ariffin, 2015 shows that the modulus of $N = p^2q$ can be factored if e satisfies the equation $eX - (N - (ap^2 + bq^2))Y = Z$ with some restrictions on some parameters. Motivated from these efforts, we will look at the modulus of the form $N = p^2q$ as the basis of our analysis.

Our contributions. In this paper, we begin with an attack on the modulus of type

$N = p^2q$ by using the continued fraction expansion method. We consider the public value, e satisfying the following generalized key equation, $eX - NY = (ap^2 + bq^2)Z$. We present a strategy to find prime factor p and q of the modulus $N = p^2q$ in polynomial time by using continued fraction expansion if $\gcd(X, Y) = 1$, $|ap^2 - bq^2| < N^{1/2}$, $1 \leq |Z| < \frac{\sqrt{2}N^{1/2}}{|ap^2-bq^2|}$, $1 \leq Y < X < \frac{N}{2|Z|(ap^2+bq^2)}$ together with an algorithm that on input public parameters and output the factor p and q. Hence, one can run the algorithm to test whether the key belongs to the coresponding weak class or not. This property is very useful in the design of cryptosystem during key generation process to ensure that one does not accidentally create a weak key.

Next, the second attack is upon k-instances (N_i, e_i). We show that we are able to factor k moduli of the form $N_i = p_i^2q_i$ satisfying the system of generalized key equations $e_ix - N_iy_i = (ap_i^2 + bq_i^2)z_i$. We prove each moduli N_i can be factored in polynomial time if $x < N^\delta$, $y_i < N^\delta$, $1 \leq |z_i| < \frac{\sqrt{2}N^{1/2}}{|ap_i^2-bq_i^2|}$ where $\delta = \frac{k}{6}$, $N = \min N_i$ simultaneously.

For the third attack, we show that we are able to factor k moduli $N_i = p_i^2q_i$ when k instances (N_i, e_i) are available and the variables (x_i, y, z, δ) in the system of generalized key equations given by $e_ix_i - N_iy = (ap_i^2 + bq_i^2)z_i$ satisfying $x_i < N^\delta$, $y < N^\delta$, $1 \leq |z_i| < \frac{\sqrt{2}N^{1/2}}{|ap_i^2-bq_i^2|}$ where $\delta = \beta k - \frac{5k}{6}$, $N = \max N_i$ and $\min e_i = N^\beta$.

For the second and third attack, we apply lattice basis reduction techniques upon the simultaneous Diophantine problem with the objective of finding the parameters (x, y_i) or (x_i, y), respectively. This leads to an appropriate approximation of $ap^2 + bq^2$ to simultaneously extract the prime factors p_i and q_i of each $N_i = p_i^2q_i$.

The paper is organized as follows. Section 2 presents an introduction on some existing essential definitions and theorems. In Section 3, 4 and 5, we consecutively present three distinct attacks, accompanied with numerical examples. In Section 6, we give the conclusion.

II. Preliminaries

A brief introduction to continued fractions expansion, the lattice basic reduction and simultaneous Diophantine approximation is described in this section which later will be utilized all through this paper.

A. Continued Fractions Expansion

An algebraic expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \ddots}}} = [a_0, a_1, \ldots, a_n, \ldots],$$

is a definition of the expansion of a continued fraction. Such algebraic form can also be represented as $x = [a_0, a_1, \ldots, a_n, \ldots]$. Since the appearance of the Wiener, 1990 work, much more results on cryptanalysis using continued fraction expansions have become available. For example are in recent years by the work of Muhammad Asyraf Asbullah, Muhammad Rezal Kamel Ariffin, and Mahad, 2016 and M. A. Asbullah and M. R. K. Ariffin, 2016a.

Theorem 1. (Legendre's Theorem) *(Hardy and Wright, 1965) . Let the continued fraction expansion of x represented as $x = [a_0, a_1, a_2, \ldots]$. If $\gcd(X, Y) = 1$ and*

$$\left|x - \frac{Y}{X}\right| < \frac{1}{2X^2}$$

then $\frac{Y}{X}$ is convergent of x.

B. Lattice Basis Reductions

For $d \leq n$, let $u_1, ..., u_d$ be d linearly independent vectors of $\mathbb{R}^n$. The set of all integer linear combinations of the vectors $u_1, ..., u_d$ is called a lattice of the form

$$\mathcal{L} = \left\{ \sum_{i=1}^{d} x_iu_i \;\; | \;\; x_i \in \mathbb{Z} \right\}.$$

The set $(u_1, ..., u_d)$ is called a basis of $\mathcal{L}$ with a dimension d. Let U be the matrix of the u_i's in

the canonical basis of $\mathbb{R}^n$. Then the determinant of $\mathcal{L}$ is defined as $\det(\mathcal{L}) = \sqrt{\det(U^T U)}$. Suppose $\|v\|$ is the Euclidean norm of a vector $v \in \mathcal{L}$. One of an important computational problem in lattice is to locate a short non-zero vector in $\mathcal{L}$.

Theorem 2. *(A. K. Lenstra, H. W. Lenstra, and Lovász, 1982). Let $\mathcal{L}$ be a lattice of dimension τ with a basis $\{v_1, ..., v_\tau\}$. The LLL algorithm produces a reduced basis $\{b_1, ..., b_\tau\}$ satisfying*

$$\|b_1\| \leq \|b_2\| \leq ... \leq \|b_i\| \leq 2^{\frac{\tau(\tau-1)}{4(\tau+1-i)}} \det(L)^{\frac{1}{\tau+1-i}},$$

for all $1 \leq i \leq \tau$.

One of the crucial uses of the LLL algorithm is provides solutions to the simultaneous Diophantine approximations problem. A. K. Lenstra, H. W. Lenstra, and Lovász, 1982 proposed a way to compute simultaneous Diophantine approximations with rational entries. They considered a lattice with real numbers as shown in the following proposition.

Proposition 1. *There exists a polynomial time algorithm that, given a positive integer n and rational numbers $\alpha_1, \alpha_2, ..., \alpha_n$, ε satisfying $0 < \varepsilon < 1$, finds integers $p_1, p_2..., p_n$ and q for which*

$$|q\alpha_i - p_i| < \varepsilon \text{ and } 1 \leq q \leq 2^{n(n+1)/4}\varepsilon^{-n}$$

for $1 \leq i \leq n$.

The above proposition follows immediately from the following classical theorem of Dirichlet (Cassels, 1971, Section V.10).

Theorem 3. (Dirichlet Theorem). *Let $\theta_1, ..., \theta_n$ be n real numbers and Q a real number such that $0 < Q < 1$. There exist integers $s_1, ..., s_n$ and a positive integer $r \leq Q^{-n}$ such that*

$$|r\theta_i - s_i| < Q \text{ for } 1 \leq i \leq n.$$

Afterward, Nitaj et al., 2014 stated a proof for a lattice with integer entries as follows.

Theorem 4. (Simultaneous Diophantine Approximations) *For rational numbers $\alpha_1, ..., \alpha_n$, there exists an algorithm in polynomial time to compute integers $p_1, ..., p_n$ and a positive integer q such that*

$$max_i|q\alpha_i - p_i| < \varepsilon \text{ and } q \leq 2^{n(n-3)/4} \cdot 3^n \cdot \varepsilon^{-n}$$

with $0 < \varepsilon < 1$,

Proof. Appendix A, page 196 (Nitaj et al., 2014).

III. The First Attack

We begin with the first attack upon the modulus $N = p^2 q$ which is based on the generalized key equation $eX - NY = \left(ap^2 + bq^2\right) Z$. Define $[x]$ as a notation for the closest integer to x. Without loss of generality, we may assume that the modulus $N = p^2 q$ satisfies $q < p < 2q$. We begin with the following lemmas.

Lemma 1. *(M. A. Asbullah and M. R. K. Ariffin, 2015). For $N = p^2 q$, then*

$$2^{-1/3} N^{1/3} < q < N^{1/3} < p < 2^{1/3} N^{1/3}$$

is true.

Lemma 2. *Let $|ap^2 - bq^2| < N^{1/2}$ with suitably small integers a, b and $gcd(a, b) = 1$. Let $S = (ap^2 + bq^2)Z$, such that $1 \leq |Z| < \frac{\sqrt{2}N^{1/2}}{|ap^2 - bq^2|}$, then $abZ^2 q = \left[\frac{S^2}{4N}\right]$.*

Proof. Consider $S = (ap^2 + bq^2)Z$. Observe that

$$\begin{aligned} S^2 &= \left((ap^2 + bq^2)Z\right)^2 \\ &= (aZp^2 + bZq^2)^2 \\ &= (aZp^2 - bZq^2)^2 + 4(aZp^2 bZq^2) \\ &= (aZp^2 - bZq^2)^2 + 4abZ^2 qN \end{aligned}$$

Hence we obtain

$$S^2 - 4abZ^2 qN = (aZp^2 - bZq^2)^2 > 0 \quad (1)$$

Divides (1) by $4N$, we have

$$\begin{aligned}\left|\frac{S^2}{4N} - abZ^2q\right| &= \left|\frac{S^2 - 4abZ^2qN}{4N}\right| \\ &= \frac{(aZp^2 - bZq^2)^2}{4N} \\ &= \frac{(ap^2 - bq^2)^2 Z^2}{4N} \\ &< \frac{(ap^2 - bq^2)^2 \left(\frac{\sqrt{2}N^{1/2}}{|ap^2 - bq^2|}\right)^2}{4N} \\ &< \frac{\left(\sqrt{2}N^{1/2}\right)^2}{4N} \\ &= \frac{1}{2}\end{aligned}$$

Hence $abZ^2q = \left\lfloor \frac{S^2}{4N} \right\rfloor$. □

Lemma 3. *Consider e and N satisfying the equation $eX - NY = \left(ap^2 + bq^2\right) Z$ with suitably small integers a, b such that $\gcd(a, b) = \gcd(X, Y) = 1$. If $1 \leq Y < X < \frac{N}{2|Z|(ap^2+bq^2)}$, then $\frac{Y}{X}$ is amongst the convergent of the continued fraction $\frac{e}{N}$.*

Proof. Consider the equation $eX - NY = \left(ap^2 + bq^2\right) Z$. Suppose $X < \frac{N}{2|Z|(ap^2+bq^2)}$, thus dividing such equation by NX gives

$$\left|\frac{e}{N} - \frac{Y}{X}\right| = \left|\frac{\left(ap^2 + bq^2\right) Z}{NX}\right|$$

Since $X < \frac{N}{2|Z|(ap^2+bq^2)}$ then $\left|\frac{\left(ap^2+bq^2\right)Z}{NX}\right| < \frac{1}{2X^2}$ holds. Hence by Theorem 1, $\frac{Y}{X}$ is one of a convergent of the continued fraction $\frac{e}{N}$. □

Theorem 5. *Let e, N satisfying the equation $eX - NY = \left(ap^2 + bq^2\right) Z$ where X and Y are coprime. Let $1 \leq |Z| < \frac{\sqrt{2}N^{1/2}}{|ap^2 - bq^2|}$. If $1 \leq Y < X < \frac{N}{2|Z|(ap^2+bq^2)}$ and $|ap^2 - bq^2| < N^{1/2}$, then N can be factored in polynomial time.*

Proof. Assume $X < \frac{N}{2|Z|(ap^2+bq^2)}$, thus from Lemma 3 gives $\frac{Y}{X}$ is amongst the convergent of the continued fraction of $\frac{e}{N}$. Define S such that $S = eX - NY$. Note that Lemma 2 clearly implies $abZ^2q = \left\lfloor \frac{S^2}{4N} \right\rfloor$. Hence we obtain $q = \gcd\left(\left\lfloor \frac{S^2}{4N} \right\rfloor, N\right)$. □

We outline the following algorithm for factoring the modulus $N = p^2q$ as per Theorem 5.

Table 1: Algorithm 1

Input: The integers (N, e) satisfies Theorem 5
Output: The prime factors p, q
1. Compute the continued fraction $\frac{e}{N}$.
2. For each convergent $\frac{Y}{X}$ of $\frac{e}{N}$, compute $S = eX - NY$.
3. Compute $\left\lfloor \frac{S^2}{4N} \right\rfloor$.
4. Compute $q = \gcd\left(\left\lfloor \frac{S^2}{4N} \right\rfloor, N\right)$.
5. If $1 < q < N$, then $p = \sqrt{\frac{N}{q}}$.

Example 1. *As an illustration of our first attack, let N and e be as follows.*

$$\begin{aligned} N &= 64779261851429 \\ e &= 54618098576427 \end{aligned}$$

Assume that the tuple (e, N) fulfill all the restrictions as stated as in Theorem 5. First of all, we determine the convergents of the continued fraction expansion of $\frac{e}{N}$ as follows.

$$\left[0, 1, \frac{5}{6}, \frac{11}{13}, \frac{16}{19}, \frac{27}{32}, \frac{43}{51}, \frac{3682}{4367}, \frac{7407}{8785}, \frac{11089}{13152}, \frac{18496}{21937}, \dots\right].$$

Observe that the convergent $\frac{5}{6}, \frac{11}{13}, \frac{16}{19}, \frac{27}{32}$, would produce S and $\left\lfloor \frac{S^2}{4N} \right\rfloor$ such that the $\gcd\left(\left\lfloor \frac{S^2}{4N} \right\rfloor, N\right) = 1$. respectively.

We proceed with the next convergent $\frac{43}{51}$, then we obtain

$$S = eX - NY = 14767786330$$

and

$$\left\lfloor \frac{S^2}{4N} \right\rfloor = 841656$$

Hence, we compute the $\gcd(841656, 64779261851429)$ *then we obtain* 35069*, which gives the prime factors* $q = 35069$ *and* $p = \sqrt{\frac{N}{q}} = 42979$.

IV. The Second Attack

We now present the second attack. The methodolgy used in this section is analogous to the work presented in Rahman et al., 2018. Suppose that we are given k moduli $N_i = p_i^2 q_i$ for system of generalized key equations satisfying $e_i x - N_i y_i = (ap_i^2 + bq_i^2)z_i$. We transform the equation into simultaneous Diophantine approximation problem, then we apply lattice basis reduction algorithm in order to obtain the parameters (x, y_i) which later recover the prime factor p_i and q_i.

Theorem 6. *Suppose that $k \geq 2$, $N_i = p_i^2 q_i$, $1 \leq i \leq k$ be k moduli. Let $N = \min N_i$. Assume that e_i, $i = 1, ..., k$ be k public exponents. Define $\delta = \frac{k}{6} - \alpha k$. Let a, b be suitably small integers with $\gcd(a, b) = 1$. Let $ap_i^2 + bq_i^2 < N^{\frac{2}{3}+\alpha}$ where $0 < \alpha < 1/3$. For $i = 1, ..., k$, if there exist integers x and y such that $x < N^{\delta}$, k integers $y_i < N^{\delta}$ and $|z_i| < \frac{\sqrt{2}N^{1/2}}{|ap_i^2 - bq_i^2|}$ satisfying*

$$e_i x - N_i y_i = (ap_i^2 + bq_i^2)z_i$$

then it is possible to factor k moduli of the form $N_i = p_i^2 q_i$ in polynomial time.

Proof. Suppose that $k \geq 2$ and $i = 1, ..., k$, and the equation $e_i x - N_i y_i = (ap_i^2 + bq_i^2)z_i$, we obtain

$$\left| \frac{e_i}{N_i} x - y_i \right| = \frac{|(ap_i^2 + bq_i^2)z_i|}{N_i} \tag{2}$$

Let $N = \min N_i$ and suppose that $y_i < N^{\delta}$ and $|z_i| < \frac{\sqrt{2}N^{1/2}}{|ap_i^2 - bq_i^2|}$. Sets $|ap_i^2 - bq_i^2| > p_i$. From here, by using $N^{1/3} < p < 2^{1/3}N^{1/3}$ and $ap_i^2 + bq_i^2 < N^{\frac{2}{3}+\alpha}$ where $0 < \alpha < 1/3$, we have

$$\begin{aligned} \frac{(ap_i^2 + bq_i^2)|z_i|}{N_i} &\leq \frac{(ap_i^2 + bq_i^2)|z_i|}{N} \\ &< \frac{(N^{\frac{2}{3}+\alpha})\left(\frac{\sqrt{2}N^{1/2}}{N^{1/3}}\right)}{N} \\ &< \frac{2^{1/2}N^{\frac{5}{6}+\alpha}}{N} \\ &= 2^{1/2}N^{-\frac{1}{6}+\alpha} \end{aligned} \tag{3}$$

By applying Theorem 4, we substitute (3) in (2), we obtain

$$\left| \frac{e_i}{N_i} x - y_i \right| < 2^{1/2}N^{-\frac{1}{6}+\alpha}$$

We can see the relation between $\left| \frac{e_i}{N_i} x - y_i \right| < 2^{1/2}N^{-\frac{1}{6}+\alpha}$ and $|q\alpha_i - p_i| < \varepsilon$ which is the condition of Theorem 4. We now proceed to prove the existence of integer x and y_i. Let $\varepsilon = 2^{1/2}N^{-\frac{1}{6}+\alpha}$ and $\delta = \frac{k}{6} - \alpha k$.

$$N^{\delta} \cdot \varepsilon^k = 2^{k/2}N^{\delta - \frac{k}{6} + \alpha k} = 2^{k/2}$$

Since $2^{3k/2} < 2^{\frac{k(k-3)}{4}} \cdot 3^k$ for $k \geq 2$, we get $N^{\delta} \cdot \varepsilon^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k$ by applying Theorem 4. It follows that if $x < N^{\delta}$, then $x < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \varepsilon^{-k}$. Summarizing for $i = 1, ..., k$, we have

$$\left| \frac{e_i}{N_i} x - y_i \right| < \varepsilon, \quad x < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \varepsilon^{-k}$$

It follows the condition of Theorem 4 are fulfilled will find x and y_i for $i = 1, ..., k$ using the LLL algorithm.

Since $1 < |z_i| < \frac{\sqrt{2}N^{1/2}}{|ap_i^2 - bq_i^2|}$ this implies that $abz_i^2 q = \left[\frac{S^2}{4N}\right]$ for $S_i = e_i x - N_i y_i$ for each $i = 1, ..., k$, we find $q_i = \gcd\left(\left[\frac{S_i^2}{4N_i}\right], N_i\right)$. This leads to the factorization of k moduli $N_1, ..., N_k$. This terminates the proof. □

Example 2. *To illustrate our proposed attack, we consider three moduli and three public exponents as follows*

$$\begin{aligned} N_1 &= 438491276834338428751722 19879, \\ N_2 &= 373381539333061239157945 89133, \\ N_3 &= 389076161621226917418494 40007, \\ e_1 &= 395110405789616765118050 87156, \\ e_2 &= 337812067342845560774837 64081, \\ e_3 &= 333707217425813772403972 85375. \end{aligned}$$

Then, $N = \min(N_1, N_2, N_3) = 373381539333061239157945 89133$. Since $k = 3$, we get $\delta = \frac{k}{6} - \alpha k = \frac{2}{5}$ and $\varepsilon = 2^{1/2}N^{-\frac{1}{6}+\alpha} \approx 0.0002192272918193153$.

Suppose we consider the parameter C as defined in [Nitaj et al. (2014), Appendix A, page 196]. Let $n = k = 3$, we find

$$C = \left[3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1}\right] = 17533820149394491.$$

Let the lattice $\mathcal{L}$ spanned by the rows of the following matrix

$$M = \begin{bmatrix} 1 & -[\frac{Ce_1}{N_1}] & -[\frac{Ce_2}{N_2}] & -[\frac{Ce_3}{N_3}] \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}.$$

From here, we execute the LLL algorithm upon $\mathcal{L}$, which gives a reduced basis with the matrix

$$K = \begin{bmatrix} -268448596723 & -167028992386 & -4917963426 & -106185527291 \\ -654605070273 & 1406018496079 & 531004736379 & -359359492007 \\ -677045425593 & 877605625120 & -2159196616321 & 846337749061 \\ -1682298812257 & 519399713921 & 1031829553753 & 3337214576858 \end{bmatrix}.$$

Now, we obtain

$$K \cdot M^{-1} = \begin{bmatrix} -268448596723 & -19155721381 & -19233721343 & -18233581353 \\ -654605070273 & -46710739016 & -46900939938 & -44462124029 \\ -677045425593 & -48312018365 & -48508739518 & -45986319161 \\ -1682298812257 & -120044014834 & -120532820680 & -114265198730 \end{bmatrix}.$$

From the first row, we deduce $x = 268448596723$, $y_1 = 19155721381$, $y_2 = 19233721343$ *and* $y_3 = 18233581353$.

By applying x *and* y_i *for* $i = 1, 2, 3$, *define* $S_i = e_i x - N_i y_i$ *is an approximation of* $ap_i^2 + bq_i^2$. *Observe that Lemma 2 and Theorem 5 obviously implies* $abz_i^2 q_i = \left\lceil \frac{S_i^2}{4N_i} \right\rfloor$ *for* $S_i = e_i x - N_i y_i$. *Then, we obtain*

$$\begin{aligned} S_1 &= 483129855602780442189, \\ S_2 &= 406002912661669067233, \\ S_3 &= 439874805597543857154. \end{aligned}$$

Next, for each $i = 1, 2, ..., 3$, *we find*

$$\left\lceil \frac{S_1^2}{4N_1} \right\rfloor = 1330781646672,$$
$$\left\lceil \frac{S_2^2}{4N_2} \right\rfloor = 1103685826194,$$
$$\left\lceil \frac{S_3^2}{4N_3} \right\rfloor = 1243264582140.$$

Then, also for each $i = 1, 2, 3$, *we find* $q_i = \gcd\left(\left\lceil \frac{S_i^2}{4N_i} \right\rfloor, N_i\right)$ *and we obtain*

$$\begin{aligned} q_1 &= 3080513071, \\ q_2 &= 2919803773, \\ q_3 &= 2960153767. \end{aligned}$$

This leads us to the factorization of three moduli N_1, N_2 *and* N_3 *which*

$$\begin{aligned} p_1 &= 3772844893, \\ p_2 &= 3576017111, \\ p_3 &= 3625435439. \end{aligned}$$

V. The Third Attack

Now, in this section, we present our third attack. Suppose that we are given k moduli of the form $N_i = p_i^2 q_i$. We consider the scenario of the system of generalized key equations satisfying $e_i x_i - N_i y = (ap_i^2 + bq_i^2) z_i$. We use the combination of simultaneous Diophantine approximation and the LLL algorithm to acquire the small unknown parameters of (y, x_i) in order to recover prime factor p_i and q_i from every moduli $N_i = p_i^2 q_i$ simultaneously. This attack is for fixed value of y instead of fixed value of x from the previous attack. In short, we are looking for k integers x_i and an integer y. Thus, we come up with the following theorem.

Theorem 7. *Suppose that* $k \geq 2$, $N_i = p_i^2 q_i$, $1 \leq i \leq k$ *be* k *moduli each with the same size* N *where* $N = \max N_i$. *Assume for* $i = 1, ..., k$ *be* k *public exponents* e_i *with* $\min e_i = N^\beta$. *Define* $\delta = \beta k - \frac{5k}{6} - \alpha k$. *Let* $ap_i^2 + bq_i^2 < N^{\frac{2}{3}+\alpha}$ *where* $0 < \alpha < 1/3$ *and* $\gcd(a, b) = 1$. *If there exist an integer* $y < N^\delta$, k *integers* $x_i < N^\delta$ *and* $1 \leq |z_i| < \frac{\sqrt{2}N^{1/2}}{|ap_i^2 - bq_i^2|}$ *such that* $e_i x_i - N_i y = (ap_i^2 + bq_i^2) z_i$, *then the* k *moduli* $N_i = p_i^2 q_i$ *can be factored in polynomial time.*

Proof. Suppose $i = 1, ..., k$ with $k \geq 2$, from the equation $e_i x_i - N_i y = (ap_i^2 + bq_i^2) z_i$, we have

$$\left| \frac{N_i}{e_i} y - x_i \right| = \frac{|(ap_i^2 + bq_i^2) z_i|}{e_i} \tag{4}$$

Let $N = \max N_i$ and suppose that $y < N^\delta$ and $|z_i| < \frac{\sqrt{2}N^{1/2}}{|ap_i^2 - bq_i^2|}$ and $\min e_i = N^\beta$. We set $|ap_i^2 - bq_i^2| > p_i$, then we use the relation $N^{1/3} < p < 2^{1/3} N^{1/3}$ and $ap_i^2 + bq_i^2 < N^{\frac{2}{3}+\alpha}$

where $0 < \alpha < 1/3$, we have

$$\begin{aligned}\frac{|(ap_i^2 + bq_i^2)z_i|}{e_i} &\leq \frac{(ap_i^2 + bq_i^2)|z_i|}{N^\beta} \\ &< \frac{(N^{\frac{2}{3}+\alpha})\left(\frac{\sqrt{2}N^{1/2}}{|ap_i^2 - bq_i^2|}\right)}{N^\beta} \\ &< \frac{2^{1/2}N^{\frac{5}{6}+\alpha}}{N^\beta} \\ &= 2^{1/2}N^{\frac{5}{6}+\alpha-\beta} \qquad (5)\end{aligned}$$

By applying Theorem 4, we substitute (5) in (4), we obtain

$$\left|\frac{N_i}{e_i}y - x_i\right| < 2^{1/2}N^{\frac{5}{6}+\alpha-\beta}.$$

We can see the relation between $\left|\frac{N_i}{e_i}y - x_i\right| < 2^{1/2}N^{\frac{5}{6}+\alpha-\beta}$ and $|q\alpha_i - p_i| < \varepsilon$ which is the condition of Theorem 4.

Next, we need to show the existence of integer y and the integers x_i. Let $\varepsilon = 2^{1/2}N^{\frac{5}{6}+\alpha-\beta}$, $\delta = \beta k - \frac{5k}{6} - \alpha k$. Then, we obtain

$$\begin{aligned}N^\delta \cdot \varepsilon^k &= N^\delta(2^{1/2}N^{\frac{5}{6}+\alpha-\beta})^k \\ &= 2^{k/2}(N^{\delta+\frac{5}{6}k+\alpha k-\beta k}) \\ &= 2^{k/2}.\end{aligned}$$

Since $2^{2^{k/2}} < 2^{\frac{k(k-3)}{4}} \cdot 3^k$ for $k \geq 2$, then by applying Theorem 4, we have $N^\delta \cdot \varepsilon^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k$. It follows that if $y < N^\delta$, then $y < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \varepsilon^{-k}$.
Summarizing for $i = 1, ..., k$, we get

$$\left|\frac{N_i}{e_i}y - x_i\right| < \varepsilon \quad \text{and} \quad y < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \varepsilon^{-k},$$

for $i = 1, ..., k$.

It follows the condition of Theorem 4 are fulfilled will find y and x_i for $i = 1, ..., k$ using the LLL algorithm.

Next, by using the equation $e_i x_i - N_i y = (ap_i^2 + bq_i^2)z_i$ and since $1 < |z_i| < \frac{\sqrt{2}N^{1/2}}{|ap_i^2 - bq_i^2|}$ and this implies that $abZ^2q = \left[\frac{S^2}{4N}\right]$ for $S_i = e_i x_i - N_i y$ for every $i = 1, ..., k$, we compute $q_i = \gcd\left(\left[\frac{S_i^2}{4N_i}\right], N_i\right)$. Therefore, it is possible to factor k moduli of the form $N_i = p_i^2 q_i$. This terminates the proof. □

Example 3. *To illustrate our third attack, we consider three moduli and three public exponents as follows*

$$\begin{aligned}N_1 &= 27303248661520705484694992809, \\ N_2 &= 41780032879859661519245731019, \\ N_3 &= 37592432260341225657259451123, \\ e_1 &= 18259248695049659113144738243, \\ e_2 &= 32208520489776939471112369809, \\ e_3 &= 27061924816296042842613508448 5.\end{aligned}$$

Then, $N = \max(N_1, N_2, N_3) = 41780032879859661519245731019$. *We also obtain* $\min(e_1, e_2, e_3) = N^\beta$ *with* $\beta \approx 0.9874397727$. *If* $k = 3$, *then we have* $\delta = \beta k - \frac{5k}{6} - \alpha k = 0.3623193180$ *and* $\varepsilon = 2^{1/2}N^{\frac{5}{6}+\alpha-\beta} \approx 0.000494164679491052$.

Again, following the work in [Nitaj et al. (2014), Appendix A, page 196], suppose the value $n = k = 3$, *then we have the following parameter* C

$$C = \left[3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1}\right] = 679153932326420.$$

Consider the matrix that spanned the lattice $\mathcal{L}$ *as follows.*

$$M = \begin{bmatrix} 1 & -[\frac{Ce_1}{N_1}] & -[\frac{Ce_2}{N_2}] & -[\frac{Ce_3}{N_3}] \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}.$$

From here, we execute the LLL algorithm upon $\mathcal{L}$, *which gives a reduced basis with the matrix*

$$K = \begin{bmatrix} -1009511951 & -724069510 & -118463291 & -963514093 \\ -116219833917 & 219478836730 & 233252159583 & -70657952571 \\ 169220144359 & 236001315130 & -147703508721 & -337730794043 \\ -722863969416 & 480683724660 & -732230635836 & 486975914092 \end{bmatrix}.$$

Now, we obtain

$$K \cdot M^{-1} = \begin{bmatrix} -1009511951 & -1509533951 & -1309511951 & -140233963 \\ -116219833917 & -173784753022 & -150757265733 & -16144403118 \\ 169220144359 & 253036680596 & 219507853442 & 23506815783 \\ -722863969416 & -1080906177195 & -937679842185 & -100414937179 \end{bmatrix}.$$

Note that, we deduce the integers $y = 1009511951$, $x_1 = 1509533951$, $x_2 = 1309511951$ *and* $x_3 = 140233963$ *from the first row, respectively.*

By applying y *and* x_i *for* $i = 1, 2, 3$, *define* $S_i = e_i x_i - N_i y$ *is an approximation of* $ap_i^2 + bq_i^2$. *Hence, by using Lemma 2 and Theorem 5, this implies that* $abZ^2 q = \left\lfloor \frac{S^2}{4N} \right\rfloor$ *for* $S_i = e_i x_i - N_i y$. *Then, we get*

$$\begin{aligned} S_1 &= 41517689924272027734, \\ S_2 &= 55131885559405179290, \\ S_3 &= 51383529854302493082. \end{aligned}$$

Next, for each $i = 1, 2, 3$, *we find*

$$\begin{aligned} \left\lfloor \frac{S_1^2}{4N_1} \right\rfloor &= 15783090486, \\ \left\lfloor \frac{S_2^2}{4N_2} \right\rfloor &= 18187664034, \\ \left\lfloor \frac{S_3^2}{4N_3} \right\rfloor &= 17558501682. \end{aligned}$$

Next, we compute $q_i = \gcd\left(\left\lfloor \frac{S_i^2}{4N_i} \right\rfloor, N_i\right)$ *for every* $i = 1, 2, 3$, *thus, obtains*

$$\begin{aligned} q_1 &= 2630515081, \\ q_2 &= 3031277339, \\ q_3 &= 2926416947. \end{aligned}$$

This leads us to the factorization of three moduli N_1, N_2 *and* N_3 *which*

$$\begin{aligned} p_1 &= 3221712367, \\ p_2 &= 3712543511, \\ p_3 &= 3584116447. \end{aligned}$$

VI. Conclusion

In conclusion, we proposed three new attacks on the modulus of the form $N = p^2 q$. For the first attack, if e satisfying the generalized key equation $eX - NY = (ap^2 + bq^2)Z$ such that $|ap^2 - bq^2| < N^{1/2}$, then the modulus $N = p^2 q$ can be factored in polynomial time using continued fraction expansion together with some restrictions on some parameters. We have successfully proved the existence of probabilistic polynomial time algorithm which output factor p and q and the scenario of weak conditions that would enable the factoring $N = p^2 q$ to be easy. One can run the proposed algorithm to test whether the key belongs to the corresponding weak class or not to ensure that one does not accidentally create a weak key during key generation process. Then, we focused on the system of generalized key equations of the form $e_i x - N_i y_i = (ap_i^2 + bq_i^2)z_i$ and $e_i x_i - N_i y = (ap_i^2 + bq_i^2)z_i$ for the second and third attack respectively. If x, x_i, y, y_i and z_i are suitably small, then the second and third attacks showed that the k moduli $N_i = p_i^2 q_i$ can be factored simultaneously in polynomial time using the combination of simultaneous Diophantine approximation and the LLL algorithm.

Acknowledgements

The present research was partially supported by the Putra Grant with Project Number GP/2017/9552200.

References

[1] Muhammad Rezal Kamel Ariffin et al. "A New Efficient Asymmetric Cryptosystem Based on the Integer Factorization Problem of $N = p^2q$". In: *Malaysian Journal of Mathematical Sciences* 7.S (2013), pp. 19–37.

[2] M. A. Asbullah and M. R. K. Ariffin. "Analysis on the AA_β Cryptosystem". In: *the 5th International Cryptology and Information Security Conference 2016 (Cryptology2016)*. 2016, pp. 41–48.

[3] M. A. Asbullah and M. R. K. Ariffin. "Design of Rabin-like Cryptosystem Without Decryption Failure". In: *Malaysian Journal of Mathematical Sciences* 10S (2016), pp. 1–18.

[4] M. A. Asbullah and M. R. K. Ariffin. "New attack on RSA with modulus $N = p^2q$ using continued fractions". In: *Journal of Physics* 622 (2015), pp. 191–199.

[5] MA Asbullah and MRK Ariffin. "Comparative Analysis of Three Asymmetric Encryption Schemes Based Upon the Intractability of Square Roots Modulo $N = p^2q$". In: *4th International Cryptology and Information Security Conference (CRYPTOLOGY2014)*. 2014.

[6] Muhammad Asyraf Asbullah and Muhammad Rezal Kamel Ariffin. "Another Proof Of Wiener's Short Secret Exponent". In: *Malaysian Journal of Science* 1.1 (2019), pp. 62–68.

[7] Muhammad Asyraf Asbullah, Muhammad Rezal Kamel Ariffin, and Zahari Mahad. "Analysis on the Rabin-p cryptosystem". In: *AIP Conference Proceedings*. Vol. 1787. 1. AIP Publishing. 2016, p. 080012.

[8] J. Blömer and A. May. "A generalized Wiener attack on RSA". In: *Practice and Theory in PublicKey Cryptography PKC 2004 LNCS Springer-Verlag* 2947 (2004), pp. 1–13.

[9] D. Boneh and G. Durfee. "Cryptanalysis of RSA with private key d less than $N^{0.292}$". In: *Advance in Cryptology-Eurocrypt'99, Lecture Notes in Computer Science* 1592 (1999), pp. 1–11.

[10] Dan Boneh, Glenn Durfee, and Nick Howgrave-Graham. "Factoring $N = p^rq$ for Large r". In: *Annual International Cryptology Conference*. Springer. 1999, pp. 326–337.

[11] J.W.S. Cassels. *Introduction to the Geometry of Numbers*. Springer-Verlag Berlin Heidelberg, 1971.

[12] W. Diffie and Hellman. "New directions in cryptography". In: *IEEE Transactions On Information Theory* 22.6 (1976), pp. 644–654.

[13] Atsushi Fujioka, Tatsuaki Okamoto, and Shoji Miyaguchi. "ESIGN: An Efficient Digital Signature Implementation for Smart Cards". In: *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer. 1991, pp. 446–457.

[14] G. Hardy and E. Wright. "An Introduction to the Theory of Numbers". In: Oxford University Press, London, 1965.

[15] J. Hinek. "On the security of some variants of RSA". PhD thesis. Waterloo, Ontario, Canada, 2007.

[16] M Jason Hinek. "Cryptanalysis of RSA and Its Variants". In: CRC press, 2009.

[17] A. K. Lenstra, H. W. Lenstra, and L. Lovász. "Factoring polynomials with rational coefficients". In: *Mathematische Annalen* 261 (1982), pp. 513–534.

[18] A. May. "Secret exponent attacks on RSA-type scheme with moduli $N = p^rq$". In: *In PKC 2004 LNCS Springer-Verlag* 2947 (2004), pp. 218–230.

[19] M. Nishioka, H. Satoh, and K. Sakurai. "Design and Analysis of Fast Provably Secure Public-Key Cryptosystems Based on A Modular Squaring". In: Springer, Berlin, Heidelberg. 2001, pp. 81–102.

[20] A. Nitaj et al. "New attacks on the RSA cryptosystem". In: *Progress in Cryptology-AFRICACRYPT 2014*. Vol. 8469. Lecture Notes in Computer Science. Springer-Verlag, 2014, pp. 178–198.

[21] T. Okamoto and S. Uchiyama. "A New Public-Key Cryptosystem As Secure As Factoring". In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 1998, pp. 308–318.

[22] René Peralta and Eiji Okamoto. "Faster Factoring of Integers of a Special Form". In: *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 79.4 (1996), pp. 489–493.

[23] Normahirah Nek Abd Rahman et al. "New Vulnerability on System of $Ni = p_i^2 q_i$ Using Good Approximation of $\phi(N)$". In: *Cryptology and Information Security Conference 2018* (2018), p. 139.

[24] R. Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems". In: *Communication of the ACM 21(2)* 21(2) (1978), pp. 17–28.

[25] S. Sarkar. "Small secret exponent attack on RSA variant with modulus $N = p^2q$". In: *Designs, Codes and Cryptography* 73.2 (2014), pp. 383–392.

[26] S. Sarkar and S Maitra. "Cryptanalysis of RSA with two decryption exponents". In: *Information Processing Letters* 110(5) (2010), pp. 178–181.

[27] T. Takagi. "Fast RSA-type cryptosystem modulo p^kq". In: *Annual International Cryptology Conference* (1998), pp. 318–326.

[28] M. Wiener. "Cryptanalysis of short RSA secret exponents". In: *IEEE Transaction on Information Theory IT-36* 36 (1990), pp. 553–558.