Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 12, Number 4 (2016), pp. 3159–3185

http://www.ripublication.com/gjpam.htm

New Weak Findings Upon RSA Modulo of Type $N = p^2q$

Muhammad Rezal Kamel Ariffin
Al-Kindi Cryptography Research Laboratory,
Institute for Mathematical Research,
Universiti Putra Malaysia,
43400 UPM Serdang, Selangor, Malaysia.
Department of Mathematics,
Faculty of Science,
Universiti Putra Malaysia,
43400 UPM Serdang, Selangor, Malaysia.

Normahirah Nek Abd Rahman
Al-Kindi Cryptography Research Laboratory,
Institute for Mathematical Research,
Universiti Putra Malaysia,
43400 UPM Serdang, Selangor, Malaysia.

Abstract

This paper proposes 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. If

$$|p^2u - q^2v| < N^{1/2},$$

$$|Z| < \frac{|p^2 - q^2|}{3(p^2 + q^2)} N^{1/3}$$

and

$$X < \frac{N}{3(p^2u + q^2v)},$$

then N can be factored in polynomial time using continued fractions. For the second and third attacks, this paper proposes new vulnerabilities in k RSA Moduli $N_i = p_i^2q_i$ for $k \geq 2$ and $i = 1, \ldots, k$. 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

$$e_i x_i - N_i y = p_i^2 u + q_i^2 v + z_i$$

where the parameters x, x_i, y, y_i and z_i are suitably small.

AMS subject classification:
Keywords: RSA, Factorization, Continued fraction, LLL algorithm, Simultaneous diophantine approximations.

1. Introduction

The RSA cryptosystem was developed by Rivest, Shamir and Adleman is the well-known public key cryptosystem [1]. The mathematical operations in RSA depend on three parameters, the modulus $N = pq$ which is the product of two large primes p and q, 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 integer factorization problem of $N = pq$, the e-th root problem from $C \equiv M^e \pmod N$ and to solve the diophantine key equation $ed + 1 = \phi(N)k$.

Many practical issues have been considered when implementing RSA in order to reduce the encryption or the execution decryption time. To reduce the encryption time, one may wish to use a small public exponent e. For discussion on security issues surrounding small encryption exponent see [4]. Logically, the RSA cryptosystem is likely to have faster decryption if the secret exponent d is relatively small. The knowledge of secret exponent d leads to factoring N in polynomial time. Thus, much research has been produced to determine the lower bound for d. Nevertheless, the use of short secret exponent will encounter serious security problems in various instances of RSA.

Based on the convergents of the continued fraction expansion of $\frac{e}{N}$, Wiener (1990) showed that the RSA cryptosystem is insecure when the secret exponent, $d < \frac{1}{3}N^{1/4}$ [2]. Later, in 1999, Boneh and Durfee proposed an extension on Wiener's work. It was determined that the RSA cryptosystem is insecure when $d < N^{0.292}$ by using lattice basis reduction technique [3]. In 2004, the work proposed by Blömer and May which combined lattice basis reduction techniques with continued fraction algorithm, showed that the RSA cryptosystem is insecure if there exist integers x, y and z satisfying the equation $ex - y\phi(N) = z$ with $x < \frac{1}{3}N^{1/4}$ and $|z| < exN^{-3/4}$ [16]. In cases where a single user generates many instances of RSA (N, e_i) with the same modulus and small private exponents, Howgrave-Graham and Seifert (1999) proved that the RSA cryptosystem is insecure in the presence of two decryption exponents (d_1, d_2) with $d_1, d_2 < N^{5/14}$ [6]. In the presence of three decryption exponents, they improved the bound to $N^{2/5}$ based on the lattice reduction method.

Then, in 2007, Hinek showed that it is possible to factor k RSA moduli 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 $N_i = p_i q_i$ [8]. In 2014, Nitaj et al. proposed a new method to factor k RSA moduli N_i in the scenario that the 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 suitably small parameters $x_i,\ y_i,\ z_i,\ x,\ y$ where $\phi(N_i) = (p_i - 1)(q_i - 1)$ [9]. The analysis utilized the LLL algorithm.

As described in [18] the moduli of the form $N = p^2q$ is frequently used in cryptography and therefore they represent one of the most important cases. According to May, the modulus in the general form of $N = p^r q$ with $r \geq 2$ is more insecure than $N = pq$. Nevertheless, the modulus $N = p^2q$ is still tempting to be used. Examples of schemes are the RSA-Takagi Cryptosystem (1997), Okamoto-Uchiyama cryptosystem (1998), Pailier cryptosystem(1999), HIME(R) Cryptosystem (2002), Schmidt-Samoa Cryptosystem (2006) and AA_β Cryptosystem (2012). Differing from the modulus $N = pq$, research on the security of $N = p^2q$ is still scarce. Sarkar (2014) proved that the modulus $N = p^2q$ can be factored if $d < N^{0.395}$ using lattice reduction techniques [19].

Recently, in 2015, Asbullah and Ariffin showed that one can factor $N = p^2q$ 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 $1 \leq Y \leq X < \dfrac{N^{1/2}}{2(ap^2 + bq^2)^{1/2}}$ [11].

Our contribution. Therefore, in this paper, we present new cryptanalysis on the modulus of $N = p^2q$ by using the continued fractions method as the first analysis motivated from some previous attacks by Wiener [2], Nitaj [12], [13],[14] and Asbullah and Ariffin [11]. We consider the public value, e satisfying the following generalized key 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. If

$$|p^2u - q^2v| < N^{1/2},\ X < \frac{N}{3(p^2u + q^2v)},\ |Z| < \frac{|p^2 - q^2|}{3(p^2 + q^2)} N^{1/3}.$$

then N can be factored in polynomial time using continued fraction. We also show that the number of such parameter e satisfying the following equation $eX - NY = p^2u + q^2v + Z$ 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

$$x < N^{\delta}, \quad y_i < N^{\delta}, |z_i| < \frac{|p_i^2 - q_i^2|}{3(p_i^2 + q_i^2)} N^{1/3} \text{ where } \delta = \frac{k}{3} - \alpha k, \; N = \min_i N_i$$

Finally, for the third attack, 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

$$x_i < N^{\delta}, \; y < N^{\delta}, \; |z_i| < \frac{|p_i^2 - q_i^2|}{3(p_i^2 + q_i^2)} N^{1/3} \text{ where } \delta = \beta k - \alpha k - \frac{2k}{3}.$$

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 apply lattice basis reduction techniques to find parameters (x, y_i) or (y, x_i). This leads to a suitable approximation of $p^2 u + q^2 v$ which allow us to compute the prime factor p_i and q_i of each moduli $N_i = p_i^2 q_i$. We also prove that the proposed attacks enables one to factor k RSA moduli of the form $N_i = p_i^2 q_i$ 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 convergence $\frac{a}{b}$ 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 2.1. (Legendre) [15] 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 $\frac{Y}{X}$ is convergent of x.

2.2. Lattice Basis Reductions

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

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

The set $(u_i, \ldots, u_d)$ 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 produces a reduced basis and the following result fixes the sizes of the reduced basis vector (see [17]).

Theorem 2.2. [10] Let L be a lattice of dimension ω with a basis $\{v_1, \ldots, v_\omega\}$. The LLL algorithm produces a reduced basis $\{b_1, \ldots, b_\omega\}$ satisfying

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

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 $\alpha_1, \ldots, \alpha_n$ be n real numbers and ε a real number such that $0 < \varepsilon < 1$. A classical theorem of Dirichlet asserts that there exist integers $p_1, \ldots, p_n$ and a positive integer $q \leq \varepsilon^{-n}$ such that

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

In [10] 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 2.3. (Simultaneous Diophantine Approximations). [10] There is a polynomial time algorithm, for given rational numbers $\alpha_1, \ldots, \alpha_n$ and $0 < \varepsilon < 1$, to compute integers $p_1, \ldots, p_n$ and a positive integer q such that

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

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 3.1. [11] 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. See [11]. ■

Lemma 3.2. Let $N = p^2q$ with $q < p < 2q$. Let $1 < u < q/2$, $1 < v < p/3$ 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 S be an approximation of $p^2u + q^2v$ such that

$$|p^2u + q^2v - S| < \frac{|p^2u - q^2v|}{3(p^2u + q^2v)}N^{1/3},$$

then $uvq = \left[\dfrac{S^2}{4N}\right]$.

Proof. Set $S = p^2u + q^2v + x$ with $|x| < \dfrac{|p^2u - q^2v|}{3(p^2u + q^2v)}N^{1/3}$. Notice that

$$\begin{aligned}
(p^2u - q^2v)^2 &= (p^2u - q^2v)(p^2u - q^2v) \\
&= (p^2u)^2 - 2(p^2q^2uv) + (q^2v)^2 \\
&= (p^2u)^2 + 2(p^2q^2uv) - 2(p^2q^2uv) - 2(p^2q^2uv) + (q^2v)^2 \\
&= (p^2u + q^2v)^2 - 4(p^2q^2uv) \\
&= (p^2u + q^2v)^2 - 4Nquv
\end{aligned}$$

Hence we get

$$(p^2u - q^2v)^2 = (p^2u + q^2v)^2 - 4Nquv \tag{1}$$

and consider

$$\begin{aligned}
S^2 - 4(p^2q^2uv) &= (p^2u + q^2v + x)^2 - 4Nquv \\
&= (p^2u)^2 - 2(p^2q^2uv) + (q^2v)^2 + 2xp^2u + 2xq^2v - 4Nquv \\
&= (p^2u + q^2v)^2 + 2x(p^2u + q^2v) + x^2 - 4Nquv
\end{aligned}$$

By using (1) we can rewrite the equation as

$$S^2 - 4Nquv = (p^2u - q^2v)^2 + 2x(p^2u + q^2v) + x^2 \tag{2}$$

Since $|p^2u - q^2v| < N^{1/2}$ and

$$|x| < \frac{|p^2u - q^2v|}{3(p^2u + q^2v)} N^{1/3},$$

hence we have

$$\begin{aligned}
|S^2 - 4Nquv| &= (p^2u - q^2v)^2 + 2|x|(p^2u + q^2v) + x^2 \\
&< (N^{1/2})^2 + 2(p^2u + q^2v)\frac{|p^2u - q^2v|}{3(p^2u + q^2v)} N^{1/3} + (N^{1/3})^2 \\
&< N + \frac{2}{3}(N^{1/2})N^{1/3} + N^{2/3} \\
&= N(1 + \frac{2}{3}(N^{-1/6}) + N^{-1/3} \\
&< 2N
\end{aligned}$$

Thus, we have $|S^2 - 4Nquv| < 2N$. Divide by $4N$, we get

$$\left|\frac{S^2}{4N} - uvq\right| < \frac{2N}{4N} = \frac{1}{2}$$

It follows that $uvq = \left[\frac{S^2}{4N}\right]$. This terminates the proof. ■

Lemma 3.3. Let $N = p^2q$ with $q < p < 2q$. Let

$$|p^2u + q^2v - S| < \frac{|p^2u - q^2v|}{3(p^2u + q^2v)} N^{1/3}$$

such that u is an integer multiple of 2 and v is an integer multiple of 3. Let $D = |S^2 - 4Nquv|$, then $\sqrt{D}$ is an approximation of $|p^2u - q^2v|$ where $|p^2u + q^2v - \sqrt{D}| < N^{1/3}$.

Proof. Observe that

$$\begin{aligned}
|(p^2u + q^2v)^2 - \sqrt{D}| &\leq \left|(p^2u - q^2v)^2 - |S^2 - 4Nquv|\right| \\
&\leq |(p^2u - q^2v)^2 + 4Nquv - S^2| \\
&\leq |(p^2u - q^2v)^2 - 4Nquv + 4Nquv - S^2| \\
&= |(p^2u + q^2v)^2 - S^2|
\end{aligned} \tag{3}$$

From left hand side of (3), we get

$$\left|(p^2u-q^2v)^2-D\right| = \left||p^2u-q^2v|-\sqrt{D}\right|\Big(|p^2u+q^2v|+\sqrt{D}\Big)$$

and right hand side of (3), we get

$$|(p^2u+q^2v)^2-S^2| = |p^2u+q^2v-S|(p^2u+q^2v+S)$$

Suppose that from Lemma 3.2, we have

$$|p^2u+q^2v-S| < \frac{|p^2u-q^2v|}{3(p^2u+q^2v)}N^{1/3},$$

this implies that

$$\begin{aligned}
p^2u+q^2v+S &< p^2u+q^2v+\Big(p^2u+q^2v+\frac{|p^2u-q^2v|}{3(p^2u+q^2v)}N^{1/3}\Big) \\
&< 2\Big(p^2u+q^2v\Big)+\frac{|p^2u-q^2v|}{3(p^2u+q^2v)}N^{1/3} \\
&< 2\Big(p^2u+q^2v\Big)+\frac{1}{3}N^{1/3} \\
&< 3\Big(p^2u+q^2v\Big) \qquad (4)
\end{aligned}$$

where $|p^2u-q^2v| < p^2u+q^2v$ and $p^2u+q^2v > p^2 > N^{2/3}$. Next, from (3) and (4), this implies that

$$\begin{aligned}
\left||p^2u-q^2v|-\sqrt{D}\right| &= \frac{|(p^2u+q^2v)^2-S^2|}{|p^2u-q^2v|+\sqrt{D}} \\
&\leq \frac{|(p^2u+q^2v)^2-S^2|}{|p^2u-q^2v|} \\
&< \frac{|p^2u+q^2v-S|(p^2u+q^2v+S)}{|p^2u-q^2v|} \\
&< \frac{|p^2u-q^2v|N^{1/3}\Big(3(p^2u+q^2v)\Big)}{3\Big(p^2u+q^2v\Big)|p^2u-q^2v|} \\
&= N^{1/3} \qquad (5)
\end{aligned}$$

This terminates the proof. ■

Lemma 3.4. 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 $\gcd(X, Y) = 1$. If $X < \dfrac{N}{3(p^2u+q^2v)}$ and

$$|Z| < \frac{|p^2-q^2|}{3(p^2+q^2)}N^{1/3},$$

then $\dfrac{Y}{X}$ is a convergent of the continued fraction $\dfrac{e}{N}$.

Proof. Suppose that

$$|Z| < \frac{|p^2 - q^2|}{3(p^2 + q^2)} N^{1/3}.$$

Thus, $|Z| < N^{1/3}$. Let $X < \dfrac{N}{3(p^2u + q^2v)}$. By using the equation $eX - NY = p^2u + q^2v + Z$ and if we divide by NX, then we obtain

$$\begin{aligned} \left|\frac{e}{N} - \frac{Y}{X}\right| &= \frac{|eX - NY|}{NX} \\ &= \frac{|p^2u + q^2v + Z|}{NX} \\ &\leq \frac{|p^2u + q^2v| + |Z|}{NX} \\ &\leq \frac{|(p^2u + q^2v) + N^{1/3}|}{NX} \end{aligned}$$

In order to apply Legendre Theorem, observe that

$$\begin{aligned} \left|\frac{e}{N} - \frac{Y}{X}\right| &< \frac{1}{2X^2} \\ \frac{|(p^2u + q^2v) + N^{1/3}|}{NX} &< \frac{1}{2X^2} \\ X &< \frac{N}{2(p^2u + q^2v) + N^{1/3}} \end{aligned}$$

Hence, we conclude that $\dfrac{Y}{X}$ is convergent continued fraction $\dfrac{e}{N}$. According to Lemma 3.3, such condition is satisfied for $X < \dfrac{N}{3(p^2u + q^2v)}$. This terminates the proof. ■

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

Theorem 3.5. 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 $X < \dfrac{N}{3(p^2u + q^2v)}$ and

$$|Z| < \frac{|p^2 - q^2|}{3(p^2 - q^2)} N^{1/3},$$

then N can be factored in polynomial time.

Proof. Suppose e be an exponent satisfying an equation $eX - NY = p^2u + q^2v + Z$ with $\gcd(X, Y) = 1$. Let X and $|Z|$ satisfying the condition in Lemma 3.4, 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 S is approximation of of $p^2u + q^2v$ satisfy

$$|p^2u + q^2v - S| = |Z| < \frac{|p^2u - q^2v|}{3(p^2u + q^2v)} N^{1/3} < \frac{|p^2 - q^2|}{3(p^2 + q^2)} N^{1/3} \tag{6}$$

Hence, this implies that $uvq = \left[\frac{S^2}{4N}\right]$. It follows that we obtain $q = \gcd\left(\left[\frac{S^2}{4N}\right], N\right)$. ∎

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

Table 1: Algorithm 1

INPUT: The public key modulus (N, e) satisfying $N = p^2q$ and Theorem 3.5.
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 $p = \sqrt{\frac{N}{q}}$.

Example 3.6. As an illustration of Algorithm 1, let N and e be as follows.

$$N = 64831586618801, \quad e = 52225855228363$$

Suppose that N and e satisfy all the conditions stated in Theorem 3.5. Then, we compute the continued fraction of $\frac{e}{N}$. The list of the convergent of continued fraction are shown as follows

$$\left[0, 1, \frac{4}{5}, \frac{25}{31}, \frac{29}{36}, \frac{3534}{4387}, \frac{229739}{285191}, \frac{233273}{289578}, \frac{5828291}{7235063}, \ldots\right].$$

We may omit the first and the second entry. We start with the convergent $\frac{4}{5}$ and we obtain

$$S = eX - NY = 1802929666611, \quad \left[\frac{S^2}{4N}\right] = 12534612957.$$

Hence, if we compute gcd(12534612957, 64505203569251) $= 1$. Then, we try for next convergent $\frac{25}{31}$, we obtain

$$S = eX - NY = -704132804473756, \quad \left[\frac{S^2}{4N}\right] = 1911888294710864$$

Hence, if we compute gcd(1911888294710864, 64505203569251) $= 1$. Then, we proceed with the next convergent which is $\frac{29}{36}$, we get $S = eX - NY = 14776275839$ and $\left[\frac{S^2}{4N}\right] = 841944$. Hence, we compute gcd(841944, 64505203569251) $= 35081$ which leads to the factorization of N since $q = 35081$ and $p = \sqrt{\frac{N}{q}} = 42989$.

3.1. Estimation of Weak Exponents Satisfying $eX - NY = p^2u + q^2v + Z$

Here, in this section, we give an estimation of the number of the exponents e satisfying the equation $eX - NY = p^2u + q^2v + Z$. 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 3.5.

Lemma 3.7. [14] Let m and n be positive integers. Then

$$\sum_{\substack{k=1 \\ gcd(k,\, n)=1}}^{m} 1 > \frac{cm}{(\log\log N)^2},$$

where c is a positive constant.

Proof. For a positive integer d, we denote by $\mu(d)$ be the Möbius function. This function is define by

$$\mu(d) = \begin{cases} 1, & \text{if } d = 1, \\ (-1)^{\omega(d)}, & \text{if } d \text{ is square free}, \\ 0, & \text{otherwise}, \end{cases}$$

where for an integer $d \geq 2$, $\omega(d)$ is the number of distinct prime factors of d. By using

Legendre formula, we get

$$\begin{aligned}
\sum_{\substack{k=1\\ gcd(k,\ n)=1}}^{m} 1 &= \sum_{d|n}\mu(d)\left\lfloor \frac{m}{d}\right\rfloor \\
&= \sum_{\substack{d|n\\ \mu(d)=1}} \left\lfloor \frac{m}{d}\right\rfloor - \sum_{\substack{d|n\\ \mu(d)=-1}} \left\lfloor \frac{m}{d}\right\rfloor \\
&\geq \sum_{\substack{d|n\\ \mu(d)=1}} \left(\frac{m}{d}-1\right) - \sum_{\substack{d|n\\ \mu(d)=-1}} \frac{m}{d} \\
&= \sum_{d|n}\mu(d)\frac{m}{d} - \sum_{\substack{d|n\\ \mu(d)=1}} 1
\end{aligned}$$

This leads to

$$\begin{aligned}
\omega(n) \sum_{\substack{k=1\\ gcd(k,\ n)=1}}^{m} 1 &\geq \sum_{\substack{k=1\\ gcd(k,\ n)=1}}^{m} 1 + \sum_{\substack{d|n\\ \mu(d)=1}} 1 \\
&\geq \sum_{d|n}\mu(d)\frac{m}{d} \\
&= m\sum_{d|n}\frac{\mu(d)}{d}.
\end{aligned}$$

For $n > 1$, we recall that

$$\sum_{d|n}\frac{\mu(d)}{d} = \frac{\phi(n)}{n}$$

(see 16.3.1, [15]). Hence

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

Other than that, it is well known that $\dfrac{\phi(n)}{n} > \dfrac{c_1}{\log\log n}$ ([15], Theorem 328) and $\omega(n) = c_2 \log\log n$ ([15], Theorem 430 & Theorem 431) where c_1, c_2 are positive constants. It follows that

$$\sum_{\substack{k=1\\ gcd(k,\ n)=1}}^{m} 1 > \frac{c_1 m}{c_2(\log\log n)^2} = \frac{cm}{\log\log n)^2},$$

where $c = \dfrac{c_1}{c_2}$ and the lemma follows. ■

Lemma 3.8. Let $N = p^2q$ be RSA modulus with $q < p < 2q$. Let $1 < u < q/2$ and $1 < v < p/3$ such that u is an integer multiple of 2 and v is an integer multiple of 3. For $i = 1{,}2$, let e_i be two exponents satisfying $eX_i - NY_i = p^2u + q^2v + Z_i$ with $\gcd(X_i, Y_i)$,

$$X_i < \frac{N}{3(p^2u + q^2v)}$$

and

$$|Z_i| < \frac{|p^2 - q^2|}{3(p^2 + q^2)} N^{1/3}.$$

Then $X_1 = X_2$, $Y_1 = Y_2$ and $Z_1 = Z_2$.

Proof. Suppose that e satisfying two equations

$$eX_1 - NY_1 = p^2u + q^2v + Z_1 \text{ and } eX_2 - NY_2 = p^2u + q^2v + Z_2$$

with

$$X_1, X_2 < \frac{N}{3(p^2u + q^2v)} \text{ and } |Z_1|, |Z_2| < \frac{|p^2 - q^2|}{3(p^2 + q^2)} N^{1/3}$$

Then, we eliminate e and we have

$$\frac{p^2u + q^2v + Z_1 + NY_1}{X_1} = \frac{p^2u + q^2v + Z_2 + NY_2}{X_2} \tag{7}$$

Rearrange (7), we obtain

$$(p^2u + q^2v)(X_2 - X_1) + Z_1X_2 - Z_2X_1 = N(X_1Y_2 - X_2Y_1) \tag{8}$$

Let $|p^2 - q^2| < p^2u + q^2v$ and $p^2u + q^2v < \dfrac{N}{2} + \dfrac{N}{3} < N$. Consider the left hand side of (8), the

$$\begin{aligned}
&|(p^2u + q^2v)(X_2 - X_1) + Z_1X_2 - Z_2X_1| \\
&\quad \le ((p^2u + q^2v)(X_2 + X_1)) + |Z_1X_2| + |Z_2X_1| \\
&\quad < \frac{2|p^2u + q^2v|N}{3(p^2u + q^2v)} + \frac{2|p^2 - q^2|N^{4/3}}{3(p^2u + q^2v)(p^2 + q^2)} \\
&\quad < \frac{2N}{3} + \frac{(p^2 + q^2)N^{2/3}}{3(p^2 + q^2)} \\
&\quad < \frac{2N}{3} + \frac{N^{2/3}}{3} \\
&\quad < N
\end{aligned}$$

Hence, from the right hand side of (8), we deduce $X_1Y_2 - X_2Y_1 = 0$, we get $X_1Y_2 = X_2Y_1$ and

$$(p^2u + q^2v)(X_2 - X_1) + Z_1X_2 - Z_2X_1 = 0.$$

Since $\gcd(X_1, Y_1) = \gcd(X_2, Y_2) = 1$ leads us to $X_1 = X_2$, $Y_1 = Y_2$ and finally $Z_1 = Z_2$. ■

Lemma 3.9. Let $N = p^2q$ be RSA modulus with $q < p < 2q$. Let $1 < u < q/2$ and $1 < v < p/3$ such that u is an integer multiple of 2 and v is an integer multiple of 3. For $i = 1, 2$, let e_i be two exponents satisfying

$$e_i = \left[\left(\frac{NY_i - p^2u + q^2v + Z_i}{X_i}\right)\right]$$

with $\gcd(X_i, Y_i) = 1$, $Y_i \leq X_i$ and

$$|Z_i| < \frac{|p^2 - q^2|}{3(p^2 + q^2)} N^{1/3}.$$

If $u_1 \neq u_2$ and $v_1 \neq v_2$, then $e_1 \neq e_2$.

Proof. Suppose for the contradiction that $u_1 \neq u_2$ and$v_1 \neq v_2$, and without loss of generality that $u_1 < u_2$ and $v_1 < v_2$, then

$$p^2u_1 + q^2v_1 - (p^2u_2 + q^2v_2) = p^2(u_1 - u_2) - q^2(v_1 - v_2) \leq -p^2 + q^2 \leq -(p^2 - q^2)$$

For $i = 1$,2, suppose that e satisfying two equations

$$eX_1 - NY_1 = p^2u_1 + q^2v_1 + Z_1 \; and \; eX_2 - NY_2 = p^2u_2 + q^2v_2 + Z_2$$

Then, we eliminate e and we get

$$\frac{p^2u_1 + q^2v_1 + Z_1 + NY_1}{X_1} = \frac{p^2u_1 + q^2v_1 + Z_2 + NY_2}{X_2}$$

$$\left(p^2u_1 + q^2v_1\right)X_2 + Z_1X_2 + NY_1X_2 = \left(p^2u_2 + q^2v_2\right)X_1 + Z_2X_1 + NY_2X_1$$

$$\left(p^2u_1 + q^2v_1\right)X_2 - \left(p^2u_2 + q^2v_2\right)X_1 + NY_1X_2 - NY_2X_1 = Z_2X_1 + Z_1X_2$$

Since $\frac{Y_1}{X_1}$ and $\frac{Y_2}{X_2}$ are two convergents of $\frac{e}{N}$, then $\frac{Y_1}{X_1} \approx \frac{Y_2}{X_2}$. This leads to

$$\left(p^2u_1 + q^2v_1\right)X_1 - NY_1X_1 - \left(p^2u_2 + q^2v_2\right)X_1 + NY_1X_1 = Z_2X_1 + Z_1X_1$$

$$\left(NY_1 + p^2u_1 + q^2v_1\right)X_1 - \left(NY_1 + p^2u_2 + q^2v_2\right)X_1 = \left(Z_1 - Z_2\right)X_1$$

Then

$$\Big(NY_1 - (p^2u_1 + q^2v_1)\Big) - \Big(NY_1 - (p^2u_2 + q^2v_2)\Big) \geq (p^2 - q^2) \tag{9}$$

Next

$$\Big[\Big(NY_1 - (p^2u_1 + q^2v_1)\Big) - \Big(NY_1 - (p^2u_2 + q^2v_2)\Big)\Big]X_1 = (Z_1 - Z_2)X_1$$

$$\Big[\Big(NY_1 - (p^2u_1 + q^2v_1)\Big) - \Big(NY_1 - (p^2u_2 + q^2v_2)\Big)\Big] \leq |Z_1| + |Z_2| \tag{10}$$

For the right hand side of (10) satisfies

$$|Z_1| + |Z_2| \leq \frac{|p^2 - q^2|}{3(p^2 + q^2)}N^{1/3}$$

This is contradict since, we combine with Lemma 3.1 and inequality (9) of the left hand side of (10) satisfies

$$p^2 - q^2 > N^{2/3} - \frac{N^{2/3}}{2^{2/3}} = N^{2/3} - 2^{-2/3}N^{2/3} > \frac{2|p^2 - q^2|}{3(p^2 + q^2)}N^{1/3}$$

Hence, $u_1 = u_2, v_1 = v_2$ and applying Lemma 3.8, it follows that $X_1 = X_2$ and $Y_1 = Y_2$. This terminates the proof. ■

Theorem 3.10. Let $N = p^2q$ be RSA modulus with $q < p < 2q$. The number of exponents e satisfying the equation $eX - NY = p^2u + q^2v + Z$ with

$$gcd(X, Y) = 1, 1 < u < \frac{q}{2}, 1 < v < \frac{p}{3}, X < \frac{N}{3(p^2u + q^2v)}$$

and

$$|Z| < \frac{|p^2 - q^2|}{3(p^2 + q^2)}N^{1/3}$$

is at least $N^{\frac{1}{3}-\epsilon}$, $\epsilon > 0$ is arbitrarily small for suitably large N.

Proof. Suppose the number of exponents satisfying the equation $eX - NY = p^2u + q^2v + Z$ with $\gcd(X, Y) = 1$ and $X < \dfrac{N}{3(p^2u + q^2v)}$. Then, since $X < \dfrac{1}{3}N^{1/3}$, we have $X < q$ and $\gcd(X, N) = 1$. Hence, we can express e as

$$e \equiv \frac{p^2u + q^2v + Z}{X} (\bmod N).$$

Other than that, if $e < N$, then this representation is unique. This implies that the number of such exponent is

$$\mathcal{N} = \sum_{|v=1|}^{\lfloor p/3 \rfloor} \sum_{|u=1|}^{\lfloor q/2 \rfloor} \sum_{|Z|=1}^{B_1} \sum_{\substack{X=1 \\ gcd(X,\ p^2u+q^2v+Z)=1}}^{B_2} 1, \tag{11}$$

where

$$B_1 = \left\lfloor \frac{|p^2 - q^2|}{3(p^2 + q^2)} N^{1/3} \right\rfloor \quad \text{and} \quad B_2 = \left\lfloor \frac{N}{3(p^2 u + q^2 v)} \right\rfloor.$$

Then, by using Lemma 3.7 with $m = B_2$ and $n = p^2 u + q^2 v + Z$, we have

$$\sum_{\substack{X=1 \\ gcd(X,\ p^2u+q^2v+Z)=1}}^{B_2} 1 > \frac{cB_2}{(\log \log |p^2 u + q^2 v + Z|)^2} > \frac{cB_2}{(\log \log N)^2} \tag{12}$$

where c is a constant ([15], Theorem 328). Then, we substitute (12) in (11), we obtain

$$\mathcal{N} > \frac{cB_2}{(\log \log N)^2} \sum_{|v=1|}^{\lfloor p/3 \rfloor} \sum_{|u=1|}^{\lfloor q/2 \rfloor} \sum_{|Z|=1}^{B_1} B_2 \tag{13}$$

Now, we have

$$\begin{aligned} \sum_{|Z|=1}^{B_1} B_2 = 2B_2 B_1 &= 2\left\lfloor \frac{|p^2 - q^2|}{3(p^2 + q^2)} N^{1/3} \right\rfloor \left\lfloor \frac{N}{3(p^2 u + q^2 v)} \right\rfloor \\ &> 2\left(\frac{N^{1/3}}{3(p^2 + q^2)} \right) \left(\frac{N}{6p^2 |u|} \right) \\ &> 2\left(\frac{N^{1/3}}{3(p^2 + q^2)} \right) \left(\frac{N^{1/3}}{6 \times 2^{2/3} |u|} \right) \end{aligned} \tag{14}$$

where we used $|p^2 u + q^2 v| < 2p^2 u$ and $p < 2^{1/3} N^{1/3}$ for $|u| < \frac{q}{2}$. Next, we substitute (14) in (13), we obtain

$$\mathcal{N} > \frac{2N^{2/3}}{18(p^2 + q^2)} \times \frac{c}{(\log \log N)^2} \sum_{|v=1|}^{\lfloor p/3 \rfloor} \sum_{|u=1|}^{\lfloor q/2 \rfloor} \frac{1}{|u|} \tag{15}$$

By using the estimation

$$\sum_{x=1}^{n} \frac{1}{x} \geq \log n$$

we get

$$\sum_{|u=1|}^{\lfloor q/2 \rfloor} \frac{1}{|u|} > 2 \log \left(\left\lfloor \frac{1}{2} q \right\rfloor \right) > \log(2q) > \log\,(2^{2/3} N^{1/3})$$

where we used $q > 2^{-1/3} N^{1/3}$. Then we plug in (15), we obtain

$$\mathcal{N} > \frac{c \log\,(2^{2/3} N^{1/3})}{9 \times 2^{2/3}\,(\log \log N)^2} \times \frac{N^{2/3}}{(p^2 + q^2)} \sum_{|v=1|}^{\lfloor p/3 \rfloor} 1 \tag{16}$$

Now, for $|v| < \frac{p}{3}$, we have

$$\sum_{|v=1|}^{\lfloor p/3 \rfloor} 1 = 2\left(\left\lfloor \frac{p}{3} \right\rfloor\right) > \frac{p}{3} > \frac{1}{3}(N^{1/3}) = \frac{N^{1/3}}{3} \tag{17}$$

Then, we substitute (17) in (16), we get

$$\mathcal{N} > \frac{c \log (2^{2/3}N^{1/3})}{9 \times 2^{2/3} (\log \log N)^2} \times \frac{N^{2/3}(N^{1/3})}{3(p^2 + q^2)}$$

Since $(p^2 + q^2) < p^2 + p^2 < 2p^2 < 2(2^{1/3}N^{1/3})^2 = 2^{5/3}N^{2/3}$, we get

$$\begin{aligned} \mathcal{N} &> \frac{c \log (2^{2/3}N^{1/3})}{9 \times 2^{2/3} (\log \log N)^2} \times \frac{N^{2/3}(N^{1/3})}{3(2^{5/3}N^{2/3})} \\ &> \frac{c \log (2^{2/3}N^{1/3})}{27 \times 2^{7/3} (\log \log N)^2} \times N^{1/3} \\ &> \frac{c}{81 \times 2^{7/3} (\log \log N)^2} \times N^{1/3} \log N = N^{\frac{1}{3}-\varepsilon} \end{aligned}$$

where

$$N^{-\varepsilon} = \frac{c \log N}{81 \times 2^{7/3} (\log \log N)^2},$$

$\varepsilon > 0$ is arbitrarily small for large N. This terminates the proof. ■

4. The Second Attack

In this section, we propose our second attack. Given k moduli $N_i = p_i^2 q_i$, we consider 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, it is possible to factor k RSA moduli $N_i = p_i^2 q_i$ when the unknown parameters x, y_i and z_i are suitably small coupled with the execution of the LLL algorithm to achieve our objective.

Theorem 4.1. For $k \geq 2$, let $N_i = p_i^2 q_i$, $1 \leq i \leq k$ be k RSA moduli. Let $N = \min_i N_i$. Let e_i, $i = 1, \ldots, k$ be k public exponents. Define $\delta = \frac{k}{3} - \alpha k$. Let $1 < u < \frac{q_i}{2}$, $1 < v < \frac{p_i}{3}$ such that u is an integer multiple of 2 and v is an integer multiple of 3. If there exist an integer $x < N^{\delta}$, k integers $y_i < N^{\delta}$ and $|z_i| < \frac{|p_i^2 - q_i|}{3(p_i^2 + q_i)} N^{1/3}$ such that $e_i x - N_i y_i = p_i^2 u + q_i^2 v + z_i$, then one can factor the k RSA moduli $N_1, \ldots, N_k$ in polynomial time.

Proof. For $k \geq 2$ and $i = 1, \ldots, k$, satisfying $e_i x - N_i y_i = p_i^2 u + q_i^2 v + z_i$, we obtain

$$\left|\frac{e_i}{N_i}x - y_i\right| = \frac{|p_i^2 u + q_i^2 v + z_i|}{N_i} \tag{18}$$

Let $N = \min_i N_i$ and suppose that $y_i < N^\delta$ and

$$|z_i| < \frac{|p_i^2 - q_i|}{3(p_i^2 + q_i)} N^{1/3}.$$

Then, $|z_i| < N^{1/3}$. Since

$$p_i^2 u + q_i^2 v < N^{\frac{2}{3}+\alpha},$$

we will get

$$\begin{aligned} \frac{|z_i + (p_i^2 u + q_i^2 v)|}{N_i} &\leq \frac{|z_i + (p_i^2 u + q_i^2 v)|}{N} \\ &\leq \frac{N^{1/3} + (N^{\frac{2}{3}+\alpha})}{N} \leq \frac{2N^{\frac{2}{3}+\alpha}}{N} \\ &= 2N^{-\frac{1}{3}+\alpha} \end{aligned} \tag{19}$$

Plugging (19) in (18), we obtain

$$\left|\frac{e_i}{N_i}x - y_i\right| = 2N^{-\frac{1}{3}+\alpha}$$

We now proceed to prove the existence of integer x. Let

$$\varepsilon = 2N^{-\frac{1}{3}+\alpha}, \delta = \frac{k}{3} - \alpha k.$$

We have

$$N^\delta \cdot \varepsilon^k = 2^k N^{\delta - \frac{k}{3} + k\alpha} = 2^k$$

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

$$N^\delta \cdot \varepsilon^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k.$$

It follows that if $x < N^\delta$, then $x < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \varepsilon^{-k}$. Summarizing for $i = 1, \ldots, k$, 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 2.3 are fulfilled will find x and y_i for $i = 1, \ldots, k$. Next, using the equation

$$e_i x - N_i y_i = p_i^2 u + q_i^2 v + z_i,$$

we get

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

Since

$$|z_i| < \frac{|p_i^2 - q_i|}{3(p_i^2 + q_i)} N^{1/3}$$

and $S_i = e_i x - N_i y_i$ is an approximation of $p_i^2 u + q_i^2 v$. Hence, by using Lemma 3.2 and Theorem 3.5, this implies that $uvq = \left[\frac{S^2}{4N}\right]$ for $S_i = e_i x - N_i y_i$ for each $i = 1, \ldots, k$, 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 $N_1, \ldots, N_k$. This terminates the proof. ∎

Example 4.2. As an illustration of the second attack on k RSA moduli N_i, we consider the following three RSA moduli and public exponents

$$\begin{aligned}
N_1 &= 1400742782080665789343022192434516043499947,\\
N_2 &= 2279746570995468792879925323043292835208673,\\
N_3 &= 1152072803752719362173502377186937222271691,\\
e_1 &= 1224890034595389013471562136601153748383222,\\
e_2 &= 1446871822661790608301665147940753062778322,\\
e_3 &= 675925885409513490783380360180834071679811.
\end{aligned}$$

Then, $N = \max(N_1, N_2, N_3) = 2279746570995468792879925323043292835208673$. Since $k = 3$ and $\alpha < 1/3$, we get $\delta = \frac{k}{3} - \alpha k = \frac{1}{4}$ and $\varepsilon = 2N^{-\frac{1}{3}+\alpha} \approx 0.000715384371299$. Set $u = 40$ and $v = 60$. Then, by using (22) with $n = k = 3$, we find

$$C = \left[3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1}\right] = 154631237294596.$$

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

$$K = \begin{bmatrix} 20851016390 & 6926039718 & 7732916632 & 3684485588 \\ 4189589029 & 25975280415 & -28739664882 & -16968110412 \\ 13554125657 & -46415456621 & -4111981582 & -17369686412 \\ -3602798513 & -6142771903 & 42076034382 & -68116796780 \end{bmatrix}.$$

Now, we obtain

$$K \cdot M^{-1} = \begin{bmatrix} 20851016390 & 18233327713 & 13233377987 & 12233377673 \\ 4189589029 & 3663617558 & 2658979025 & 2458049235 \\ 13554125657 & 11852506868 & 8602308144 & 7952261659 \\ -3602798513 & -3150494189 & -2286564532 & -2113776809 \end{bmatrix}.$$

From the first row, we deduce $x = 20851016390$, $y_1 = 18233327713$, $y_2 = 13233377987$ and $y_3 = 12233377673$. 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 applying Lemma 3.2 and Theorem 3.5, this implies that $uvq = \left[\frac{S^2}{4N}\right]$ for $S_i = e_i x - N_i y_i$. Then, we get

$$\begin{aligned} S_1 &= 232630468379538676645636916369, \\ S_2 &= 342395983944160748742312443829, \\ S_3 &= 225309644357222482847794853547. \end{aligned}$$

Next, for each $i = 1, 2, 3$, we find $\left[\frac{S_i^2}{4N_i}\right]$ and we get

$$\left[\frac{S_1^2}{4N_1}\right] = 96586138994944800, \left[\frac{S_2^2}{4N_2}\right] = 128561449891663200,$$

$$\left[\frac{S_3^2}{4N_3}\right] = 110158914599450400.$$

Then, also for each $i = 1, 2, 3$, we find

$$q_i = \gcd\left(\left[\frac{S_i^2}{4N_i}\right], N_i\right)$$

and we obtain

$$q_1 = 40244224581227, q_2 = 53567270788193$$

and $q_3 = 45899547749771$. This leads us to the factorization of three RSA moduli N_1, N_2 and N_3 which $p_1 = 58996658535481$, $p_2 = 65236931548931$, and $p_3 = 50099773115039$.

5. The Third Attack

In this section, we propose our third attack. Given k moduli $N_i = p_i^2 q_i$, we consider 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, 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 5.1. For $k \geq 2$, let $N_i = p_i^2 q_i$, $1 \leq i \leq k$ be k RSA moduli with the same size N. Let e_i, $i = 1, \ldots, k$ be k public exponents with $\min_i e_i = N^{\beta}$. Define $\delta = \beta k - \alpha k - \frac{2k}{3}$. Let $1 < u < \frac{q_i}{2}$, $1 < v < \frac{p_i}{3}$ 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

$$|z_i| < \frac{|p_i^2 - q_i|}{3(p_i^2 + q_i)} N^{1/3}$$

such that

$$e_i x_i - N_i y = p_i^2 u + q_i^2 v + z_i$$

for $i = 1, \ldots, k$, then one can factor the k RSA moduli $N_1, \ldots, N_k$ in polynomial time.

Proof. For $k \geq 2$ and $i = 1, \ldots, k$, the equation

$$e_i x_i - N_i y = p_i^2 u + q_i^2 v + z_i,$$

we get

$$\left| \frac{N_i}{e_i} y - x_i \right| = \frac{|p_i^2 u + q_i^2 v + z_i|}{e_i} \tag{20}$$

Let $N = \max_i N_i$ and suppose that $y < N^{\delta}$ and

$$|z_i| < \frac{|p_i^2 - q_i|}{3(p_i^2 + q_i)} N^{1/3}.$$

Then, $|z_i| < N^{1/3}$. Also, suppose that $\min_i e_i = N^{\beta}$. Since

$$p_i^2 u + q_i^2 v < N^{\frac{2}{3}+\alpha},$$

we will get

$$\begin{aligned} \frac{|p_i^2 u + q_i^2 v + z_i|}{e_i} &\leq \frac{|z_i| + p_i^2 u + q_i^2 v}{N^{\beta}} \\ &< \frac{N^{1/3} + (N^{\frac{2}{3}+\alpha})}{N^{\beta}} \\ &< \frac{2N^{\frac{2}{3}+\alpha}}{N^{\beta}} \\ &= 2N^{\frac{2}{3}+\alpha-\beta} \end{aligned} \tag{21}$$

Plugging (21) in (20), we obtain

$$\left| \frac{N_i}{e_i} y - x_i \right| = 2N^{\frac{2}{3}+\alpha-\beta}.$$

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

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

Then, since $2^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k$ 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 2.3 are fulfilled will find y and x_i for $i = 1, \ldots, k$. Next, using the equation

$$e_i x_i - N_i y = p_i^2 u + q_i^2 v + z_i,$$

we get

$$(ap_i^2 + bq_i^2) - N_i y + e_i x_i = z_i.$$

Since

$$|z_i| < \frac{|p_i^2 - q_i|}{3(p_i^2 + q_i)} N^{1/3}$$

and $S_i = e_i x_i - N_i y$ is an approximation of $p_i^2 u + q_i^2 v$. Hence, by using Lemma 3.2 and Theorem 3.5 this implies that $uvq = \left[\dfrac{S^2}{4N}\right]$ since $S_i = e_i x_i - N_i y$ for each $i = 1, \ldots, k$, 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 $N_1, \ldots, N_k$. This terminates the proof. ■

Example 5.2. As an illustration of this third attack on k RSA moduli N_i, we consider the following three RSA moduli and public exponents

$$\begin{aligned}
N_1 &= 16751359767960963517446785725583846485 7557, \\
N_2 &= 1621937119427431529493441697364435560 34929, \\
N_3 &= 2151500252648680358954471818236690070 36303, \\
e_1 &= 1306217359766435474676760844352350700 75545, \\
e_2 &= 1296459278425452533081245110307377983 04949, \\
e_3 &= 1810613880468773969660489020645298077 19640.
\end{aligned}$$

Then, $N = \max(N_1, N_2, N_3) = 215150025264868035895447181823669007036303$. We also obtain $\min(e_1, e_2, e_3) = N^{\beta}$ with $\beta \approx 0.9946777661$. Since $k = 3$ and $\alpha <$

$1/3$, we get $\delta = \beta k - \alpha k - \dfrac{2k}{3} = 0.234033298$ and $\varepsilon = 2N^{\frac{2}{3}+\alpha-\beta} \approx 0.0011929366910476$. Set $u = 24$ and $v = 36$. Then, by using (22) with $n = k = 3$, we find

$$C = \left[3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1}\right] = 19997948141251.$$

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

$$K = \begin{bmatrix} -3186595759 & -3175535180 & -2508543925 & -2476344545 \\ 3597868419 & 8192169166 & -5374188372 & -4451292135 \\ -5980436867 & 8290726243 & 881173597 & -2602034148 \\ 8196227911 & 1329332700 & 4686046277 & -11477132170 \end{bmatrix}.$$

Now, we obtain

$$K \cdot M^{-1} = \begin{bmatrix} -3186595759 & -4086594899 & -3986594899 & -3786539833 \\ 3597868419 & 4614024445 & 4501118112 & 4275243273 \\ -5980436867 & -7669508354 & -7481833565 & -7106380642 \\ 8196227911 & 10511111451 & 10253901923 & 9739341232 \end{bmatrix}.$$

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 applying Lemma 3.2 and Theorem 3.5, this implies that $uvq = \left[\dfrac{S^2}{4N}\right]$ for $S_i = e_i x_i - N_i y$. We get

$$\begin{aligned} S_1 &= 172955024052703147678372558270, \\ S_2 &= 163577818481355525216922589040, \\ S_3 &= 205759285452509704623457581143. \end{aligned}$$

Next, for each $i = 1, 2, 3$, we find $\left[\dfrac{S_i^2}{4N_i}\right]$ and we get

$$\left[\frac{S_1^2}{4N_1}\right] = 44643301737039072,$$

$$\left[\frac{S_2^2}{4N_2}\right] = 41243434129809504,$$

$$\left[\frac{S_3^2}{4N_3}\right] = 49194606760802208.$$

For each $i = 1, 2, 3$, we find

$$q_i = \gcd\left(\left[\frac{S_i^2}{4N_i}\right], N_i\right)$$

and we obtain

$$q_1 = 51670488121573, q_2 = 47735456168761,$$

and $q_3 = 56938202269447$. This leads us to the factorization of three RSA moduli N_1, N_2 and N_3 which $p_1 = 56938202269447$, $p_2 = 58290323825483$ and $p_3 = 61470794347307$.

6. Conclusion

In conclusion, this paper presents three new attacks on RSA moduli type $N = p^2q$. The first attack is based on the equation $eX - NY = p^2u + q^2v + Z$ 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] Rivest, R., Shamir, A. and Adleman, L., A method for obtaining digital signatures and public-key cryptosystems, Communication of the ACM 21(2), 21(2):17–28 (1978)

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

[3] Boneh, D. and Durfee, G.,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 (1999)

[4] Boneh, D., Twenty years of attacks on the RSA cryptosystem, Notices of the AMS, 46(2):203–213 (1999).

[5] de Weger, B., Cryptanalysis of RSA with small prime difference, Applicable Algebra in Engineering Communication and Computing, 13(1), 1728 (2002)

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

[7] Sarkar, S. and Maitra, S., Cryptanalysis of RSA with two decryption exponents, Information Processing Letters, Vol. 110, 178–181 (2010)

[8] Hinek, J., On the security of some variants of RSA, PhD thesis, Waterloo, Ontario, Canada (2007)

[9] Nitaj, A., Ariffin, M. R. K., Nassr, D. I. and Bahig, H. M., New attacks on the RSA cryptosystem, Lecture Notes in Computer Science, Vol. 8469 Springer Verlag, pp. 178–198 (2014)

[10] Lenstra, A. K., Lenstra, H. W. and Lovász, L., Factoring polynomials with rational coefficients, Mathematische Annalen, vol. 261, pp.513–534 (1982)

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

[12] Nitaj, A., Cryptanalysis of RSA using the ratio of the primes, In Progress in Cryptology - AFRICACRYPT 2009, pages 98–115, Springer (2009)

[13] Nitaj, A., A new vulnerable class of exponents in RSA, JP Journal of Algebra, Number Theory and Applications, 21(2):203–220 (2011a)

[14] Nitaj, A., New weak RSA keys, JP Journal of Algebra, Number Theory and Applications, 23(2):131–148 (2011b)

[15] Hardy, G. and Wright, E., An introduction to the theory of numbers, Oxford University Press, London (1965)

[16] Blömer, J. and May, A., A generalized Wiener attack on RSA, Practice and Theory in Public Key Cryptography PKC 2004 LNCS Springer-Verlag, 2947:1–13, (2004).

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

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

[19] Sarkar, S., Small secret exponent attack on RSA variant with modulus $N = p^r q$, Designs, Codes and Cryptography, 73(2):383–392, Springer (2014).

Appendix

Proof of Theorem 2.3.

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

$$C = \left\lceil 3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1} \right\rceil \tag{22}$$

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 $(b_1, \ldots, b_{n+1})$ 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 $b_1 = \pm[q, p_1, p_2, \ldots, p_n]M$, that is

$$b_1 = \pm[q, Cp_1 - q[C\alpha_1], Cp_2 - q[C\alpha_2], \ldots, Cp_n - q[C\alpha_n]], \tag{23}$$

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

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

which leads to

$$q \leq \left\lfloor 2^{n/4}C^{n/(n+1)} \right\rfloor \text{ and } \max_i |Cp_i - q[C\alpha_i]| \leq 2^{n/4}C^{n/(n+1)}. \tag{24}$$

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

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

Using the two inequalities in (22), we get

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

Observe that (25) gives

$$3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1} \leq C \leq\leq 3^{n+1} \cdot 2^{\frac{(n+1)(n-3)}{4}} \cdot \varepsilon^{-n-1}, \tag{25}$$

which leads to $\varepsilon \geq \dfrac{3 \cdot 2^{(n-4)/4}}{C^{1/(n+1)}}$. As a consequence, we get $|q\alpha_i - p_i| \leq \varepsilon$. On the other hand, using (24) and (25), we get

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

To compute the vector $[q, p_1, p_2, \ldots, p_n]$, we use (23)

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

This terminates the proof. ■