International Journal of Cryptology Research 8(1): 17 - 32 (2018)

New Cryptanalysis of Multiple Moduli $N_i = p_i^2 q_i$ Using Good Approximation of $\phi(N_i)$

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

[1]*Pusat PERMATApintar Negara, Universiti Kebangsaan Malaysia , 43600 UKM Bangi, Selangor, Malaysia.*
[2]*Al-Kindi Cryptography Research Laboratory, 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.*

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

ABSTRACT

By using the term $N - 2N^{2/3} - N^{1/3}$ as a good approximation of $\phi(N)$ and then applying the LLL algorithm enable one to factor m moduli of the form $N_i = p_i^2 q_i$ simultaneously. This paper presents another attacks work when m public keys (N_i, e_i) for $i = 1, ..., m$ and $m \geq 2$ if there exist m relations of the form $e_i d - k_i \phi(N_i) = 1$ or $e_i d_i - k\phi(N_i) = 1$ with the parameters d, d_i, k and k_i are suitably small.

Keywords: Factorization, LLL algorithm, Simultaneous Diophantine approximations

1 INTRODUCTION

The RSA Cryptosystem, named after its great inventors Rivest et al. (1978) become a well-known public key cryptosystem for assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage. In recent years, RSA is an extremely well-research area in cryptography. Since its publication, the RSA Cryptosystem has been analyzed and the simple structure of the RSA cryptosystem has also attracted many cryptanalysts.

Basically, by multiplying two large primes are computationally easy to compute but factoring the resulting product is very hard. The mathematical operations in RSA depend on three parameters, the modulus $N = pq$, the public exponent e and the private exponent d, related by the congruence relation $ed \equiv 1 \pmod{\phi(N)}$ where $\phi(N) = (p-1)(q-1)$. Hence, the difficulty of breaking the RSA cryptosystem is based on three hard mathematical problems which is the integers factorization problem of $N = pq$, the e-th root problem from the congruence relation given by $C \equiv M^e \pmod{N}$ and to solve the Diophantine key equation $ed + 1 = \phi(N)k$. That is, to solve the key equation which contain three variables which is $d, \phi(N)$ and k (Menezes et al. (1997)).

In 1990, Wiener (1990) proved that if the secret exponent $d < \frac{1}{3}N^{1/4}$ based on the convergent of the continued fraction expansion of $\frac{e}{N}$ making RSA totally insecure. Wiener was able to obtain the integer solution of the Diophantine key equation and eventually factoring N through the continued fraction of $\frac{e}{N}$. Furthering this, Boneh and Durfee (1999) came up an attack on RSA by applying Coppersmiths lattice reduction based method to improve the bound to $d < N^{0.292}$.

Later, de Weger (2002) proposed and extension of these attacks with small difference between its prime factors. They showed that by choosing an RSA modulus with a small difference of its prime factors yield improvement on the small private exponent attacks of Wiener and Boneh and Durfee. As studied by de Weger, if the difference between p and q is small, then $N - 2\sqrt{N} + 1$ is better approximation to $\phi(N)$ instead of N. Hence, $\frac{k}{d}$ is one of the convergent of the continued fractions expansion of $\frac{e}{N-2\sqrt{N}+1}$.

On different setting, Maitra and Sarkar (2008) consider the case that p and $2q$ are too close which is the difference between $2q$ and p is small. They apply $N - \frac{3}{2}\sqrt{N} + 1$ as a good approximation to $\phi(N)$ instead of N. Hence, in their studied revealed that $\frac{k}{d}$ is one of the convergent of the continued fractions expansion of $\frac{e}{N-\frac{3}{2}\sqrt{N}+1}$. Over the past few years, we have witnessed steady progress toward cryptanalysis using the continued fraction expansion as a tool. For instance, Asbullah and Ariffin (2016a,b) and Bunder and Tonien (2017).

In general, the use of short secret exponent encounters serious security problem in various instances of RSA. As the work that has been introduced by Howgrave-Graham and Seifert (1999) showed an extension of Wieners attack that allows the RSA system to be insecure in the presence of two decryption exponents (d_1, d_2) with $d_1, d_2 < N^{\frac{5}{14}}$. In the presence of three decryption exponents, they improved the bound to $N^{\frac{2}{5}}$.

As studied by Hinek (2007) showed that it is possible to factor the k modulus N_i using equations $e_i d - k_i \phi(N_i) = 1$ if $d < N^{\delta}$ with $\delta = \frac{k}{2(k+1)} - \epsilon$ where ϵ is a small constant depending on the size of $\max N_i$. Later on, Nitaj et al. (2014) presented new method to factor all the RSA moduli $N_1, ..., N_k$ in the scenario that RSA instances satisfy k equations of the form $e_i x - y_i \phi(N_i) = z_i$ or $e_i x_i - y\phi(N_i) = z_i$ with suitable parameters x, x_i, y, y_i and z_i, $\phi(N_i) = (p_i - 1)(q_i - 1)$ based on the LLL algorithm, the idea from Lenstra et al. (1982) for lattice basis reduction.

As described in May (2004) the modulus of the form $N = p^2 q$ is frequently used in cryptography. For example Takagi (1998) showed that the decryption process is about three times faster than RSA cryptosystem by using the RSA modulus of the form $N = p^2 q$. On the other hand, the HIME(R) cryptosystem (Nishioka et al., 2002) became a standard in Japan because it was able to encapsulate and sends more data securely than the original RSA cryptosystem.

Additionally, the AA_β cryptosystem (Ariffin et al., 2013) incorporating the hardness of factoring integer $N = p^2 q$ coupled with the square root problem as its cryptographic primitive which gives advantage for encryption without "expensive" mathematical operation. Recently, by incorporating the modulus $N = p^2 q$, a variant of Rabin cryptosystem succesfully eliminate the decryption failure which was due to a 4-to-1 mapping scenario (Asbullah and Ariffin,

2016a).

In 2015, motivated from de Weger's generalization attack and Maitra and Sarkars attack, Asbullah and Ariffin (2015) proposed new attack on RSA-type modulus $N = p^2q$ using the term $N - 2N^{2/3} - N^{1/3}$ as a good approximation to $\phi(N)$ satisfying the equation $ed - k\phi(N) = 1$. Hence, they showed that $\frac{k}{d}$ is one of the convergent of the continued fractions expansion of $\frac{e}{N-2N^{2/3}-N^{1/3}}$ and later led to the factorization of $N = p^2q$ in polynomial time.

Our contribution. In this work, we will look at a variant of the RSA modulus of the form $N = p^2q$. A new cryptanalysis to factor m moduli of the form $N_i = p_i^2q_i$ for $i = 1, ..., m$ by using the term $N - 2N^{2/3} - N^{1/3}$ as a good approximation of $\phi(N)$ will be introduced satisfy the key equation $ed - k\phi(N) = 1$. Both cryptanalysis are upon m-instances (N_i, e_i).

The first cryptanalysis works when there exist an integer d and m integers k_i satisfy $e_id - k_i\phi(N_i) = 1$. We prove that m moduli $N_i = p_i^2q_i$ can be factored in polynomial time satisfy $d < N^{\delta}, k_i < N^{\delta}$ where $\delta = \frac{m(1-\beta)}{1+m}$, $\beta < 2/3$ and $N = \min N_i$.

For the second cryptanalysis, we show that m moduli $N_i = p_i^2q_i$ can be factored in polynomial time if $d_i < N^{\delta}, k < N^{\delta}$ where $\delta = \frac{m(\alpha-\beta)}{m+1}, \beta < 2/3, N = \max N_i$ and $\min e_i = N^{\alpha}$ if there exist an integer k and m integers d_i satisfy $e_id_i - k\phi(N_i) = 1$.

For both cryptanalysis, we transform the equations into a simultaneous Diophantine problem and then we apply lattice basis reduction techniques to find parameters (d, k_i) or (k, d_i) in order to compute the prime factor p_i and q_i of each $N_i = p_i^2q_i$ simultaneously.

The layout of the paper is as follows. In Section 2, we begin with a brief review on lattice basic reduction, simultaneous Diophantine approximation and also some useful results that will be used throughout the paper. In Sections 3 and 4 we present our first and second cryptanalysis consecutively together with examples. Then, we conclude the paper in Section 5.

2 PRELIMINARIES

2.1 Lattice Basis Reductions

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

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

The set $(u_1, ..., u_d)$ is called a basis of $\mathcal{L}$ and d is its dimension. The determinant of $\mathcal{L}$ is defined as $\det(\mathcal{L}) = \sqrt{\det(U^T U)}$ where U is the matrix of the u_i's in the canonical basis of $\mathbb{R}^n$. Define $\|v\|$ to be the Euclidean norm of a vector $v \in \mathcal{L}$. A central problem in lattice reduction is to find a short non-zero vector in $\mathcal{L}$. The LLL algorithm of Lenstra et al. (1982) produces a reduced basis and the following result fixes the sizes of the reduced basis vector (see May (2003)).

Theorem 2.1. *Let $\mathcal{L}$ be a lattice of dimension ω with a basis $\{v_1, ..., v_\omega\}$. The LLL algorithm produces a reduced basis $\{b_1, ..., b_\omega\}$ satisfying*

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

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

One of the important application that the LLL algorithm provided is a way to solve the simultaneous Diophantine approximations problem. Lenstra, Lenstra and Lovász proposed a way to compute simultaneous Diophantine approximations to rational numbers. They considered a lattice with real entries as shown in the following proposition (Lenstra et al., 1982).

Proposition 2.1. *(Lenstra et al., 1982). There exists a polynomial time algorithm that, given a positive integer n and rational numbers $\alpha_1, \alpha_2, ..., \alpha_n$ and ε satisfy $0 < \varepsilon < 1$, finds integers $p_1, p_2, ..., p_n$,q for which*

$$|q\alpha_i - p_i| < \varepsilon, \quad 1 \leq q \leq 2^{n(n+1)/4} \varepsilon^{-n} \text{ for } 1 \leq i \leq n.$$

The above proposition follows immediately from the following classical theorem of Dirichlet (Cassels (2012), Section V.10).

Theorem 2.1. (Dirichlet Theorem). *Let $\vartheta_1, ..., \vartheta_n$ 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*

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

As studied by Nitaj et al. (2014) revealed a similar result for a lattice with integer entries as shown in the following theorem.

Theorem 2.2. (Simultaneous Diophantine Approximations). *(Nitaj et al., 2014). There is a polynomial time algorithm, for given rational numbers $\alpha_1, ..., \alpha_n$ and $0 < \varepsilon < 1$, to compute integers $p_1, ..., p_n$ and a positive integer q such that*

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

Next, we introduce some useful lemmas and theorem proposed by Asbullah and Ariffin (2015) that have been used throughout this paper.

Lemma 2.1. *(Asbullah and Ariffin, 2015). Let $N = p^2q$ with $q < p < 2q$. Then*

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

Let $N = p^2q$ with $q < p < 2q$. Then $\phi(N) = N - (p^2 + pq - p)$. The following result gives an interval for $N - \phi(N) = p^2 + pq - p$ in terms of N. It shows that if $p \approx q$, then $N - 2N^{2/3} - N^{1/3}$ is a good approximation to $\phi(N)$ while if $p \approx 2q$, then $N - \left((2^{2/3} + 2^{-1/3})N^{2/3} + 2^{1/3}N^{1/3}\right)$ is a good approximation to $\phi(N)$.

Lemma 2.2. *(Asbullah and Ariffin, 2015) Let $N = p^2q$ and $\phi(N) = N - (p^2 + pq - p)$ with $q < p < 2q$. Then*

$$2N^{2/3} - N^{1/3} < N - \phi(N) < (2^{2/3} + 2^{-1/3})N^{2/3} - 2^{1/3}N^{1/3}$$

and

$$|N - (2N^{2/3} - N^{1/3}) - \phi(N)| < 2p^{5/3}|p^{1/3} - q^{1/3}|$$

Theorem 2.3. *(Asbullah and Ariffin, 2015). Let $N = p^2 q$ be an RSA modulus with $q < p < 2q$. Let $1 < e < \phi(N) < N - (2N^{2/3} - N^{1/3})$ satisfying $ed - k\phi(N) = 1$ for some unknown integers $\phi(N)$, d and k. Assume $\phi(N) > \frac{2}{3}N$ and $N > 6d$. Let $2p^{5/3}|p^{1/3} - q^{1/3}| < \frac{1}{3}N^{\beta}$ and $d < N^{\delta}$. If $\delta < N^{\frac{1-\beta}{2}}$, then $\left|\frac{e}{N-(2N^{2/3}-N^{1/3})} - \frac{k}{d}\right| < \frac{1}{2d^2}$.*

3 THE FIRST CRYPTANALYSIS ON m MODULI $N_i = p_i^2 q_i$

In this section, we propose our first attack. We extend the result proposed by Asbullah (2015) as in Theorem 2.3 which is the basis of our analysis. The following theorem proved that we are given m moduli of the form $N_i = p_i^2 q_i$. We consider in this scenario given $e_i d - k_i \phi(N_i) = 1$ with fixed d and the term $N - (2N^{2/3} - N^{1/3})$ as a good approximation of $\phi(N_i)$ satisfy the key equation. Then, we transform the equation into simultaneous Diophantine approximation problem and apply lattice basis reduction algorithm in order to obtain the parameter (d, k_i). Later, we compute the prime factor p_i and q_i of each $N_i = p_i^2 q_i$ simultaneously in polynomial time.

Theorem 3.1. *Suppose that $m \geq 2$, $N_i = p_i^2 q_i$ for $i = 1, ..., m$ be m moduli each with the same size N where $N = \min N_i$. Assume e_i, $i = 1, ..., m$ be m public exponents. Let $\Phi = 2N^{2/3} - N^{1/3}$, $1 < e < \phi(N_i) < N_i - \Phi$. Define $\delta = \frac{m(1-\beta)}{m+1}$. If there exist an integer $d < N^{\delta}$ and m integers $k_i < N^{\delta}$ such that $e_i d - k_i \phi(N_i) = 1$, then it is possible to factor m moduli $N_i = p_i^2 q_i$ in polynomial time.*

Proof. Suppose $m \geq 2$ and $i = 1, ..., m$, the equation $e_i d - \phi(N_i) k_i = 1$ can be written as $e_i d - k_i(N_i - \Phi) = 1 - k_i(N_i - \phi(N_i) - \Phi)$. Hence,

$$\left|\frac{e_i}{N_i - \Phi} d - k_i\right| = \frac{|1 - k_i(N_i - \phi(N_i) - \Phi)|}{N_i - \Phi} \tag{1}$$

Let $N = \min N_i$ and suppose that $k_i < N^{\delta}$ and $(2N^{2/3} - N^{1/3}) < p^2 + \frac{N}{p} - p < \left((2^{2/3} + 2^{-1/3})N^{2/3} - 2^{1/3}N^{1/3}\right)$, we will get,

$$\begin{aligned}
\frac{|1-k_i(N_i-\phi(N_i)-\Phi)|}{N_i-\Phi} &\leq \frac{|1+k_i(N_i-\phi(N_i)-\Phi)|}{N-\Phi} \\
&< \frac{1+N^{\delta}\Big(N-(2N^{2/3}-N^{1/3})-\phi(N)\Big)}{\phi(N)} \\
&< \frac{1+N^{\delta}(2p^{5/3}|p^{1/3}-q^{1/3}|)}{\phi(N)} \\
&< \frac{N^{\delta}(\frac{1}{6}N^{\beta})}{\frac{2}{3}N} \\
&= \frac{1}{4}N^{\beta-1+\delta} \qquad (2)
\end{aligned}$$

By applying Theorem 2.2, we substitute (2) in (1). Then, we obtain

$$\left|\frac{e_i}{N_i-\Phi}d-k_i\right| < \frac{1}{4}N^{\beta-1+\delta}.$$

We can see clearly the relation between $\left|\frac{e_i}{N_i-\Phi}d-k_i\right| < \frac{1}{4}N^{\beta-1+\delta}$ and $|q\alpha_i - p_i| < \varepsilon$ which is the condition in Theorem 2.2.

Now, we proceed to show the existence of integer d and the integers k_i. We assume $\varepsilon = \frac{1}{4}N^{\beta-1+\delta}$ and $\delta = \frac{m(1-\beta)}{m+1}$. We have

$$N^{\delta}\cdot\varepsilon^m = \left(\frac{1}{4}\right)^m \cdot N^{m\beta-m+\delta m+\delta} = \left(\frac{1}{4}\right)^m.$$

Since $\left(\frac{1}{4}\right)^m < 2^{\frac{m(m-3)}{4}}\cdot 3^m$ for $m \geq 2$, we get $N^{\delta}\cdot\varepsilon^m < 2^{\frac{m(m-3)}{4}}\cdot 3^m$ by applying Theorem 2.2. It follows that if $d < N^{\delta}$, then $d < 2^{\frac{m(m-3)}{4}}\cdot 3^m \cdot \varepsilon^{-m}$.

Summarizing for $i = 1, ..., m$, we have

$$\left|\frac{e_i}{N_i-\Phi}d-k_i\right| < \varepsilon \text{ and } d < 2^{\frac{m(m-3)}{4}}\cdot 3^m\cdot\varepsilon^{-m}.$$

If the conditions of Theorem 2.2 are fulfilled, then this lead us to find d and k_i for $i = 1, ..., m$ by using the LLL algorithm.

Next, we look at the relation $\frac{e_i d-1}{k_i} = \phi(N_i) = p_i(p_i-1)(q_i-1)$ of the equation $e_i d - k_i\phi(N_i) = 1$. We can compute $\gcd\left(\frac{e_i d-1}{k_i}, N_i\right)$ which later give the prime factor p_i and q_i. This leads to the factorization of m moduli of the form $N_i = p_i^2 q_i$ simultaneously. This terminates the proof. ■

Example 3.1. To illustrate our first cryptanalysis, we consider the three moduli and three public exponents as follows:

$$\begin{aligned}
N_1 &= 26351611350368084214986274421695222512032 9,\\
N_2 &= 12836556371738013360487076838163890708671 3,\\
N_3 &= 18798168063383867201101496195943909824651 9,\\
e_1 &= 80792911443410905692392637406380886780007,\\
e_2 &= 12357813699220091827360709482999496142264 7,\\
e_3 &= 20961451900454998790761026472974297795827.
\end{aligned}$$

Then, $N = \min(N_1, N_2, N_3) = 12836556371738013360487076838163890708671 3$. If $m = 3$ and $\beta < 2/3$, we have $\delta = \frac{m(1-\beta)}{m+1} = \frac{3}{8}$ and $\varepsilon = \frac{1}{4}N^{\beta-1+\delta} \approx 0.000001817121$.

Suppose that we consider the parameter C as defined in [Nitaj et al. (2014), Appendix A, page 196], $n = m = 3$, leads to

$$C = \left\lfloor 3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1} \right\rfloor = 37146615860448694728804 25.$$

Now, we consider the lattice $\mathcal{L}$ spanned by the rows of the matrix

$$M = \begin{bmatrix} 1 & -\left\lfloor \frac{C*e_1}{N_1-\Phi} \right\rceil & -\left\lfloor \frac{Ce_2}{N_2-\Phi} \right\rceil & -\left\lfloor \frac{Ce_3}{N_3-\Phi} \right\rceil \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}.$$

Then, the LLL algorithm is applied to lattice $\mathcal{L}$ leads to the reduced basis together with the matrix as follows.

$$K = \begin{bmatrix} 531150414983 & 301257228587 & 499463626192 & 178001942286 \\ -168389513847154765291 & -51627503530491328427 & -162109383604390765943 & -18776769540238268234 \\ 124074656146938841057 & 38040758013500360884 & 119447259923583684692 & 13835310590480351043 \\ 100588675112833001015 & 30840056847179847024 & 96837194594698950848 & 11216436984704075968 \end{bmatrix}.$$

We obtain
$K \cdot M^{-1}$

$$= \begin{bmatrix} 531150414983 & 162848441677 & 511341023600 & 59227494073 \\ -294151413649686019969 & -90185563220300129309 & -283180960997331683543 & -32800221212401676852 \\ 52224763545169658695 & 16011888761402698006 & 50277027552185434292 & 5823476337553763421 \\ 135845721544043483999 & 41649716234605959720 & 130779320408203043648 & 15147877965697829272 \end{bmatrix}.$$

According to the first row of the above matrix, we have

$$d = 531150414983,\ \ k_1 = 162848441677,\ \ k_2 = 511341023600,\ \ k_3 = 59227494073.$$

By applying d and k_i for $i = 1, 2, 3$, we look at the relation $\frac{e_i d-1}{k_i} = \phi(N_i) = p_i(p_i - 1)(q_i - 1)$ of the equation $e_i d - k_i\phi(N_i) = 1$, we get

$$\frac{e_1 d - 1}{k_1} = 263516113503672185830235590020192839191440,$$

$$\frac{e_2 d - 1}{k_2} = 128365563717374975692327918192177017411200,$$

$$\frac{e_3 d - 1}{k_3} = 187981680633832049824018263550877466963780.$$

Then, for each $i = 1, 2, 3$, we find $p_i = \gcd\left(\frac{e_i d-1}{k_i}, N_i\right)$ and we obtain

$$p_1 = 69904752761407,\ \ p_2 = 51738406927601,\ \ p_3 = 58282229331211.$$

It is possible to factor three moduli N_1, N_2 and N_3 since

$$q_1 = 53925448837321,\ \ q_2 = 47953733769113,\ \ q_3 = 55340517648239.$$

4 THE SECOND CRYPTANALYSIS ON m MODULI $N_i = p_i^2 q_i$

In this section, we propose our second cryptanalysis. Suppose that we are given m moduli $N_i = p_i^2 q_i$. We consider in this scenario that the following system of equation given by $e_i d_i - k\phi(N_i) = 1$ with fixed k will lead us the factor

of each moduli which are all of the same size. We show that it is possible to factor such moduli of the form $N_i = p_i^2 q_i$. This is achievable when the unknown parameters d_i and k are suitably small. We couple this information together with the execution of the LLL algorithm to achieve our objective since we use the term $N - 2N^{2/3} - N^{1/3}$ as a good approximation of $\phi(N)$ satisfy the key equation.

We prove the following theorem based on Theorem 2.3. We transform the key equation into the simultaneous Diophantine approximation and then we apply lattice basis reduction algorithm to find parameters (d_i, k) which later lead to the factorization of m moduli of the form $N_i = p_i^2 q_i$ simultaneously.

Theorem 4.1. *Suppose that $m \geq 2$ and $N_i = p_i^2 q_i$, for $i = 1, ..., m$ be m moduli each with the same size N where $N = \max N_i$. Assume e_i, $i = 1, ..., m$ be m public exponents with $min\ e_i = N^\alpha$ and $\Phi = 2N^{2/3} - N^{1/3}$, $1 < e < \phi(N_i) < N_i - \Phi$. Define $\delta = \frac{m(\alpha-\beta)}{m+1}$. If exist an integer $k < N^\delta$ and m integers $d_i < N^\delta$ such that $e_i d_i - \phi(N_i)k = 1$, then it is possible to factor m moduli of the form $N_i = p_i^2 q_i$ in polynomial time simultaneously.*

Proof. For $i = 1, ..., m$, starting with the equation $e_i d_i - k\phi(N_i) = 1$, we get

$$\Big|\frac{N_i - \Phi}{e_i}k - d_i\Big| = \frac{|1 - k(N_i - \phi(N_i) - \Phi)|}{e_i} \tag{3}$$

Let $N = \max N_i$ and suppose that $k_i < N^\delta$ and $(2N^{2/3} - N^{1/3}) < p^2 + \frac{N}{p} - p < \Big((2^{2/3} + 2^{-1/3})N^{2/3} + 2^{1/3}N^{1/3}\Big)$, we will get,

$$\begin{aligned}
\frac{|1 - k(N_i - \phi(N_i) - \Phi)|}{e_i} &\leq \frac{|1 + k(N_i - \phi(N_i) - \Phi)|}{N^\alpha} \\
&< \frac{1 + N^\delta\Big(N - (2N^{2/3} - N^{1/3}) - \phi(N)\Big)}{N^\alpha} \\
&< \frac{1 + N^\delta(2p^{5/3}|p^{1/3} - q^{1/3}|)}{N^\alpha} \\
&< \frac{N^\delta(\frac{1}{6}N^\beta)}{N^\alpha} \\
&= \frac{1}{6}N^{\beta+\delta-\alpha}
\end{aligned} \tag{4}$$

By applying Theorem 2.2, we substitute (4) in (3). Then, we obtain

$$\left|\frac{N_i - \Phi}{e_i}k - d_i\right| < \frac{1}{6}N^{\beta+\delta-\alpha}.$$

We can see the relation between $\left|\frac{N_i-\Phi}{e_i}k - d_i\right| < \frac{1}{6}N^{\beta+\delta-\alpha}$ and $|q\alpha_i - p_i| < \varepsilon$ which is the condition of Theorem 2.2.

Now, we proceed to show the existence of integer k and the integers d_i. Let $\varepsilon = \frac{1}{6}N^{\beta+\delta-\alpha}$, $\delta = \frac{m(\alpha-\beta)}{m+1}$. We have

$$N^{\delta} \cdot \varepsilon^m = \left(\frac{1}{6}\right)^m \cdot N^{m\beta+m\delta-m\alpha+\delta} = \left(\frac{1}{6}\right)^m$$

Since $\left(\frac{1}{6}\right)^m < 2^{\frac{m(m-3)}{4}} \cdot 3^m$ for $m \geq 2$, we get $N^{\delta} \cdot \varepsilon^m < 2^{\frac{m(m-3)}{4}} \cdot 3^m$ by applying Theorem 2.2. It follows that if $k < N^{\delta}$, then $k < 2^{\frac{m(m-3)}{4}} \cdot 3^m \cdot \varepsilon^{-m}$.

Summarizing for $i = 1, ..., m$, we have

$$\left|\frac{N_i - \Phi}{e_i}k - d_i\right| < \varepsilon \text{ and } k < 2^{\frac{m(m-3)}{4}} \cdot 3^m \cdot \varepsilon^{-m}$$

If the conditions of Theorem 2.2 are fulfilled, then this lead us to find k and d_i for $i = 1, ..., m$ using the LLL algorithm.

Next, we look at the relation $\frac{e_i d_i - 1}{k} = \phi(N_i) = p_i(p_i - 1)(q_i - 1)$ of the equation $e_i d_i - k\phi(N_i) = 1$. We can compute $\gcd\left(\frac{e_i d_i - 1}{k}, N_i\right)$ which later give the prime factor p_i and q_i. This leads to the factorization of m moduli of the form $N_i = p_i^2 q_i$. This terminates the proof. ■

Example 4.1. As an illustration of this proposed cryptanalysis, we look at three moduli and three public exponents as follows

$$\begin{aligned}
N_1 &= 75008312957047469348732538527519866244681,\\
N_2 &= 12338264165663139224663164323591788316220 9,\\
N_3 &= 23664030208130335858435041461067030804 3781,\\
e_1 &= 31754220269884338669277120219619839718053,\\
e_2 &= 52233138249590873962310663900788852848217,\\
e_3 &= 18528757193747502685316067665844754428 1045.
\end{aligned}$$

Then, $N = \max(N_1, N_2, N_3) = 23664030208130335858435041461067030804 3781$. We also get $\min(e_1, e_2, e_3) = N^{\alpha}$ with $\alpha \approx 0.9789170642$. Since $m = 3$ and $\beta < 2/3$, we get $\delta = \frac{m(\alpha-\beta)}{m+1} = 0.3591877982$ and $\varepsilon = \frac{1}{6}N^{\beta+\delta-\alpha} \approx 0.000001854212$.

Suppose that we consider the parameter C as defined in [Nitaj et al. (2014), Appendix A, page 196], $n = m = 3$, leads to

$$C = \left\lfloor 3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1} \right\rfloor = 34262347530471320663 10644.$$

Next, we look at the lattice $\mathcal{L}$ spanned by the rows of the matrix

$$M = \begin{bmatrix} 1 & -\left\lfloor \frac{C(N_1-\Phi)}{e_1} \right\rfloor & -\left\lfloor \frac{C(N_2-\Phi)}{e_2} \right\rfloor & -\left\lfloor \frac{C(N_3-\Phi)}{e_3} \right\rfloor \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}.$$

Then, the LLL algorithm is applied to lattice $\mathcal{L}$ leads to the reduced basis together with the matrix as follows

$$K = \begin{bmatrix} -182524372654 & -146456473850 & -116350956196 & -161112380644 \\ -16683193846076224169 & -96006951081027194305 & -12803413578135971700 & 115420170547926858788 \\ -677461226345054183660 & 267316396489637852564 & 399791487973525630452 & 235778569220139902640 \\ 91011227434211881899 & -507503522055241331933 & 831338501094560594144 & -242139184242751706576 \end{bmatrix}.$$

Now, we obtain

$$K \cdot M^{-1} = \begin{bmatrix} -182524372654 & -431150415597 & -431150415607 & -233111277947 \\ -16683193846076224169 & -39408249186843288687 & -39408249187757314228 & -21306966193871351804 \\ -677461226345054183660 & -1600266775567642689324 & -1600266775604758895587 & -865220627451237659280 \\ 91011227434211881899 & 214982404605424684025 & 214982404610410934689 & 116235126444902519447 \end{bmatrix}.$$

According to the first row of the above matrix, we have

$$k = 182524372654, d_1 = 431150415597, d_2 = 431150415607, d_3 = 233111277947.$$

By using k and d_i for $i = 1, 2, 3$, we look at the relation $\frac{e_i d_i - 1}{k} = \phi(N_i) = p_i(p_i - 1)(q_i - 1)$ of the equation $e_i d_i - k\phi(N_i) = 1$, we get

$$\frac{e_1 d_1 - 1}{k} = 750083129570437719214489420712803093121 60,$$
$$\frac{e_2 d_2 - 1}{k} = 123382641656626251332238684396564345529200,$$
$$\frac{e_3 d_3 - 1}{k} = 236640302081295426831936822683007388436496.$$

Then, for each $i = 1, 2, 3$, we find $p_i = \gcd\left(\frac{e_i d_i - 1}{k}, N_i\right)$ and we obtain

$$p_1 = 45104908616699, \ \ p_2 = 53063352809947, \ \ p_3 = 65874665082797.$$

It is possible to factor three moduli N_1, N_2 and N_3 since

$$q_1 = 36869036060081, \ \ q_2 = 43819224726601, \ \ q_3 = 54532055826109.$$

5 CONCLUSION

In conclusion, this paper presents two new cryptanalysis on m moduli $N_i = p_i^2 q_i$ for $i = 1, ..., m$. We focus on the system of key equation of the form $e_i d - k_i \phi(N_i) = 1$ for the first cryptanalysis and the form $e_i d_i - k\phi(N_i) = 1$ for the second cryptanalysis. We show that both of cryptanalysis are successful when the parameters d, d_i, k and k_i are suitably small. It shows that these cryptanalysis are not dangerous. Additionally, we prove that both cryptanalysis enable us to factor m moduli of the form $N_i = p_i^2 q_i$ simultaneously based on the LLL algorithm.

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. R. K. (2015). New Attack on RSA With Modulus $N = p^2q$ Using Continued Fractions. *Journal of Physics*, 622:191–199.

Asbullah, M. A. and Ariffin, M. R. K. (2016a). Analysis on the AA_β 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.

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

Bunder, M. and Tonien, J. (2017). A New Attack on the RSA Cryptosystem Based on Continued Fractions. *Malaysian Journal of Mathematical Sciences*, 11(S):45–57.

Cassels, J. W. S. (2012). *An introduction to the geometry of numbers*. Springer Science & Business Media.

de Weger, B. (2002). Cryptanalysis of RSA With Small Prime Difference. *Applicable Algebra in Engineering, Communication and Computing*, 13(1):17–28.

Hinek, M. J. (2007). On the security of some variants of rsa.

Howgrave-Graham, N. and Seifert, J. (1999). Extending Wiener attack in the presence of many decrypting exponents. *In Secure Networking-CQRE (Secure)'99 LNCS 1740 Springer-Verlag*, 1740:153–166.

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

Maitra, S. and Sarkar, S. (2008). Revisiting Wieners Attack-New Weak Keys In RSA. *In Information Security Springer-Verlag*, pages 228–243.

May, A. (2003). *New RSA vulnerabilities using lattice reduction methods*. PhD thesis, University of Paderborn Paderborn.

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

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

Nishioka, M., Satoh, H., and Sakurai, K. (2002). Design and Analysis of Fast Provably Secure Public-Key Cryptosystems Based on a Modular Squaring. *In Information Security And Cryptology - ICISC 2001*, pages 81–102.

Nitaj, A., Ariffin, M. R. K., Nassr, D. I., and Bahig, H. M. (2014). *New attacks on the RSA cryptosystem*, volume 8469 of *Lecture Notes in Computer Science*, pages 178–198. Springer-Verlag.

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

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

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