International Journal of Pure and Applied Mathematics
Volume 110 No. 4 2016, 587-607
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: 10.12732/ijpam.v110i4.3

NEW PRACTICAL ATTACK ON RSA MODULUS OF TYPE $N = p^2q$

Normahirah Nek Abd Rahman[1 §], Muhammad Rezal Kamel Ariffin[2]

[1,2]Al-Kindi Cryptography Research Laboratory
Institute for Mathematical Research
Universiti Putra Malaysia
43400 UPM Serdang, Selangor, MALAYSIA

[2]Department of Mathematics
Faculty of Science
Universiti Putra Malaysia
43400 UPM Serdang, Selangor, MALAYSIA

Abstract: This paper proposes three new attacks on RSA with the modulus $N = p^2q$. The first attack is based on the equation $eX - NY = (p^2u + q^2v)Z$ such that u is an integer multiple of 2 and v is an integer multiple of 3 with $|p^2u - q^2v| < N^{1/2}$ and $\gcd(X, Y) = 1$. If $X|Z| < \frac{N}{2|p^2u+q^2v|}$, then N can be factored in polynomial time using continued fractions expansion. For the second and third attack, this paper proposes new vulnerabilities in k RSA cryptosystem moduli $N_i = p_i^2q_i$ for $k \geq 2$ and $i = 1, ..., k$. The attacks work when k RSA public keys (N_i, e_i) are related through $e_ix - N_iy_i = (p_i^2u + q_i^2v)z_i$ or $e_ix_i - N_iy = (p_i^2u + q_i^2v)z_i$ where the parameters x, x_i, y, y_i and z_i are suitably small.

AMS Subject Classification: 11A51, 11A55, 11K60, 03G10
Key Words: RSA, factorization, continued fraction, LLL algorithm, simultaneous diophantine approximations

1. Introduction

The RSA cryptosystem has been proposed by Rivest, Shamir and Adleman

Received: June 23, 2016
Revised: August 15, 2016
Published: November 9, 2016

§Correspondence author

became a well-known asymmetric cryptosystem for transmission of data [17]. Basically, the difficulty of breaking the RSA cryptosystem is based three hard mathematical problems which is the integer factorization problem of $N = pq$, the eth root problem from $C \equiv M^e \pmod{N}$ and to solve the Diophantine key equation $ed + 1 = \phi(N)k$.

The encryption and decryption processes in RSA require executing exponential multiplications modulo the integer $N = pq$. To reduce the encryption time, one may wish to use a small public exponent, e while to reduce the decryption time, one may tempted to use a short secret exponent, d. The choice of small d is especially interesting when the device performing secret operations has limited power.

Hence, the RSA cryptosystem is likely to have faster decryption when the secret exponent d is relatively small. This idea was firstly introduced by Wiener in 1990. After investigating the diophantine key equation, Wiener proved that if the secret exponent $d < \frac{1}{3}N^{1/4}$ would result in RSA to be totally insecure [21]. That is through the continued fractions of $\frac{e}{N}$, Wiener was able to obtain the integer solutions of the diophantine key equation and eventually factoring N.

Later, in 1999, by using lattice basis reduction technique, Boneh and Durfee proposed an extension on Wiener's work. It was determined that the RSA cryptosystem is insecure when $d < N^{0.292}$[4]. On the other hand, de Weger proposed an extension of these attacks to an RSA modulus with small difference between its prime factors [5]. Similarly, by combining lattice basis reduction techniques and the continued fraction expansion algorithm, Blömer and May come up with an attack extension of Wiener's attack [3].

Later, Howgrave-Graham and Seifert proposed an extension of Wiener's attack that allows the RSA system to be insecure in the presence of two decryption exponents (d_1, d_2) with $d_1, d_2 < N^{5/14}$ [8]. In the presence of three decryption exponents, they improved the bound to $N^{2/5}$ based on lattice reduction method. In 2007, Hinek 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 $\delta = \frac{k}{2(k+1)} - \varepsilon$ where ε is a small constant depending on the size of max N_i [7].

In 2014, Nitaj et al. presented new method to factor all the RSA moduli $N_1, ..., N_k$ in the scenario that RSA instances satisfy k equations of the shape $e_i x - y_i\phi(N_i) = z_i$ or of the shape $e_i x_i - y\phi(N_i) = z_i$ 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 which has been introduced by Lenstra et al. [9] for lattice basis reduction [15].

Furthering this, many RSA variant have been propose to achieve better throughput. That is to be able to send large data sets and to achieve better

computational time while maintaining the level of security. These new variants capatilize on the concept *Prime Power RSA.* In Prime Power RSA the modulus N is in the form $N = p^r q$ for $r \geq 2$. Takagi (1997) showed how to used the Prime Power RSA to speed up the decryption process when the public and private exponents satisfy an equation $ed \equiv 1 (\text{mod } (p-1)(q-1))$ [20]. Okamoto and Uchiyama (1998) presented a public key cryptosystem that is provably as secure as factoring a modulus in the form $N = p^2 q$ [16].

In 2004, May improved the bound of private exponent to $d < N^{\frac{r}{(r+1)^2}}$ for RSA modulus in the form $N = p^r q$ [11]. Later, Sarkar (2014) improved the bound to $d < N^{0.395}$ for RSA modulus $N = p^2 q$ [18].

Recently, Asbullah and Ariffin showed that one can factor $N = p^2 q$ in polynomial time if e satisfies the equation $eX - (N - (ap^2 + bq^2)Y = Z$ where a, b are positive integer satisfying $\gcd(a, b) = 1$, $|ap^2 - bq^2| < N^{1/2}$, $|Z| < \frac{|ap^2-bq^2|}{3(ap^2+bq^2)} N^{1/3} Y$ and $1 \leq Y \leq X < \frac{N^{1/2}}{2(ap^2+bq^2)^{1/2}}$ [2].

Our contribution. Therefore, in this paper, we present new cryptanalysis on the modulus of $N = p^2 q$ by using continued fractions method as the first analysis motivated from some previous attacks by [21], [12], [13],[14] and [1]. We consider the public value, e satisfying the following generalized key equation, $eX - NY = (p^2 u + q^2 v)Z$ such that u is an integer multiple of 2 and v is an integer multiple of 3. If

$$gcd(X, Y) = 1, \ |p^2 u - q^2 v| < N^{1/2}, \ X|Z| < \frac{N}{2|p^2 u + q^2 v|}$$

then N can be factored in polynomial time using continued fractions. We also show that the number of such parameters e satisfying the equation are at least $N^{\frac{1}{3}-\varepsilon}$ where $\varepsilon > 0$ is arbitrarily small for large N.

In the second attack, we focus on k instances of (N_i, e_i) where $N_i = p_i^2 q_i$ together with its generalized system of key equations $e_i x - N_i y_i = (p_i^2 u + q_i^2 v) z_i$. We prove that, each RSA moduli N_i can be factored in polynomial time if

$$x < N^{\delta}, \quad y_i < N^{\delta}, |z_i| < \frac{\sqrt{2} N^{1/2}}{|p_i^2 u - q_i^2 v|} \quad \text{where} \quad \delta = \frac{k}{3} - \alpha k, \quad N = \min_i N_i.$$

Finally, for the third attack, we we prove that we are able to factor k RSA moduli of the form $N_i = p_i^2 q_i$ when k instance of (N_i, e_i) are available and the variables (x_i, y, z_i, δ) in the generalized system of key equations given by $e_i x_i - N_i y = (p_i^2 u + q_i^2 v) z_i$ satisfying

$$x_i < N^{\delta}, \quad y < N^{\delta}, |z_i| < \frac{\sqrt{2} N^{1/2}}{|p_i^2 u - q_i^2 v|} \quad \text{where} \quad \delta = \beta k - \alpha k - \frac{2k}{3},$$

with $N = \max_i N_i$ and $\min_i e_i = N^{\beta}$.

For the second and third attack, we transform the equations into a simultaneous diophantine problem and applying lattice basis reduction techniques to find parameters (x, y_i) or (y, x_i). This leads to a suitable approximation of $p^2u + q^2v$ which allow us to apply the theorem that we propose in first cryptanalysis to compute the prime factor p_i and q_i of the moduli N_i. We also prove that the propose attacks enables to factor the k RSA moduli N_i simultaneously.

The layout of the paper is as follows. In Section 2, we begin with a brief review on continued fractions expansion, lattice basic reduction, simultaneous diophantine approximation and also some useful results that will be used throughout the paper. In Section 3, Section 4 and Section 5, we present our first, second and third attacks consecutively together with examples. Then, we conclude the paper in Section 6.

2. Preliminaries

In this section, we give brief review on continued fractions expansion, lattice basic reduction and simultaneous diophantine approximation that will be used throughout this paper.

2.1. Continued Fractions Expansion

A continued fraction is an expression of the form

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

which, for simplicity, can be rewritten as $x = [a_0, a_1, \ldots, a_n, \ldots]$. If x is a rational number, then the process of calculating the continued fractions expansion will finish in some finite index n and then $x = [a_0, a_1, \ldots, a_n]$. The convergents $\frac{a}{b}$ of x are the fractions denoted by $\frac{a}{b} = [a_0, a_1, \ldots, a_i]$ for $i \geq 0$. An important result on continued fractions that will be used is the following theorem.

Theorem 1. *(Legendre) [6]. Let $x = [a_0, a_1, a_2, \ldots]$ be the continued fraction expansion of x. If X and Y are coprime integers such that*

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

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

2.2. 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 and is in the form

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

The set $(u_i, ..., u_d)$ 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 [9] produces a reduced basis and the following result fixes the sizes of the reduced basis vector (see [10]).

Theorem 2. *[9]. Let 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 of the LLL algorithm is it provides a solution to the simultaneous Diophantine approximations problem which is defined as follows. Let $\alpha_1, ..., \alpha_n$ be n real numbers and ε a real number such that $0 < \varepsilon < 1$. A classical theorem of Dirichlet asserts that there exist integers $p_1, ..., p_n$ and a positive integer $q \leq \varepsilon^{-n}$ such that

$$|q\alpha_i - p_i| < \varepsilon \quad \text{for} \quad 1 \leq i \leq n.$$

In [9] described a method to find simultaneous diophantine approximations to rational numbers which they consider a lattice with real entries. Hence, we state here a similar result for a lattice with integer entries.

Theorem 3. *(Simultaneous Diophantine Approximations) [9]. 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*

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

Proof. See Appendix. □

3. The First Attack

In this section, we present our first attack on RSA with the modulus $N = p^2q$. The following lemma shows that any approximation of $p^2u + q^2v$ will lead to an approximation of q. We begin with a lemma fixing the size of prime factor p and q of RSA-type modulus $N = p^2q$.

Lemma 1. *Let $N = p^2q$ with $q < p < 2q$. Then $2^{-1/3}N^{1/3} < q < N^{1/3} < p < 2^{1/3}N^{1/3}$.*

Proof. Suppose $q < p < 2q$. Multiplying by p^2, we get $N < p^3 < 2N$. Hence $N^{1/3} < p < 2^{1/3}N^{1/3}$. Multiplying $q < p < 2q$ by pq and q^2, we get $q^3 < pq^2 < 2q^3$ and $pq^2 < N < 2pq^2$, respectively. This implies $2^{-2/3}N^{1/3} < q < N^{1/3}$. This terminate the proof. □

Lemma 2. *Let $N = p^2q$ with $q < p < 2q$. Let $u, v \in \mathbb{N}$ such that u is an integer multiple of 2 and v is an integer multiple of 3. Let $|p^2u - q^2v| < N^{1/2}$.Set $S = (p^2u + q^2v)Z$, where $1 \leq |Z| < \frac{\sqrt{2}N^{1/2}}{|p^2u-q^2v|}$, then $uvZ^2q = \left[\frac{S^2}{4N}\right]$.*

Proof. First, we consider $S = (p^2u + q^2v)Z$ Then, observe that

$$\begin{aligned} S^2 &= \Big((p^2u + q^2v)Z\Big)^2 \\ &= (p^2Zu + q^2Zv)^2 \\ &= (p^2Zu + q^2Zv)(p^2Zu + q^2Zv) \\ &= (p^2Zu)^2 + 2(p^2Zu)(q^2Zv) + (q^2Zv)^2 \\ &= (p^2Zu - q^2Zv)^2 + 4(p^2q^2uvZ^2) \\ &= (p^2Zu - q^2Zv)^2 + 4Nquv Z^2 \end{aligned}$$

We obtain

$$S^2 - 4Nquv Z^2 = \Big(p^2Zu - q^2Zv\Big)^2 > 0 \tag{1}$$

Hence, we divide (1) by $4N$ and we get

$$\begin{aligned} \left|\frac{S^2}{4N} - uvZ^2q\right| &= \left|\frac{S^2 - 4Nquv Z^2}{4N}\right| \\ &= \frac{\Big(p^2Zu - q^2Zv\Big)^2}{4N} \end{aligned}$$

$$\begin{aligned} &= \frac{\left(p^2u - q^2v\right)^2 Z^2}{4N} \\ &< \frac{\left(p^2u - q^2v\right)^2 \left(\frac{\sqrt{2}N^{1/2}}{|p^2u-q^2v|}\right)^2}{4N} \\ &< \frac{\left(\sqrt{2}N^{1/2}\right)^2}{4N} = \frac{1}{2} \end{aligned}$$

which we deduce $uvZ^2q = \left\lfloor \frac{S^2}{4N} \right\rfloor$. This terminate the proof. □

Lemma 3. *Let $N = p^2q$ with $q < p < 2q$. Let e be an exponent satisfying an equation $eX - NY = (p^2u + q^2v)Z$ for some $u, v \in \mathbb{N}$ and with $gcd(X, Y) = 1$ and $X|Z| < \frac{N}{2|p^2u+q^2v|}$ then $\frac{Y}{X}$ is a convergent of the continued fraction $\frac{e}{N}$.*

Proof. Suppose that $X|Z| < \frac{N}{2|p^2u+q^2v|}$. Starting with the equation $eX - NY = (p^2u + q^2v)Z$ and if we divide by NX, then we obtain

$$\left| \frac{e}{N} - \frac{Y}{X} \right| = \left| \frac{(p^2u + q^2v)Z}{NX} \right|$$

In order to apply Legendre theorem, observe that, if $X|Z| < \frac{N}{2|p^2u+q^2v|}$, then $\frac{|(p^2u+q^2v)Z|}{NX} < \frac{1}{2X^2}$ is satisfied. Hence, we conclude that $\frac{Y}{X}$ is convergent of continued fraction $\frac{e}{N}$. □

The following theorem shows that how to factor $N = p^2q$ completely.

Theorem 4. *Let $N = p^2q$ with $q < p < 2q$. Let $u, v \in \mathbb{N}$ such that u is an integer multiple of 2 and v is an integer multiple of 3. Let $|p^2u - q^2v| < N^{1/2}$. Let e be an exponent satisfying an equation $eX - NY = (p^2u + q^2v)Z$ with $gcd(X, Y) = 1$. If $X|Z| < \frac{N}{2|p^2u+q^2v|}$ then N can be factored in polynomial time.*

Proof. Suppose that e be an exponent satisfying an equation $eX - NY = (p^2u+q^2v)Z$ with $\gcd(X, Y) = 1$. Let X and $|Z|$ satisfy the condition in Lemma 2, then $\frac{Y}{X}$ is convergent of continued fraction $\frac{e}{N}$. From the value of X and Y, we define $S = eX - NY$. Then from Lemma 2, this implies that $uvZ^2q = \left\lfloor \frac{S^2}{4N} \right\rfloor$. It follows that we obtain $q = \gcd\left(\left\lfloor \frac{S^2}{4N} \right\rfloor, N\right)$. □

Now, we proposed the following algorithm for further recovering prime factorization of RSA-type modulus $N = p^2q$.

INPUT: The public key modulus (N, e) satisfying $N = p^2q$.
OUTPUT: The prime factor 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 $\left[\frac{S^2}{4N}\right]$.
4. Compute $q = \gcd\left(\left[\frac{S^2}{4N}\right], N\right)$
5. If $1 < q < N$, then $p = \sqrt{\frac{N}{q}}$.

Table 1: Algorithm 1

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

$$N = 64846371051769$$
$$e = 54715049302680$$

Suppose that N and e satisfy all the conditions stated in Theorem 4. Then, we compute the continued fraction of $\frac{e}{N}$. The list of the convergent of continued fraction are shown as follows

$$\left[0, 1, \frac{5}{6}, \frac{11}{13}, \frac{27}{32}, \frac{1847}{2189}, \frac{11109}{13166}, \frac{12956}{15355}, \frac{37021}{43876}, \dots\right],$$

We may omit the first and the second entry. We start with the convergent $\frac{5}{6}$ and we obtain

$$S = eX - NY = 4058440557235$$

and

$$\left[\frac{S^2}{4N}\right] = 63499851608$$

Hence, if we compute $\gcd(63499851608, 64505203569251) = 1$. Then, we try for next convergent $\frac{11}{13}$, we obtain

$$S = eX - NY = -2014440634619$$

and

$$\left[\frac{S^2}{4N}\right] = 15644557299$$

Then, if we compute $\gcd(15644557299, 64505203569251) = 1$. We proceed with the next convergent which is $\frac{27}{32}$ and we get

$$S = eX - NY = 29559287997$$

and

$$\left[\frac{S^2}{4N}\right] = 3368544$$

Thus, we compute $\gcd(3368544, 64505203569251) = 35089$ which leads to the factorization of N since $q = 35089$ and $p = \sqrt{\frac{N}{q}} = 42989$.

Now, we give an estimation of the number of the exponents e satisfying the equation $eX - NY = (p^2u + q^2v)Z$. We begin by showing the following result. Suppose that u is an integer multiple of 2 and v is an integer multiple of 3 and the public parameter $e < N$ satisfies at most one equation $eX - NY = (p^2u+q^2v)Z$ where the parameters X, Y and Z satisfy the condition in Theorem 4.

Suppose that $u, v \in \mathbb{N}$ and the public parameter $e < N$ satisfy at most one equation $eX - NY = (p^2u + q^2v)Z$ with $gcd(X, (p^2u + q^2v)Z) = 1$. Observe that since $\gcd(X, N) = 1$, then reduce the equation to $e \equiv (p^2u + q^2v)ZX^{-1} \pmod N$. We describe the following lemma which show that different parameter X_1, X_2 define different exponents e_1, e_2.

Lemma 4. *[13]. Let m and n be positive integers. Then*

$$m\frac{\phi(n)}{n} - 2^{\omega(n)} \; < \sum_{\substack{k=1 \\ gcd(k,\ n)=1}}^{m} 1 \; < m\frac{\phi(n)}{n} + 2^{\omega(n)}$$

where $\omega(n)$ is the number of distinct prime factors of n.

Proof. Let $\mu(d)$ be the Möbius function which is defined by $\mu(1) = 1$, $\mu(d) = 0$ if d is not square-free and $\mu(d) = (-1)^{\omega(d)}$ id d is square-free where $\omega(d)$ is the number of distinct prime factors of d. Then, from Legendre Theorem gives

$$\sum_{\substack{k=1 \\ gcd(k,\ n)=1}}^{m} 1 = \sum_{d|n} \mu(d)\left\lfloor \frac{m}{d} \right\rfloor.$$

Since $\left\lfloor \frac{m}{d} \right\rfloor \leq \frac{m}{d} < \left\lfloor \frac{m}{d} \right\rfloor + 1$, then

$$\begin{aligned}
\sum_{d|n} \mu(d) \left\lfloor \frac{m}{d} \right\rfloor &= \sum_{\substack{d|n \\ \mu(d)=1}} \mu(d) \left\lfloor \frac{m}{d} \right\rfloor + \sum_{\substack{d|n \\ \mu(d)=-1}} \mu(d) \left\lfloor \frac{m}{d} \right\rfloor \\
&> \sum_{\substack{d|n \\ \mu(d)=1}} \mu(d) \left(\frac{m}{d} - 1 \right) + \sum_{\substack{d|n \\ \mu(d)=-1}} \mu(d) \frac{m}{d} \\
&= \sum_{d|n} \mu(d) \frac{m}{d} - \sum_{\substack{d|n \\ \mu(d)=1}} 1 \\
&> m \sum_{d|n} \frac{\mu(d)}{d} - \sum_{d|n} |\mu(d)| \\
&= m \frac{\phi(n)}{n} - 2^{\omega(n)}
\end{aligned}$$

The Möbius function satisfies $\sum_{d|n} \frac{\mu(d)}{d} = \frac{\phi(n)}{n}$. (see 16.3.1 in [6])

It also satisfies $\sum_{d|n} |\mu(d)| = 2^{\omega(n)}$ ([6], Theorem 264). It follows that

$$\sum_{\substack{k=1 \\ gcd(k,\ n)=1}}^{m} 1 > m \frac{\phi(n)}{n} - 2^{\omega(n)}$$

On the other hand, using $\left\lfloor \frac{m}{d} \right\rfloor \leq \frac{m}{d} < \left\lfloor \frac{m}{d} \right\rfloor + 1$ we obtain

$$\begin{aligned}
\sum_{d|n} \mu(d) \left\lfloor \frac{m}{d} \right\rfloor &= \sum_{\substack{d|n \\ \mu(d)=1}} \mu(d) \left\lfloor \frac{m}{d} \right\rfloor + \sum_{\substack{d|n \\ \mu(d)=-1}} \mu(d) \left\lfloor \frac{m}{d} \right\rfloor \\
&< \sum_{\substack{d|n \\ \mu(d)=-1}} \mu(d) \frac{m}{d} + \sum_{\substack{d|n \\ \mu(d)=1}} \mu(d) \left(\frac{m}{d} - 1 \right) \\
&= \sum_{d|n} \mu(d) \frac{m}{d} - \sum_{\substack{d|n \\ \mu(d)=-1}} 1 \\
&< m \sum_{d|n} \frac{\mu(d)}{d} + \sum_{d|n} |\mu(d)| \\
&= m \frac{\phi(n)}{n} + 2^{\omega(n)}
\end{aligned}$$

This terminates the proof. □

Lemma 5. *Let $N = p^2q$ be RSA modulus with $q < p < 2q$ and $u, v \in \mathbb{N}$. For $i = 1,2$, let e_i be two exponents satisfying $eX_i - NY_i = (p^2u + q^2v)Z$ with $gcd(X_i, (p^2u + q^2v)Z)$ and $X_i|Z| < \frac{N}{2|p^2u+q^2v|}$. Then $X_1 \neq X_2$ and $e_1 \neq e_2$.*

Proof. Suppose that for $i = 1, 2$ and assume for contradiction that $e_1 = e_2$ and e satisfying

$$(p^2u + q^2v)ZX_1^{-1} \equiv (p^2u + q^2v)ZX_2^{-1} \pmod{N} \tag{2}$$

Rearrange (2), we obtain

$$(p^2u + q^2v)Z(X_1^{-1} - X_2^{-1}) \equiv 0 \pmod{N}$$

Then, we notice that, since $\gcd(X_i, (p^2u+q^2v)Z)$, then $X_2^{-1}-X_1^{-1} \equiv 0 \pmod{N}$ and $X_2 - X_1 \equiv 0 \pmod{N}$. Then, we have

$$|X_2 - X_1| \leq X_2 + X_1 < 2\left(\frac{N}{2(p^2u + q^2v)}\right) < N \tag{3}$$

Hence, $X_2 - X_1 = 0$ and $X_2 = X_1$. It follows that $e_1 = e_2$. This terminate the proof. □

Here, the following theorem shows the result estimation of the weak exponents e with the structure $e \equiv (p^2u + q^2v)X^{-1} \pmod{N}$ with $\gcd(X, (p^2u + q^2v)) = 1$ and $X < \frac{N}{2(p^2u+q^2v)}$ by applying Lemma 4 and Theorem 4 and we consider only for the case when $Z = 1$.

Theorem 5. *Let $N = p^2q$ be RSA modulus with $q < p < 2q$ and $u, v \in \mathbb{N}$. The number of exponents e satisfying $e \equiv (p^2u + q^2v)X^{-1} \pmod{N}$ with $gcd(X, (p^2u + q^2v)) = 1$ and $X < \frac{N}{2(p^2u+q^2v)}$ where $|p^2u + q^2v| = N^{\frac{1}{3}+\beta}$ is at least $N^{\frac{1}{3}-\varepsilon}$, $\varepsilon > 0$ is arbitrarily small for suitably large N.*

Proof. Suppose the number of exponents satisfying

$$e \equiv (p^2u + q^2v)X^{-1} \pmod{N}$$

with the condition of the theorem is

$$\mathcal{N} = \sum_{\substack{X=1 \\ gcd(X, p^2u+q^2v)=1}}^{B_1} 1. \tag{4}$$

where

$$B_1 = \left\lfloor \frac{N}{2(p^2u + q^2v)} \right\rfloor$$

Now, by using Lemma 4 with $n = p^2u + q^2v$ and $m = B_1$, we obtain

$$B_1 \frac{\phi(N)(p^2u + q^2v)}{p^2u + q^2v} - 2^{\omega(p^2u+q^2v)} < \mathcal{N} < B_1 \frac{\phi(N)(p^2u + q^2v)}{p^2u + q^2v} + 2^{\omega(p^2u+q^2v)} \quad (5)$$

Notice that, $2^{\omega(p^2u+q^2v)}$ is the number of square free divisors of p^2u+q^2v which is upper bounded by the total number $\pi(p^2u + q^2v)$ of divisors of $p^2u + q^2v$. Since $\pi(n)$ satisfies $\pi(n) = \log \log n$ ([6], Theorem 430-431).

Since $n = p^2u+q^2v = N^{2/3+\beta}$ and $B_1 = \left\lfloor \frac{N}{2(p^2u+q^2v)} \right\rfloor$, then $B_1 = \left\lfloor \frac{1}{2}N^{\frac{1}{3}-\beta} \right\rfloor$. Hence, we obtain

$$\mathcal{N} = B_1 \frac{\phi(N)(p^2u + q^2v)}{p^2u + q^2v} = N^{-\frac{1}{3}-2\beta}\phi(p^2u + q^2v) \quad (6)$$

By using ([6], Theorem 328)

$$\phi(n) > \frac{cn}{\log \log n} \quad (7)$$

Then, we substitute (7) in (6), we get

$$\mathcal{N} = \frac{c(N^{\frac{2}{3}+\beta})}{\log \log (N^{\frac{2}{3}+\beta})} \times N^{-\frac{1}{3}-2\beta} = N^{\frac{1}{3}-\beta-\varepsilon}$$

where we set $N^{-\varepsilon} = \frac{c}{\log \log N}$ and $\varepsilon > 0$ is arbitrarily small for large N. This terminates the proof. □

4. The Second Attack

In this section, we propose our second attack. Suppose that we are given k moduli $N_i = p_i^2 q_i$. We consider in this scenario that the following generalized system of key equation given by $e_i x - N_i y_i = (p_i^2 u + q_i^2 v)z_i$ will provide us the factor of each moduli which are all of the same size. We show that there, it is possible to factor k RSA moduli. This is achievable when the unknown parameters x, y_i and z_i are suitably small. We couple this information together with the execution of the LLL algorithm to achieve our objective.

Theorem 6. *For $k \geq 2$, let $N_i = p_i^2 q_i$, $1 \leq i \leq k$ be k RSA moduli each with the same size N where $N = \min_i N_i$. Let e_i, $i = 1, ..., k$ be k public exponents. Define $\delta = \frac{k}{6}$. Let $u, v \in \mathbb{N}$ such that u is an integer multiple of 2 and v is an integer multiple of 3. If there exist an integer $x < N^{\delta}$ and k integers $y_i < N^{\delta}$ and $|z_i| < \frac{\sqrt{2}N^{1/2}}{|p_i^2 u - q_i^2 v|}$ such that $e_i x - N_i y_i = (p_i^2 u + q_i^2 v) z_i$ for $i = 1, ..., k$, then one can factor the k RSA moduli $N_1, ...N_k$ in polynomial time.*

Proof. For $k \geq 2$ and $i = 1, ..., k$, starting with the equation $e_i x - N_i y_i = (p_i^2 u + q_i^2 v) z_i$, we obtain

$$\left| \frac{e_i}{N_i} x - y_i \right| = \frac{|(p_i^2 u + q_i^2 v) z_i|}{N_i} \tag{8}$$

Let $N = \min_i N_i$ and suppose that $y_i < N^{\delta}$ and $|z_i| < \frac{\sqrt{2}N^{1/2}}{|p_i^2 u - q_i^2 v|}$. We set $|p_i^2 u - q_i^2 v| > p_i$ since we use the relation $N^{1/3} < p < 2^{1/3} N^{1/3}$ and $p_i^2 u + q_i^2 v < 2N^{2/3}$ then we will get

$$\begin{aligned} \frac{(p_i^2 u + q_i^2 v)|z_i|}{N_i} &\leq \frac{(p_i^2 u + q_i^2 v)|z_i|}{N} \\ &\leq \frac{(2N^{\frac{2}{3}})\left(\frac{\sqrt{2}N^{1/2}}{N^{1/3}}\right)}{N} \\ &\leq \frac{2^{3/2} N^{5/6}}{N} \\ &= 2^{3/2} N^{-\frac{1}{6}} \end{aligned} \tag{9}$$

Plugging (9) in (8), we obtain

$$\left| \frac{e_i}{N_i} x - y_i \right| \leq 2^{3/2} N^{-\frac{1}{6}}$$

We now proceed to prove the existence of integer x. Let $\varepsilon = 2^{3/2} N^{-\frac{1}{6}}$, $\delta = \frac{k}{6}$. We have

$$N^{\delta} \cdot \varepsilon^k = 2^{3k/2} N^{\delta - \frac{k}{6}} = 2^{3k/2}$$

Then, since $2^{3k/2} < 2^{\frac{k(k-3)}{4}} \cdot 3^k$ for $k \geq 2$, we get $N^{\delta} \cdot \varepsilon^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k$. 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 3 are fulfilled will find x and y_i for $i = 1, ..., k$. Next, using the equation $e_i x - N_i y_i = (p_i^2 u + q_i^2 v) z_i$ and $1 < |z_i| <$

$\frac{\sqrt{2}N^{1/2}}{|p_i^2u-q_i^2v|}$, this implies that $uvZ^2q = \left\lfloor \frac{S^2}{4N} \right\rfloor$ for $S_i = e_ix - N_iy_i$ for each $i = 1, ..., k$, we find $q_i = \gcd\left(\left\lfloor \frac{S_i^2}{4N_i} \right\rfloor, N_i\right)$. This leads to the factorization of k RSA moduli $N_1, ..., N_k$. This terminates the proof. □

Example 2. As an illustration of this second attack, we consider the following three RSA moduli and public exponents

$$\begin{aligned}
N_1 &= 114000760222549864279781270853885152295461,\\
N_2 &= 228115095149010518316554945466909090873661,\\
N_3 &= 231236890212417970842411124690482829278481,\\
e_1 &= 109098385125715102458611794533226114000584,\\
e_2 &= 142008308621371178234527659441810463340520,\\
e_3 &= 155000153884152408505814407363292624088474.
\end{aligned}$$

Then, $N = \min(N_1, N_2, N_3) = 114000760222549864279781270853885152295461$. Since $k = 3$, we get $\delta = \frac{k}{6} = \frac{1}{2}$ and $\varepsilon = 2^{3/2}N^{-\frac{1}{6}} \approx 0.0000004061$. Set $u = 260$ and $v = 390$. Then, by using (12) with $n = k = 3$, we find

$$C = \left\lfloor 3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1} \right\rfloor = 14878079695151597558909586 45.$$

Consider the lattice $\mathcal{L}$ spanned by the matrix

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

Then, applying the LLL algorithm to $\mathcal{L}$, we get a reduced basis with the matrix

$$K = \begin{bmatrix} -20928770380 & 18379710443495355 \\ -821694325288669743815 & -530766368893408117395 \\ 3954727165130615012467 & 763232605728921873804 \\ 3366893382339493311163 & -614957357921563880223 9 \\ 14570849265561705 & 14623041108483595 \\ 2473756275407667582000 & -1797809971033007371660 \\ 152563492536187551627 & -1111295022726225808720 \\ 307267888801090221306 3 & 466767647537800074375 5 \end{bmatrix}.$$

Now, we obtain

$$K \cdot M^{-1} = \begin{bmatrix} -20928770380 & -20028770393 \\ -821694325288669743815 & -786359001299235418497 \\ 3954727165130615012467 & 378466201879944768 8318 \\ 3366893382339493311163 & 322210685425795534 5071 \end{bmatrix}$$
$$\begin{matrix} -13028770767 & -14028741809 \\ -511528714317654489673 & -550789049050439590568 \\ 2461933154455801268684 & 265088895894589607 3772 \\ 2095989457524477103184 & 225685872135176400 3931 \end{matrix} \Bigg] .$$

From the first row, we deduce $x = 20928770380$, $y_1 = 20028770393$, $y_2 = 13028770767$ and $y_3 = 14028741809$. By using x and y_i for $i = 1, 2, 3$, define $S_i = e_i x - N_i y_i$ is an approximation of $p_i^2 u + q_i^2 v$. Hence, by using Lemma 2 and Theorem 4, this implies that $uvZ^2 q = \left\lfloor \frac{S^2}{4N} \right\rfloor$ for $S_i = e_i x - N_i y_i$. Then, we obtain

$$\begin{aligned} S_1 &= 1408315151419853220300456815747, \\ S_2 &= 2234046567945829713849902729613, \\ S_3 &= 2272731290043918799693441887991. \end{aligned}$$

Then, for each $i = 1, 2, 3$, we find $\left\lfloor \frac{S_i^2}{4N_i} \right\rfloor$ and we obtain

$$\left\lfloor \frac{S_1^2}{4N_1} \right\rfloor = 4349426183314188600, \quad \left\lfloor \frac{S_2^2}{4N_2} \right\rfloor = 5469787153377900600,$$

$$\left\lfloor \frac{S_3^2}{4N_3} \right\rfloor = 5584432821250709400.$$

For each $i = 1, 2, 3$, we find $q_i = \gcd\left(\left\lfloor \frac{S_i^2}{4N_i} \right\rfloor, N_i \right)$ and we obtain

$$q_1 = 42893749342349, \quad q_2 = 53942674096429, \quad q_3 = 55073301984721.$$

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

$$p_1 = 51553347319883, \quad p_2 = 65029554162953 \quad p_3 = 64797462962081.$$

5. The Third Attack

On the other hand, in this section, we propose our third attack. Suppose that we are given k moduli $N_i = p_i^2 q_i$. We consider in this scenario that the following generalized system of key equation given by $e_i x_i - N_i y = (p_i^2 u + q_i^2 v) z_i$ will provide us the factor of each moduli which are all of the same size. We show that there, it is possible to factor k RSA moduli. This is achievable when the unknown parameters x_i, y and z_i are suitably small. We couple this information together with the execution of the LLL algorithm to achieve our objective.

Theorem 7. *For $k \geq 2$, let $N_i = p_i^2 q_i$, $1 \leq i \leq k$ be k RSA moduli each with the same size N where $N = \max_i N_i$. Let e_i, $i = 1, ..., k$ be k public exponents with $\min_i e_i = N^\beta$. Define $\delta = \beta k - \frac{5k}{6}$. Let $u, v \in \mathbb{N}$ such that u is an integer multiple of 2 and v is an integer multiple of 3. If there exist an integer $y < N^\delta$, k integers $x_i < N^\delta$ and $|z_i| < \frac{\sqrt{2}N^{1/2}}{|p_i^2 u - q_i^2 v|}$ such that $e_i x_i - N_i y = (p_i^2 u + q_i^2 v) z_i$ for $i = 1, ..., k$, then one can factor the k RSA moduli $N_1, ..., N_k$ in polynomial time.*

Proof. For $k \geq 2$ and $i = 1, ..., k$, the equation $e_i x_i - N_i y = (p_i^2 u + q_i^2 v) z_i$, we get

$$\left| \frac{N_i}{e_i} y - x_i \right| = \frac{|(p_i^2 u + q_i^2 v) z_i|}{e_i} \tag{10}$$

Let $N = \max_i N_i$ and suppose that $y < N^\delta$, $|z_i| < \frac{\sqrt{2}N^{1/2}}{|p_i^2 u - q_i^2 v|}$ and $\min_i e_i = N^\beta$. We set $|p_i^2 u - q_i^2 v| > p_i$ since we use the relation $N^{1/3} < p < 2^{1/3} N^{1/3}$ and $p_i^2 u + q_i^2 v < 2N^{2/3}$ then we will get

$$\begin{aligned} \frac{|(p_i^2 u + q_i^2 v) z_i|}{e_i} &\leq \frac{(p_i^2 u + q_i^2 v)|z_i|}{N^\beta} \\ &< \frac{(2N^{\frac{2}{3}}) \frac{\sqrt{2}N^{1/2}}{|p_i^2 u - q_i^2 v|}}{N^\beta} \\ &< \frac{(2N^{\frac{2}{3}})(\frac{\sqrt{2}N^{1/2}}{N^{1/3}})}{N^\beta} \\ &= 2^{\frac{3}{2}} N^{\frac{5}{6} - \beta} \end{aligned} \tag{11}$$

Plugging (11) in (10), we obtain

$$\left| \frac{N_i}{e_i} y - x_i \right| < 2^{\frac{3}{2}} N^{\frac{5}{6} - \beta}.$$

We now proceed to prove the existence of integer y and the integers x_i. Let $\varepsilon = 2^{\frac{3}{2}} N^{\frac{5}{6}-\beta}$, $\delta = \beta k - \frac{5k}{6}$. Then, we obtain

$$N^{\delta} \cdot \varepsilon^k = N^{\delta}(2^{\frac{3}{2}} N^{\frac{5}{6}-\beta})^k = 2^{\frac{3k}{2}}(N^{\delta+\frac{5}{6}k-\beta k}) = 2^{\frac{3}{2}k}.$$

Then, since $2^{\frac{3}{2}k} < 2^{\frac{k(k-3)}{4}} \cdot 3^k$ for $k \geq 2$, we get $N^{\delta} \cdot \varepsilon^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k$. 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

$$\left| \frac{N_i}{e_i} y - x_i \right| < \varepsilon, \quad y < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \varepsilon^{-k}, \quad \text{for} \quad i = 1, ..., k,$$

It follows the condition of Theorem 3 are fulfilled will find y and x_i for $i = 1, ..., k$. Next, by using the equation $e_i x_i - N_i y = (p_i^2 u + q_i^2 v) z_i$ and since $1 < |z_i| < \frac{\sqrt{2} N^{1/2}}{|p_i^2 u - q_i^2 v|}$ and this implies that $uvZ^2 q = \left[\frac{S^2}{4N} \right]$ for $S_i = e_i x_i - N_i y$ 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 RSA moduli $N_1, ..., N_k$. This terminates the proof. □

Example 3. As an illustration of the third attack, consider the following three RSA moduli and public exponents

$$\begin{aligned}
N_1 &= 14731423762622589711231181358815426842654 1, \\
N_2 &= 23777591690017295427254379110750608908058 3, \\
N_3 &= 33946925628012644830584242496902361512168 3, \\
e_1 &= 11487092223770958877124557906102835983208 2, \\
e_2 &= 19006087841443043055825748837280793604469 6, \\
e_3 &= 28568332569634823544683029620556400973062 9.
\end{aligned}$$

Then, $N = \max(N_1, N_2, N_3) = 339469256280126448305842424969023615121683$. We also obtain $\min(e_1, e_2, e_3) = N^{\beta}$ with $\beta \approx 0.9886688835$. Since $k = 3$ we get $\delta = \beta k - \frac{5k}{6} = 0.466006650$ and $\varepsilon = 2^{\frac{3}{2}} N^{\frac{5}{6}-\beta} \approx 0.0000010007$. Set $u = 300$ and $v = 450$. Then, by using (12) with $n = k = 3$, we find

$$C = \left[3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1} \right] = 4037513574407732543670055 1.$$

Consider the lattice $\mathcal{L}$ spanned by the matrix

$$M = \begin{bmatrix} 1 & -[CN_1/e_1] & -[CN_2/e_2] & -[CN_3/e_3] \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}.$$

Then, applying the LLL algorithm to $\mathcal{L}$, we get a reduced basis with the matrix K

$$= \begin{bmatrix} -3186595759 & -666654400396680 & -538317459032548 & -502459761727128 \\ -80004816082475565419 & -256706228905171710597 & 186745528335567423374 & 140520570411343159128 \\ -38498156388438 6646447 & -58239693649250278240 & 37246015231993662609 & 37369006403280349418 \\ -137762503349110575602 & -40146208250920113708 & 383386780152511327889 & -357481563550077921439 \end{bmatrix}.$$

Now, we obtain
$K \cdot M^{-1}$

$$= \begin{bmatrix} -3186595759 & -4086594899 & -3986594899 & -3786539833 \\ -80004816082475565419 & -102600799732652192026 & -100090132483550528817 & -95067415461319812077 \\ -38498156388438 6646447 & -49371298218029 7031867 & -48163170193641 6978224 & -45746248877087777 5947 \\ -137762503349110575602 & -176671151924402499790 & -172347964618324415739 & -163699209399846282679 \end{bmatrix}.$$

From the first row, we deduce $y = 3186595759$, $x_1 = 4086594899$, $x_2 = 3986594899$ and $x_3 = 3786539833$. By using y and x_i for $i = 1, 2, 3$, define $S_i = e_i x_i - N_i y$ is an approximation of $p_i^2 u + q_i^2 v$. Hence, by using Lemma 2 and Theorem 4, this implies that $uvZ^2 q = \left\lfloor \frac{S^2}{4N} \right\rfloor$ for $S_i = e_i x_i - N_i y$. Then, we get

$$\begin{aligned} S_1 &= 189668940148874057 8359644110099, \\ S_2 &= 253405059062711161 1641312558207, \\ S_3 &= 355526384499052075 8622991902560. \end{aligned}$$

Next, for each $i = 1, 2, 3$, we find $\left\lfloor \frac{S_i^2}{4N_i} \right\rfloor$ and we get $\left\lfloor \frac{S_1^2}{4N_1} \right\rfloor = 6105028854792915000$, $\left\lfloor \frac{S_2^2}{4N_2} \right\rfloor = 6751537833995145000$, $\left\lfloor \frac{S_3^2}{4N_3} \right\rfloor = 9308575646881605000$. For each $i = 1, 2, 3$, we find $q_i = \gcd\left(\left\lfloor \frac{S_i^2}{4N_i} \right\rfloor, N_i \right)$ and we obtain

$$q_1 = 45222435961429, \quad q_2 = 50011391362927, \quad q_3 = 68952412199123.$$

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

$$p_1 = 57074929677173, \quad p_2 = 68952412199123, \quad p_3 = 70165801822561.$$

6. Conclusion

In conclusion, this paper presents three new attacks on RSA moduli type $N = p^2 q$. The first attack is based on the equation $eX - NY = (p^2 u + q^2 v)Z$ where u is an integer multiple of 2 and v is an integer multiple of 3 together with some conditions on the parameters. Continuing our work, we focused on the

system of generalized key equations of the form $e_i x - N_i y_i = (p_i^2 u + q_i^2 v) z_i$ for the second attack and in the form of $e_i x_i - N_i y = (p_i^2 u + q_i^2 v) z_i$ for the third attack. We proved the two attacks are successful when the parameters x, x_i, y, y_i and z_i are suitably small. On top of that, we also proved that both of our attacks enables us to factor k RSA moduli of the form $N_i = p_i^2 q_i$ simultaneously based on LLL algorithm.

References

[1] M.A. Asbullah, *Cryptanalysis on the Modulus $N = p^2q$ and Design of Rabin-Like Cryptosystem without Decryption Failure*, PhD Thesis, Universiti Putra Malaysia, 2015.

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

[3] J. Blömer, A. May, A generalized Wiener attack on RSA, *Practice and Theory in Public Key Cryptography PKC 2004 LNCS Springer-Verlag*, **2947** (2004), 1-13, **doi:** 10.1007/978-3-540-24632-9-1.

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

[5] B. de Weger, Cryptanalysis of RSA with small prime difference, *Applicable Algebra in Engineering Communication and Computing*, **13** No. 1 (2002), pages 17, **doi:** 10.1007/s002000100088.

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

[7] J. Hinek, *On the Security of Some Variants of RSA*, PhD Thesis, Waterloo, Ontario, Canada, 2007.

[8] N. Howgrave-Graham, J. Seifert, Extending Wiener attack in the presence of many decrypting exponents, In: *Secure Networking-CQRE (Secure)'99 Lecture Notes in Computer Science*, **1740**, Springer-Verlag (1999), 153-166.

[9] A.K. Lenstra, H.W. Lenstra, L. Lovász, *Factoring Polynomials with Rational Coefficients*, Mathematische Annalen, **261**(1982), 513-534, **doi:** 10.1007/BF01457454.

[10] A. May, *New RSA Vulnerabilities Using Lattice Reduction Methods*, PhD Thesis, University of Paderborn, 2003.

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

[12] A. Nitaj, Cryptanalysis of RSA using the ratio of the primes, *Progress in Cryptology - AFRICACRYPT*, Springer (2009), 98-115, **doi:** 10.1007/978-3-642-02384-2_7.

[13] A. Nitaj, A new vulnerable class of exponents in RSA, *JP Journal of Algebra, Number Theory and Applications*, **21** No. 2 (2011a), 203-220.

[14] A. Nitaj, New weak RSA keys, *JP Journal of Algebra, Number Theory and Applications*, **23** No. 2 (2011b), 131-148.

[15] A. Nitaj, M. Ariffin, D.I. Nassr, H.M. Bahig, New attacks on the RSA cryptosystem, *Lecture Notes in Computer Science*, **8469**, Springer Verlag (2014), 178-198, **doi:** 10.1007/978-3-319-06734-6_12.

[16] T. Okamoto, S. Uchiyama, A new public-key cryptosystem as secure as factoring, In: *Advances In Cryptology-EUROCRYPT'98*, Springer (1998), 308-318, **doi:** 10.1007/BFb0054135.

[17] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communication of the ACM*, **21**, No. 2 (1978), 17-28, **doi:** 10.1145/359340.359342.

[18] S. Sarkar, Small secret exponent attack on RSA variant with modulus $N = p^r q$, *Designs, Codes and Cryptography*, **73**, No. 2, Springer (2014), 383-392, **doi:** 10.1007/s10623-014-9928-6.

[19] S. Sarkar, S. Maitra, Cryptanalysis of RSA with two decryption exponents, *Information Processing Letters*, **110** (2010), 178-181, **doi:** 10.1016/j.ipl.2009.11.016.

[20] T. Takagi, Fast RSA-type cryptosystem modulo $p^k q$, *Advances in Cryptology-CRYPTO'98*, Springer (1998), 318-326, **doi:** 10.1007/BFb0055738.

[21] M. Wiener, Cryptanalysis of short RSA secret exponents, *IEEE Transaction on Information Theory IT-36*, **36** (1990), 553-558, **doi:** 10.1109/18.54902.

Appendix: Proof of Theorem 3

Proof. [9] Let $\varepsilon \in (0,1)$. Set

$$C = \left\lceil 3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1} \right\rceil, \tag{12}$$

where $\lceil x \rceil$ is the integer greater than or equal to x. Consider the lattice $\mathcal{L}$ spanned by the rows of the matrix

$$M = \begin{bmatrix} 1 & -[C\alpha_1] & -[C\alpha_2] & \cdots & -[C\alpha_n] \\ 0 & C & 0 & \cdots & 0 \\ 0 & 0 & C & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & C \end{bmatrix},$$

where $[x]$ is the nearest integer to x. The determinant of $\mathcal{L}$ is $\det(\mathcal{L}) = C^n$ and the dimension is $n+1$. Applying the LLL algorithm, we find a reduced basis $(b_1, ..., b_{n+1})$ with

$$\|b_1\| \leq 2^{n/4} \det(\mathcal{L})^{1/(n+1)} = 2^{n/4} C^{n/(n+1)}.$$

Since $b_1 \in \mathcal{L}$, we can write $b_1 = \pm[q, p_1, p_2, ..., p_n]M$, that is

$$b_1 = \pm[q, Cp_1 - q[C\alpha_1], Cp_2 - q[C\alpha_2], ..., Cp_n - q[C\alpha_n]], \tag{13}$$

where $q > 0$. Hence, the norm of b_1 satisfies

$$\|b_1\| = \Big(q^2 + \sum_{i=1}^{n} |Cp_i - q[C\alpha_i]|^2\Big)^{1/2} \leq 2^{n/4} C^{n/(n+1)},$$

which leads to

$$q \leq \Big\lfloor 2^{n/4} C^{n/(n+1)} \Big\rfloor \quad \text{and} \quad \max_i |Cp_i - q[C\alpha_i]| \leq 2^{n/4} C^{n/(n+1)}. \tag{14}$$

Let us consider the entries $q\alpha_i - p_i$. We have

$$\begin{aligned} |q\alpha_i - p_i| &= \frac{1}{C}|Cq\alpha_i - Cp_i| \\ &\leq \frac{1}{C}(|Cq\alpha_i - q[C\alpha_i]| + |q[C\alpha_i] - Cp_i|) \\ &= \frac{1}{C}(q|C\alpha_i] - [C\alpha_i]| + |q[C\alpha_i] - Cp_i|) \\ &\leq \frac{1}{C}\Big(\frac{1}{2}q + |q[C\alpha_i] - Cp_i|\Big). \end{aligned}$$

Using the two inequalities in (14), we get

$$|q\alpha_i - p_i| \leq \frac{1}{C}\Big(\frac{1}{2} \cdot 2^{n/4} C^{n/(n+1)} + 2^{n/4} C^{n/(n+1)}\Big) = \frac{3 \cdot 2^{(n-4)/4}}{C^{1/(n+1)}}.$$

Observe that (12) gives

$$3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1} \leq C \leq\leq 3^{n+1} \cdot 2^{\frac{(n+1)(n-3)}{4}} \cdot \varepsilon^{-n-1}, \tag{15}$$

which leads to $\varepsilon \geq \frac{3 \cdot 2^{(n-4)/4}}{C^{1/(n+1)}}$. As a consequence, we get $|q\alpha_i - p_i| \leq \varepsilon$. On the other hand, using (14) and (15), we get

$$q \leq \Big\lfloor 2^{n/4} C^{n/(n+1)} \Big\rfloor \leq 2^{n/4} C^{n/(n+1)} \leq 2^{n(n-3)/4} \cdot 3^n \cdot \varepsilon^{-n}.$$

To compute the vector $[q, p_1, p_2, ..., p_n]$, we use (13)

$$[q, p_1, p_2, ..., p_n] = \pm[q, Cp_1 - q[C\alpha_1], Cp_2 - q[C\alpha_2], ..., Cp_n - q[C\alpha_n]]M^{-1}.$$

This terminates the proof. □