Malaysian Journal of Mathematical Sciences 11(S) August: 75 - 88 (2017)
Special Issue: The 5th International Cryptology and Information Security Conference (New Ideas in Cryptology)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

New Vulnerability of RSA Modulus Type $N = p^2q$

Rahman, N. N. A. R.[*1] and **Ariffin, M. R. K.**[1,2]

[1]*Laboratory of Cryptology, Analysis and Structure, Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia*
[2]*Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, Malaysia*

E-mail: *mahirah_mayrah@yahoo.com, rezal@upm.edu.my
Corresponding author

ABSTRACT

This paper proposes new attacks on modulus of type $N = p^2q$. Given k moduli of the form $N_i = p_i^2q_i$ for $k \geq 2$ and $i = 1, ..., k$, the attack works when k public keys (N_i, e_i) are such that there exist k relations of the shape $e_ix - N_iy_i = z_i - (ap_i^2 + bq_i^2)y_i$ or of the shape $e_ix_i - N_iy = z_i - (ap_i^2 + bq_i^2)y$ where the parameters x, x_i, y, y_i and z_i are suitably small in terms of the prime factors of the moduli. The proposed attacks utilizing the LLL algorithm enables one to factor the k moduli N_i simultaneously.

Keywords: Factorization, modulus $N = p^2q$, LLL algorithm, Simultaneous diophantine approximations.

1. Introduction

The RSA cryptosystem was developed by Rivest et al. (1978) is the well-known public key cryptosystem. 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 $ed + 1 = \phi(N)k$.

RSA is most commonly used for providing privacy and ensuring authenticity of digital data. Hence, 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. 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 instance 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, $d < N^{1/4}$. Later, by using lattice basis reduction technique, Boneh and Durfee (1999) proposed an extension on Wiener's work. It was determined that the RSA cryptosystem is insecure when $d < N^{0.292}$. The work proposed by Blömer and May (2004) 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 $|z| < exN^{-3/4}$. 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 $d_1, d_2 < N^{5/14}$. In the presence of three decryption exponents, they improved the bound to $N^{2/5}$ based on the lattice reduction method.

Then, Hinek (2007) 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 $N_i = p_i q_i$. Later, Nitaj et al. (2014) 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 $e_ix_i - y\phi(N_i) = z_i$ with suitably small parameters x_i, y_i, z_i, x, y where $\phi(N_i) = (p_i - 1)(q_i - 1)$. The analysis utilized the LLL algorithm.

As described in May (2004) the moduli of the form $N = p^2q$ is frequently used in cryptography and therefore they represent one of the most important cases. In this work, we will look at a variant of the RSA modulus of the form $N = p^2q$. Examples of schemes that utilize the modulus $N = p^2q$ are Fujioke, Okamoto and Miyaguchi Cryptosystem(1991), RSA-Takagi Cryptosystem (1997), Okamoto-Uchiyama Cryptosystem (1998), HIME(R) Cryptosystem (2002), Schmidt-Samoa Cryptosystem (2006) and AA_β Cryptosystem (2012).

Variant designs of the RSA utilizing $N = p^2q$ exist because of various reasons. For example the HIME(R) design became a standard in Japan because it was able to "carry" more data securely than the existing RSA. On the other hand, Takagi (1998) showed that the decryption process is about three times faster than RSA cryptosystem using CRT if they choose the 768-bit modulus p^2q for 256-bit primes p and q. Additionally, AA_β Cryptosystem that has been proposed by Ariffin et al. (2013) overcome Rabin's cryptosystem decryption failure which was due to a 4-to-1 mapping by incorporating the hardness of factoring integer $N = p^2q$ coupled with the square root problem as its cryptographic primitive. The design for encryption does not involve "expensive" mathematical operation.

Our contribution. Hence, in this paper, we introduce new attacks to factor k moduli of the form $N_i = p_i^2q_i$. The first attack is upon k-instances (N_i, e_i). The attack works when there exist an integer x, k integers y_i and k integers z_i satisfying $e_ix - N_iy_i = z_i - (ap_i^2 + bq_i^2)y_i$. We show that the k moduli $N_i = p_i^2q_i$ can be factored in polynomial time

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

with $N = \min_i N_i$.

The second attack works when there exist an integer y, k integers x_i and k integers z_i satisfying $e_ix_i - N_iy = z_i - (ap_i^2 + bq_i^2)y$. Similarly, we show that the k moduli $N_i = p_i^2q_i$ can be factored in polynomial time

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

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

For both attacks, 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 $ap^2 + bq^2$ which allow us to apply a theorem proposed by Asbullah (2015) in order to compute the prime factor p_i and q_i of each $N_i = p_i^2 q_i$ simultaneously.

The layout of the paper is as follows. In Section 2, we begin with a brief review on lattice basic reduction and simultaneous diophantine approximation and also some useful results that will be used throughout the paper. In Section 3 and Section 4, we present our first and second attacks 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 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 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 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

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

Lenstra, Lenstra and Lovász described a method to find simultaneous diophantine approximations to rational numbers which they consider a lattice with real entries (Lenstra et al. (1982)). Later, in Nitaj et al. (2014) state a similar result for a lattice with integer entries as in the following theorem.

Theorem 2.2. (Simultaneous Diophantine Approximations). *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. □

2.2 Approximation of The Prime in RSA

The following is a result by Asbullah (2015) which is the basis of our analysis is given in the first and second attack on k moduli $N_i = p_i^2q_i$. The following lemma shows that any approximation of ap^2+bq^2 will lead to an approximation of q and Theorem 2.3 is an attack on $N = p^2q$ via generalized key equation $eX - NY = Z - (ap^2 + bq^2)Y$.

Lemma 2.1. (Asbullah, 2015). *Let* $N = p^2q$ *with* $q < p < 2q$. *Let* a, b *be suitable small integers with* $\gcd(a, b) = 1$. *Let* $|ap^2 - bq^2| < N^{1/2}$. *Let* S *be an approximation of* $ap^2 + bq^2$ *such that* $|ap^2 + bq^2 - S| < \frac{|ap^2-bq^2|}{3(ap^2+bq^2)}N^{1/3}$, *then* $abq = \left[\frac{S^2}{4N}\right]$.

Proof. See Asbullah (2015). □

Theorem 2.3. (Asbullah, 2015). *Let* $N = p^2q$ *with* $q < p < 2q$. *Let* a, b *be integers with* $\gcd(a, b) = 1$ *such that* $|ap^2 - bq^2| < N^{1/2}$. *Let* e *be a public exponent satisfying the equation* $eX - NY = Z - (ap^2 + bq^2)Y$ *with* $\gcd(X, Y) = 1$. *If* $1 \leq Y \leq X < \frac{N^{1/2}}{2(ap^2+bq^2)^{1/2}}$ *and* $|Z| < \frac{|ap^2-bq^2|}{3(ap^2+bq^2)}N^{1/3}Y$, *then* N *can be factored in polynomial time.*

Proof. See Asbullah (2015). □

3. The First Attack on k Moduli $N_i = p_i^2q_i$

In this section, we extend Asbullah (2015) work via Theorem 3.1. Suppose that we are given k moduli $N_i = p_i^2q_i$ each with the same size N where $N =$

$\min_i N_i$. We consider in this scenario, the k moduli satisfy k equations $e_i x - N_i y_i = z_i - (ap_i^2 + bq_i^2)y_i$. We show that it is possible to factor each moduli $N_i = p_i^2 q_i$ if the unknown parameters x, y_i and z_i are suitably small.

Theorem 3.1. *Suppose $k \geq 2$, $N_i = p_i^2 q_i$, $1 \leq i \leq k$ be k moduli each with the same size N where $N = \min N_i$. Assume e_i, $i = 1, ..., k$ be k public exponents. Define $\delta = \frac{k-3\alpha k}{3(1+k)}$. Let a, b be suitable small integers with $\gcd(a, b) = 1$ such that $ap_i^2 + bq_i^2 < N^{\frac{2}{3}+\alpha}$ with $0 < \alpha < 1/3$. If exist an integer $x < N^{\delta}$, k integers $y_i < N^{\delta}$ and $|z_i| < \frac{|ap_i^2 - bq_i^2|}{3(ap_i^2+bq_i^2)} N^{1/3} y_i$ such that*

$$e_i x - N_i y_i = z_i - (ap_i^2 + bq_i^2)y_i \quad \text{for} \quad i = 1, ..., k,$$

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

Proof. Suppose $k \geq 2$ and $i = 1, ..., k$ and the equation $e_i x - \Big(N_i - (ap_i^2 + bq_i^2)\Big)y_i = z_i$ can be written as $e_i x - N_i y_i = z_i - (ap_i^2 + bq_i^2)y_i$. Hence,

$$\left| \frac{e_i}{N_i} x - y_i \right| = \frac{|z_i - y_i(ap_i^2 + bq_i^2)|}{N_i} \tag{1}$$

Let $N = \min N_i$ and suppose that $y_i < N^{\delta}$ and $|z_i| < \frac{|ap_i^2 - bq_i^2|}{3(ap_i^2+bq_i^2)} N^{1/3} y_i$. Then, $|z_i| < y_i N^{1/3} < N^{\delta + \frac{1}{3}}$. We set $ap_i^2 + bq_i^2 < N^{\frac{2}{3}+\alpha}$ with $0 < \alpha < 1/3$, we will get

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

Plugging (2) in (1), we obtain

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

In order to show the existence of integer x, let $\varepsilon = 2N^{\delta-\frac{1}{3}+\alpha}$, $\delta = \frac{k-3\alpha k}{3(1+k)}$. We have

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

Then, since $2^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k$ for $k \geq 2$, by Theorem 2.2 we get $N^\delta \cdot \varepsilon^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k$. It follows that if $x < N^\delta$, then $x < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \varepsilon^{-k}$. Next, for $i = 1, ..., k$, we obtain

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

If the condition of Theorem 2.2 are fulfilled, then this lead us to find x and y_i for $i = 1, ..., k$. Next, using the equation $e_i x - \Big(N_i - (ap_i^2 + bq_i^2)\Big) y_i = z_i$, we get

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

Since $|z_i| < \frac{|ap_i^2 - bq_i^2|}{3(ap_i^2 + bq_i^2)} N^{1/3} y_i$ then $\frac{z_i}{y_i} < \frac{|ap_i^2 - bq_i^2|}{3(ap_i^2 + bq_i^2)} N^{1/3}$ and $S_i = N_i - \frac{e_i x}{y_i}$ is an approximation of $ap_i^2 + bq_i^2$. Hence, by using Lemma 2.1 and Theorem 2.3, this implies that $abq = \left\lceil \frac{S^2}{4N} \right\rceil$ for $S_i = N_i - \frac{e_i x}{y_i}$, $i = 1, ..., k$, we compute $q_i = \gcd\Big(\left\lceil \frac{S_i^2}{4N_i} \right\rceil, N_i\Big)$. Therefore, it is possible us to factor k moduli $N_1, ..., N_k$. This terminates the proof. □

Example 3.1. *As an illustration of our proposed attack, we consider the following three moduli and three public exponents*

$$\begin{aligned}
N_1 &= 3876679304397305665012058878 7, \\
N_2 &= 4544563494402792723389167561 1, \\
N_3 &= 4288178816431580712188089951 7, \\
e_1 &= 1144543412130735120370492063 5, \\
e_2 &= 1659126352970611658426089963 7, \\
e_3 &= 2954078736343968696537912951 8.
\end{aligned}$$

Then, $N = \min(N_1, N_2, N_3) = 38766793043973056650120588787$. *Suppose* $k = 3$, *we obtain* $\delta = \frac{k - 3\alpha k}{3(1+k)} = \frac{1}{10}$ *and* $\varepsilon = 2N^{\delta - \frac{1}{3} + \alpha} \approx 0.2228852521821256$. *By using (5) from the proof of Theorem 2.2 and* $n = k = 3$, *we find*

$$C = \left\lceil 3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1} \right\rceil = 16410.$$

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

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

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

$$K = \begin{bmatrix} 315 & 270 & 300 & 210 \\ -874 & -124 & 470 & 876 \\ 556 & -2024 & 790 & 6 \\ 1318 & -902 & -1610 & 1608 \end{bmatrix}.$$

Now, we obtain

$$K \cdot M^{-1} = \begin{bmatrix} 315 & 93 & 115 & 217 \\ -874 & -258 & -319 & -602 \\ 556 & 164 & 203 & 383 \\ 1318 & 389 & 481 & 908 \end{bmatrix}.$$

According to the first row of the above matrix, we obtain $x = 315$, $y_1 = 93$, $y_2 = 115$ and $y_3 = 217$. By applying x and y_i for $i = 1, 2, 3$, we look at the relation $S_i = N_i - \frac{e_i x}{y_i}$ is an approximation of $ap_i^2 + bq_i^2$. Hence, by using Lemma 2.1 and Theorem 2.3, this implies that $abq = \left[\frac{S^2}{4N}\right]$ for $S_i = N_i - \frac{e_i x}{y_i}$. Then, we obtain

$$\begin{aligned} \left[\frac{S_1^2}{4N_1}\right] &= 17739468498, \\ \left[\frac{S_2^2}{4N_2}\right] &= 18704727714, \\ \left[\frac{S_3^2}{4N_3}\right] &= 18346150398. \end{aligned}$$

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

$$q_1 = 2956578083, \quad q_2 = 3117454619, \quad q_3 = 3057691733.$$

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

$$p_1 = 3621056167, \quad p_2 = 3818088737 \quad p_3 = 3744894557.$$

4. The Second Attack on k Moduli $N_i = p_i^2 q_i$

In this section, we consider the scenario when k moduli of the form $N_i = p_i^2 q_i$ satisfy k equations of the form $e_i x_i - N_i y = z_i - (ap_i^2 + bq_i^2)y$ where the

parameters x_i, y and z_i are suitably small unknown parameters.

Theorem 4.1. *Suppose that $k \geq 2$ and $N_i = p_i^2 q_i$, $1 \leq i \leq k$ be k moduli each with the same size N where $N = \max N_i$. Assume e_i, $i = 1, ..., k$ be k public exponents with $\min e_i = N^\beta$. Define $\delta = \frac{k(3\beta-2-3\alpha)}{3(k+1)}$. Let a, b be suitable small integers with $\gcd(a, b) = 1$ such that such that $ap_i^2 + bq_i^2 < N^{\frac{2}{3}+\alpha}$ with $0 < \alpha < 1/3$. For $i = 1, ..., k$, if there exist k integer $x_i < N^\delta$, an integer $y < N^\delta$ and $|z_i| < \frac{|ap_i^2 - bq_i^2|}{3(ap_i^2+bq_i^2)} N^{1/3} y$ such that*

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

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

Proof. Suppose $k \geq 2$ and $i = 1, ..., k$, the equation $e_i x_i - \Big(N_i - (ap_i^2 + bq_i^2)\Big)y = z_i$ can be written as $e_i x_i - N_i y = z_i - (ap_i^2 + bq_i^2)y$. Hence,

$$\Big|\frac{N_i}{e_i} y - x_i\Big| = \frac{|z_i - y(ap_i^2 + bq_i^2)|}{e_i} \tag{3}$$

Let $N = \max N_i$ and suppose that $y < N^\delta$ and $|z_i| < \frac{|ap_i^2 - bq_i^2|}{3(ap_i^2+bq_i^2)} N^{1/3} y$. Then, $|z_i| < yN^{1/3} < N^{\delta+\frac{1}{3}}$. Also, suppose that $\min e_i = N^\beta$. We set $ap_i^2 + bq_i^2 < N^{\frac{2}{3}+\alpha}$ with $0 < \alpha < 1/3$, then we will get

$$\begin{aligned}
\frac{|z_i - y(ap_i^2 + bq_i^2)|}{e_i} &\leq \frac{|z_i| + y(ap_i^2 + bq_i^2)|}{N^\beta} \\
&< \frac{N^{\delta+1/3} + N^\delta(N^{\frac{2}{3}+\alpha})}{N^\beta} \\
&< \frac{2N^{\delta+\frac{2}{3}+\alpha}}{N^\beta} \\
&= 2N^{\delta+\frac{2}{3}\alpha-\beta}
\end{aligned} \tag{4}$$

Plugging (4) in (3), we obtain

$$\Big|\frac{N_i}{e_i} x_i - y\Big| < 2N^{\delta+\frac{2}{3}\alpha-\beta}.$$

In order to show the existence of integer y and the integers x_i, let $\varepsilon = 2N^{\delta+\frac{2}{3}\alpha-\beta}$, $\delta = \frac{k(3\beta-2-3\alpha)}{3(k+1)}$. Then, we obtain

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

Then, since $2^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k$ for $k \geq 2$, by Theorem 2.2 we get $N^\delta \cdot \varepsilon^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k$. It follows that if $y < N^\delta$, then $y < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \varepsilon^{-k}$. Next, for $i = 1, ..., k$, we get

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

It follows the condition of Theorem 2.2 are fulfilled will find y and x_i for $i = 1, ..., k$. Next, using the equation $e_i x_i - \Big(N_i - (ap_i^2 + bq_i^2)\Big) y = z_i$, we get

$$(ap_i^2 + bq_i^2) - N_i + \frac{e_i x_i}{y} = \frac{z_i}{y}$$

If $|z_i| < \frac{|ap_i^2 - bq_i^2|}{3(ap_i^2 + bq_i^2)} N^{1/3} y$, then $\frac{|z_i|}{y} < \frac{|ap_i^2 - bq_i^2|}{3(ap_i^2 + bq_i^2)} N^{1/3}$ and $S_i = N_i - \frac{e_i x_i}{y}$ is an approximation of $ap_i^2 + bq_i^2$. Hence, by using Lemma 2.1 and Theorem 2.3, this implies that $abq = \left\lceil \frac{S_i^2}{4N} \right\rceil$ for $S_i = N_i - \frac{e_i x_i}{y}$, $i = 1, ..., k$, we compute $q_i = \gcd\Big(\left\lceil \frac{S_i^2}{4N_i} \right\rceil, N_i \Big)$. Therefore, it is possible us to factor k moduli $N_1, ..., N_k$. This terminates the proof. □

Example 4.1. *For illustration of our proposed attack, we consider three moduli and public exponents as follows*

$$\begin{aligned}
N_1 &= 37159722696095612510782748953, \\
N_2 &= 19474173499329799030609546903, \\
N_3 &= 61284862609699996705266409589, \\
e_1 &= 17181377136985024142431807113, \\
e_2 &= 11794217733042502682464813542, \\
e_3 &= 43200804740271910086906145446.
\end{aligned}$$

Then, $N = \max(N_1, N_2, N_3) = 61284862609699996705266409589$. *We obtain* $\min(e_1, e_2, e_3) = N^\beta$ *with* $\beta \approx 0.9751389$. *If* $k = 3$, *then we have* $\delta = \frac{k(3\beta - 2 - 3\alpha)}{3(k+1)} = 0.08135420600$ *and* $2N^{\delta + \frac{2}{3}\alpha - \beta} \approx 0.331415314079361$. *By using (5) in the proof of Theorem 2.2 and consider* $n = k = 3$, *leads to*

$$C = \left\lfloor 3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1} \right\rfloor = 3357.$$

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

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

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

$$K = \begin{bmatrix} -43 & -21 & -41 & -11 \\ -289 & 15 & 349 & -152 \\ -26 & 768 & -259 & -397 \\ 653 & -696 & -80 & -1004 \end{bmatrix}.$$

Now, we obtain

$$K \cdot M^{-1} = \begin{bmatrix} -43 & -93 & -71 & -61 \\ -289 & -625 & -477 & -410 \\ -26 & -56 & -43 & -37 \\ 653 & 1412 & 1078 & 926 \end{bmatrix}.$$

According to the first row of the above matrix, we obtain $y = 43$, $x_1 = 93$, $x_2 = 71$ and $x_3 = 61$. By applying y and x_i for $i = 1, 2, 3$, we look at the relation $S_i = N_i - \frac{e_i x_i}{y}$ is an approximation of $ap_i^2 + bq_i^2$. Hence, by using Lemma 2.1 and Theorem 2.3, this implies that $abq = \left[\frac{S^2}{4N}\right]$ for $S_i = N_i - \frac{e_i x_i}{y}$. Then, we obtain

$$\begin{aligned} \left[\frac{S_1^2}{4N_1}\right] &= 17490871878, \\ \left[\frac{S_2^2}{4N_2}\right] &= 14101767402, \\ \left[\frac{S_3^2}{4N_3}\right] &= 20665143966. \end{aligned}$$

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

$$q_1 = 2915145313, \quad q_2 = 2350294567, \quad q_3 = 3444190661.$$

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

$$p_1 = 3570311659, \quad p_2 = 2878514153, \quad p_3 = 4218256807.$$

5. Conclusion

In conclusion, this paper presents two new attacks on k moduli $N_i = p_i^2 q_i$. We focus on the system of generalized key equations of the form $e_i x - N_i y_i = z_i - (ap_i^2 + bq_i^2)y_i$ for the first attack and the form $e_i x_i - N_i y = z_i - (ap_i^2 + bq_i^2)y$ for the second attack. We show that both of the attacks are successful when the parameters x, x_i, y, y_i and z_i are suitably small. On top of that, we also prove that our attacks enables us to factor k moduli of the form $N_i = p_i^2 q_i$ under our conditions simultaneously based on the LLL algorithm.

Acknowledgement

We would like to acknowledge the Ministry of Education for supported this research under Fundamental Research Grant Scheme (FRGS) with project number FRGS/1/2015/ST06/UPM/02/6.

Appendix

Proof of Theorem 2.2.

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

$$C = \left\lceil 3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1} \right\rceil \tag{5}$$

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

$$b_1 = \pm[q, Cp_1 - q[C\alpha_1], Cp_2 - q[C\alpha_2], ..., Cp_n - q[C\alpha_n]], \tag{6}$$

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

$$q \leq \Big\lfloor 2^{n/4} C^{n/(n+1)} \Big\rfloor \quad \text{and} \quad \max_i |Cp_i - q[C\alpha_i]| \leq 2^{n/4} C^{n/(n+1)}. \tag{7}$$

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 (7), 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 (5) gives

$$3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1} \leq C \leq\leq 3^{n+1} \cdot 2^{\frac{(n+1)(n-3)}{4}} \cdot \varepsilon^{-n-1}, \tag{8}$$

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 (7) and (8), 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 (6)

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

This terminates the proof.

□

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. (2015). *Cryptanalysis on the Modulus $N = p^2q$ and Design of Rabin-like Cryptosystem Without Decryption Failure*. PhD thesis, Universiti Putra Malaysia.

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

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.

Hinek, J. (2007). *On the Security of Some Variants of RSA*. PhD thesis, Waterloo, Ontario, Canada.

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.

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

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

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^kq. *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.