Journal of Mathematical Research with Applications
Jul., 2017, Vol. 37, No. 4, pp. 404–418
DOI:10.3770/j.issn:2095-2651.2017.04.003
Http://jmre.dlut.edu.cn

New Finding on Factoring Prime Power RSA Modulus $N = p^r q$

Sadiq SHEHU[1], **Muhammad Rezal Kamel ARIFFIN**[1,2,*]

1. *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. In the first attack we consider the class of the public exponents satisfying an equation $eX - NY + (ap^r + bq^r)Y = Z$ for suitably small positive integers a, b. Applying continued fractions we show that $\frac{Y}{X}$ can be recovered among the convergents of the continued fraction expansion of $\frac{e}{N}$. Moreover, we show that the number of such exponents is at least $N^{\frac{2}{(r+1)}-\varepsilon}$ where $\varepsilon \geq 0$ is arbitrarily small for large N. The second and third attacks works upon k RSA public keys (N_i, e_i) when there exist k relations of the form $e_i x - N_i y_i + (ap_i^r + bq_i^r)y_i = z_i$ or of the form $e_i x_i - N_i y + (ap_i^r + bq_i^r)y = z_i$ and the parameters x, x_i, y, y_i, z_i are suitably small in terms of the prime factors of the moduli. We apply the LLL algorithm, and show that our strategy enables us to simultaneously factor k prime power RSA moduli.

Keywords RSA prime power; factorization; LLL algorithm; simultaneous diophantine approximations; continued fraction

MR(2010) Subject Classification 11A51; 11A55; 11K60

1. Introduction

The underlying one-way function of RSA is the integer factorization problem: Multiplying two large primes is computationally easy, but factoring the resulting product is very hard. It is also well known that the security of RSA is based on the difficulty of solving the so-called RSA problem: Given an RSA public key (e, N) and a ciphertext $c \equiv m^e \pmod{N}$, compute the plaintext m. The RSA problem is not harder to solve than the integer factorization problem, because factoring the RSA modulus N leads to computing the private exponent d, and to solving the RSA problem. However, it is not clear, if the converse is true. In the RSA cryptosystem, the public modulus $N = pq$ is a product of two primes of the same bit size. The public and private exponent e and d satisfy the congruence

$$ed \equiv 1 \pmod{\phi(N)},$$

where $\phi(N) = (p-1)(q-1)$ is the Euler totient function [1,2].

Received July 18, 2016; Accepted September 7, 2016
* Corresponding author
E-mail address: rezal@upm.edu.my (Muhammad Rezal Kamel ARIFFIN)

In 1990, Wiener showed that RSA is insecure if $d < \frac{1}{3}N^{0.25}$ (see [3]). Later based on the lattice basis reduction, Boneh and Durfee improved the bound to $d < N^{0.292}$ (see [4]). The number of exponents for which their attack applies can be estimated as $N^{0.292-\varepsilon}$. Wiener's attack as well as its generalization by Boneh and Durfee is based on the RSA key equation $ed - k\phi(N) = 1$ where k is a positive integer. In 2004, Blomer and May combined both Wiener method with Boneh and Durfee method to show that RSA is insecure if the public exponent e satisfies an equation $ex - k\phi(N) = y$ (see [5]). Applying the continued fraction algorithm and Coppersmith's method [6], they showed that the RSA modulus can be factored in polynomial time if the parameters x and y satisfy

$$x < \frac{1}{3}N^{\frac{1}{4}} \quad \text{and} \quad |y| \leq N^{-\frac{3}{4}}ex.$$

Additionally, Blomer and May proved that the number of such weak exponents is at least $N^{\frac{3}{4}-\varepsilon}$ (see [7,8,2]).

Many RSA variants have been proposed in order to ensure computational efficiency while maintaining the acceptable levels of security. One such important variant is the prime power RSA. In prime power RSA the modulus N is in the form $N = p^r q$ for $r \geq 2$. In 1998, Takagi showed how to use the prime power RSA to speed up the decryption process when the public and private exponents satisfy an equation $ed \equiv 1 \pmod{(p-1)(q-1)}$ (see [9]). As in the standard RSA cryptosystem, the security of the prime power RSA depends on the difficulty of factoring integers of the form $N = p^r q$ (see [10–12]).

Containing the discussion of variants of RSA moduli by manipulating k instances of RSA moduli and public key pair (N_i, e_i) via their k equations. In 2007, Hinek, showed that it is possible to factor the k modulus N_i using k equations of the form $e_i d - k_i\phi(N_i) = 1$ if $d < N^{\delta}$ with $\delta = \frac{k}{2(k+1)} - \varepsilon$ where ε is a small constant depending on the size of $\max N_i$ (see [13]). Very recently in 2014, with k RSA public keys (N_i, e_i), Nitaj, et al. presented a method that factors the k RSA moduli N_i using k equations of the shape $e_i x - y_i\phi(N_i) = z_i$ or of the shape $e_i x_i - y\phi(N_i) = z_i$ where $N_i = p_i q_i$, $\phi(N_i) = (p_i - 1)(q_i - 1)$ and the parameters x, x_i, y, y_i, z_i are suitably small in terms of the prime factors of the moduli [14].

Our contribution, as motivated from the recent result of [14] and [2]. This paper proposes three new attacks on the Prime Power RSA with a modulus $N = p^r q$. In the first attack, we consider an instance of the prime power RSA with modulus $N = p^r q$ and public of exponent e satisfying the equation $eX - NY + (ap^r + bq^r)Y = Z$ for suitable positive integers a, b. Using continued fraction we show that $\frac{Y}{X}$ can be recovered among the convergents of the continued fraction expansion of $\frac{e}{N}$. We show that the number of such exponents is at least $N^{\frac{2}{(r+1)}-\varepsilon}$ where $\varepsilon \geq 0$ is arbitrarily small for large N. Hence one can factor the modulus $N = p^r q$ in polynomial time.

For $k \geq 2$, $r \geq 2$, let $N_i = p_i^r q_i$, $i = 1, \ldots, k$. The second attack works when k instances (N_i, e_i) are such that there exist an integer x, k integers y_i, and k integers z_i satisfying $e_i x - N_i y_i + (ap_i^r + bq_i^r)y_i = z_i$. We show that the k RSA moduli N_i can be factored in polynomial

time if $N = \min_i N_i$ and

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

In the third attack we show that the k RSA moduli N_i can be factored in polynomial time, when the k instance (N_i, e_i) of RSA are such that there exist an integer y, and k integers x_i and k integers z_i satisfying $e_i x_i - N_i y + (ap_i^r + bq_i^r)y = z_i$ with $\min_i N = \min_i N_i$, $e_i = N^{\beta}$ and

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

For the second and third attack we transform the equations into simultaneous diophantine problem and apply lattice basis reduction techniques to find the parameters (x, y_i) or (y, x_i) which leads to factorization of k RSA moduli N_i.

The rest of the paper is structured as follows. In Section 2, we give a brief review of basic facts about the continued fraction, lattice basis reduction and simultaneous diophantine approximations with some useful results needed for the attack. In Section 3, we propose the first attack with estimation of the number of exponents for which our attack works. In Sections 4 and 5, we give the second and third attack. We conclude this paper in Section 6.

2. Preliminaries

We start with definition and an important result concerning the continued fraction, lattice basis reduction techniques and simultaneous diophantine equations as well as some useful lemmas needed for the attacks.

2.1. Continued fraction

Definition 2.1 (Continued fraction) *The continued fraction of a real number R is an expression of the form*

$$R = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

where $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{N} - 0$ for $i \geq 1$. The numbers $a_0, a_1, a_2, \ldots$ are called the partial quotients. We use the notation $R = [a_0, a_1, a_2, \ldots]$. For $i \geq 1$ the rational $\frac{r_i}{s_i} = [a_0, a_1, a_2, \ldots]$ are called the convergents of the continued fraction expansion of R. If $R = \frac{a}{b}$ is a rational number such that $\gcd(a, b) = 1$, then the continued fraction expansion is finite.

Hardy and Wright (1965) (see [15]). Let $x = [a_0, a_1, a_2, \ldots, a_m]$ be a 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 $Y = p_n$ and $X = q_n$ for some convergent $\frac{p_n}{q_n}$ of x with $n \geq 0$.

2.2. Lattice

A lattice is a discrete (additive) subgroup of $\mathbb{R}^n$. Equivalently, given $m \leq n$ linearly independent vectors $b_1, \ldots, b_m \in \mathbb{R}^n$, the set

$$\mathcal{L} = \mathcal{L}(b_1, \ldots, b_m) = \Big\{ \sum_{i=1}^{m} \alpha_i b_i | \alpha_i \in \mathbb{Z} \Big\}$$

is a lattice. The b_i are called basis vectors of $\mathcal{L}$ and $B = b_1, \ldots, b_m$ is called a lattice basis for $\mathcal{L}$. Thus, the lattice generated by a basis B is the set of all integer linear combinations of the basis vectors in B.

The dimension (or rank) of a lattice, denoted $\dim(\mathcal{L})$, is equal to the number of vectors making up the basis. The dimension of a lattice is equal to the dimension of the vector subspace spanned by B. A lattice is said to be full dimensional (or full rank) when $\dim(\mathcal{L}) = n$ (see [12]).

A lattice $\mathcal{L}$ can be represented by a basis matrix. Given a basis B, a basis matrix M for the lattice generated by B is the $m \times n$ matrix defined by the rows of the set $b_1, \ldots, b_m$

$$M = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}.$$

It is often useful to represent the matrix M by B. A very important notion for the lattice $\mathcal{L}$ is the determinant.

Let $\mathcal{L}$ be a lattice generated by the basis $B = \langle b_1, \ldots, b_m \rangle$. The determinant of $\mathcal{L}$ is defined as

$$\det(\mathcal{L}) = \sqrt{\det(BB^T)}.$$

If $n = m$, we have

$$\det(\mathcal{L}) = \sqrt{\det(BB^T)} = |\det(B)|.$$

Lenstra et al. (1982) (see [16]). 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

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

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

An application of the LLL algorithm is that 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

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

A method to find simultaneous diophantine approximations to rational numbers was described by [16]. In their work, they considered a lattice with real entries. The following is a similar result for a lattice with integer entries.

Theorem 2.2 (Simultaneous diophantine approximations) ([14]) *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

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

Proof See [14] Appendix A. □

Lemma 2.3 *Let $N = p^r q$ be an RSA modulus prime power with $q < p < 2q$. Then*

$$2^{-\frac{r}{r+1}} N^{\frac{1}{r+1}} < q < N^{\frac{1}{r+1}} < p < 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}.$$

Proof Suppose $N = p^r q$. Then multiplying $q < p < 2q$ by p^r, we get $p^r q < p^r p < 2p^r q$ which implies $N < p^{r+1} < 2N$, that is $N^{\frac{1}{r+1}} < p < 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$. Also since $N = p^r q$, $q = \frac{N}{p^r}$ which in turn implies $2^{-\frac{r}{r+1}} N^{\frac{1}{r+1}} < q < N^{\frac{1}{r+1}}$, we have $2^{-\frac{r}{r+1}} N^{\frac{1}{r+1}} < q < N^{\frac{1}{r+1}} < p < 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$. □

Lemma 2.4 *Let $N = p^r q$ be an RSA modulus prime power with $q < p < 2q$. Let a, b be suitably small integers with $gcd(a, b) = 1$. Let $|ap^r - bq^r| < N^{\frac{1}{r}}$. Let S be an approximation of $|ap^r + bq^r|$ such that*

$$|ap^r + bq^r - S| < \frac{|ap^r - bq^r|}{3(ap^r + bq^r)} N^{\frac{1}{r^2}}.$$

Then $abq^{r-1} = [\frac{S^2}{4N}]$.

Proof Set $S = ap^r + bq^r + k$ with $k < \frac{|ap^r - bq^r|}{3(ap^r + bq^r)} N^{\frac{1}{r^2}}$. Observe that

$$\begin{aligned}(ap^r - bq^r)^2 &= (ap^r - bq^r)(ap^r - bq^r) = (ap^r + bq^r)^2 - 4abq^r p^r \\ &= (ap^r + bq^r)^2 - 4abNq^{r-1}.\end{aligned}$$

Therefore, we obtain

$$(ap^r - bq^r)^2 = (ap^r + bq^r)^2 - 4abNq^{r-1}. \tag{1}$$

Now we consider

$$\begin{aligned}S^2 - 4abNq^{r-1} &= (ap^r + bq^r + k)^2 - 4abNq^{r-1} \\ &= a^2p^{2r} + 2abq^r p^r + 2akp^r + b^2q^{2r} + 2bkq^r - 4abNq^{r-1} \\ &= a^2p^{2r} + 2abq^r p^r + b^2q^{2r} + 2k(ap^r + bq^r) + k^2 - 4abNq^{r-1} \\ &= (ap^r + bq^r)^2 - 4abNq^{r-1} + 2k(ap^r + bq^r) + k^2.\end{aligned}$$

Therefore using (1) above, we can rewrite

$$S^2 - 4abNq^{r-1} = (ap^r - bq^r)^2 + 2k(ap^r + bq^r) + k^2. \tag{2}$$

Suppose that $|ap^r - bq^r| < N^{\frac{1}{r}}$ and $k < \frac{|ap^r - bq^r|}{3(ap^r + bq^r)} N^{\frac{1}{r^2}} < N^{\frac{1}{r^2}}$. Then, from (2), we have

$$\begin{aligned}|S^2 - 4abNq^{r-1}| &= |(ap^r - bq^r)^2 + 2k(ap^r + bq^r) + k^2| \\ &< (N^{\frac{1}{r}})^2 + 2(ap^r + bq^r)\frac{|ap^r - bq^r|}{3(ap^r + bq^r)} N^{\frac{1}{r^2}} + (N^{\frac{1}{r^2}})^2 \\ &< N^{\frac{2}{r}} + \frac{2}{3}|ap^r - bq^r| N^{\frac{1}{r^2}} + (N^{\frac{1}{r^2}})^2 \\ &< N^{\frac{2}{r}} + \frac{2}{3} N^{\frac{1}{r}} N^{\frac{1}{r^2}} + N^{\frac{2}{r^2}}\end{aligned}$$

$$< N^{\frac{2}{r}} + \frac{2}{3}N^{\frac{r+1}{r^2}} + N^{\frac{2}{r^2}}$$
$$< 2N.$$

Thus we have $|S^2 - 4abNq^{r-1}| < 2N$. When dividing by $4N$, we obtain

$$\Big|\frac{S^2}{4N} - abq^{r-1}\Big| = \frac{|S^2 - 4abNq^{r-1}|}{4N} < \frac{2N}{4N} = \frac{1}{2}$$

which implies that $abq^{r-1} = [\frac{S^2}{4N}]$. □

3. The first attack on prime power RSA with moduli $N = p^r q$

Let (N, e) be a public key satisfying an equation $eX - NY + (ap^r + bq^r)Y = Z$ with small parameters X, Y and Z where a, b are suitably small positive integers. In this section, we present a result based on continued fractions and show how to factor the Prime Power RSA modulus N.

Lemma 3.1 *Let $N = p^r q$ be an RSA modulus prime power with $q < p < 2q$. Let a, b be suitably small integers with $gcd(a, b) = 1$. Let e be a public key exponent satisfying the equation $eX - NY + (ap^r + bq^r)Y = Z$ with $gcd(X, Y) = 1$, if $1 \le Y \le X < \frac{N^{\frac{1}{2}}}{2(ap^r+bq^r)^{\frac{1}{2}}}$ and $|Z| < \frac{|ap^r-bq^r|}{3(ap^r+bq^r)}N^{\frac{1}{r^2}}$. Then $\frac{Y}{X}$ is among the convergent of the continued fraction expansion of $\frac{e}{N}$.*

Proof Assume that $Z < \frac{|ap^r-bq^r|}{3(ap^r+bq^r)}N^{\frac{1}{r^2}}Y$, thus $Z < |ap^r - bq^r|Y$. Hence from the equation

$$eX - NY + (ap^r + bq^r)Y = Z,$$

we get

$$\begin{aligned}\Big|\frac{e}{N} - \frac{Y}{X}\Big| &= \frac{|eX - NY|}{NX} = \frac{|Z - (ap^r + bq^r)Y|}{NX} \\ &< \frac{|Z + (ap^r + bq^r)Y|}{NX} \le \frac{|Z|}{NX} + \frac{|(ap^r + bq^r)Y|}{NX} \\ &\le \frac{|(ap^r + bq^r)Y|}{NX} + \frac{|(ap^r + bq^r)Y|}{NX} \\ &\le \frac{2(ap^r + bq^r)Y}{NX} \le \frac{2(ap^r + bq^r)X}{NX} \\ &= \frac{2(ap^r + bq^r)}{N}.\end{aligned}$$

Therefore, if the condition $\frac{2(ap^r+bq^r)}{N} < \frac{1}{2X^2}$ holds, then from the theorem of the continued fraction, $\frac{Y}{X}$ is one of the convergents of the continued fraction of $\frac{e}{N}$. This is equivalent to

$$\frac{2(ap^r + bq^r)}{N} < \frac{1}{2X^2}, \quad 4X^2(ap^r + bq^r) < N,$$

$$X^2 < \frac{N}{4(ap^r + bq^r)}, \quad X < \frac{N^{\frac{1}{2}}}{2(ap^r + bq^r)^{\frac{1}{2}}}. \ \square$$

Theorem 3.2 *Let $N = p^r q$ be an RSA modulus prime power with $q < p < 2q$. Let a, b be suitably small integers with $\gcd(a, b) = 1$. Suppose that e is a public key exponent satisfying the*

equation $eX - NY + (ap^r + bq^r)Y = Z$ *with* $\gcd(X, Y) = 1$, *if* $1 \leq Y \leq X < \frac{N^{\frac{1}{2}}}{2(ap^r+bq^r)^{\frac{1}{2}}}$ *and* $|Z| < \frac{|ap^r-bq^r|}{3(ap^r+bq^r)} N^{\frac{1}{r^2}} Y$, *then* N *can be factored in polynomial time.*

Proof Suppose that the public key e satisfies an equation

$$eX - NY + (ap^r + bq^r)Y = Z$$

with $\gcd(X, Y) = 1$. Let $1 \leq Y \leq X < \frac{N^{\frac{1}{2}}}{2(ap^r+bq^r)^{\frac{1}{2}}}$ and $|Z| < \frac{|ap^r-bq^r|}{3(ap^r+bq^r)} N^{\frac{1}{r^2}} Y$ satisfy the condition of Lemma 3.1 above. Then $\frac{Y}{X}$ is one of the convergents of the continued fraction of $\frac{e}{N}$. Let us rewrite equation $eX - NY + (ap^r + bq^r)Y = Z$ as

$$\frac{eX}{Y} - N + (ap^r + bq^r) = \frac{Z}{Y}, \quad (ap^r + bq^r) + \frac{eX}{Y} - N = \frac{Z}{Y}.$$

This implies

$$(ap^r + bq^r) - (N - \frac{eX}{Y}) = \frac{Z}{Y}.$$

We define $S = N - \frac{eX}{Y}$, therefore by Lemma 2.4, S is an approximation of $|ap^r + bq^r|$ satisfying

$$\begin{aligned} |ap^r + bq^r - S| &\leq |(ap^r + bq^r) - (N - \frac{eX}{Y})| = \frac{Z}{Y} \\ &\leq \frac{|ap^r - bq^r|}{3(ap^r + bq^r)Y} N^{\frac{1}{r^2}} Y < \frac{|ap^r - bq^r|}{3(ap^r + bq^r)} N^{\frac{1}{r^2}}, \end{aligned}$$

which, by Lemma 2.4, implies that $abq^{r-1} = [\frac{S^2}{4N}]$, for value of $S = N - \frac{eX}{Y}$. Therefore, it follows that $q = \gcd([\frac{S^2}{4N}], N)$. □

Example 3.3 The following shows an illustration of our attack for $r = 3$, given N and e as

$$N = 35873192098203857081, \quad e = 28134227590946405731.$$

Suppose that the public key (e, N) satisfies $N = p^r q$, $q < p < 2q$ and $eX - NY + (ap^r + bq^r)Y = Z$ for small parameters X, Y, Z as stated in the Theorem 1. Following the above algorithm, we first compute the continued fraction expansion of $\frac{e}{N}$. The list of first convergents of the continued fraction expansion of $\frac{e}{N}$ are

$$\big[0, 1, \frac{3}{4}, \frac{4}{5}, \frac{7}{9}, \frac{11}{14}, \frac{29}{37}, \frac{40}{51}, \frac{309}{394}, \frac{349}{445}, \frac{2054}{2619}, \frac{4457}{5683}, \frac{15425}{19668}, \frac{189557}{241699}, \frac{394539}{503066}, \dots\big].$$

Therefore omitting the first and second entry and starting with the convergent $\frac{3}{4}$, we obtain

$$S = N - \frac{eX}{Y} = \frac{-4917334069174051681}{3}, \quad [\frac{S^2}{4N}] = 18723494352664627.$$

Hence $\gcd([\frac{S^2}{4N}], N) = (18723494352664627, 35873192098203857081) = 1$. Therefore applying the factorization algorithm with the convergent $\frac{40}{51}$, we obtain

$$S = N - \frac{eX}{Y} = \frac{82076789887590959}{40}, \quad [\frac{S^2}{4N}] = 29342068566.$$

We compute $\gcd([\frac{S^2}{4N}], N) = (29342068566, 35873192098203857081) = 69931$. Finally with $q = 69931$, we compute $p = \sqrt[3]{\frac{N}{q}} = 80051$, which leads to the factorization of N.

Algorithm 1

Input: A public key (e, N) satisfying $N = p^r q$, $q < p < 2q$ and $eX - NY + (ap^r + bq^r)Y = Z$ for small parameters X, Y, Z

Output: The prime factors p and q.

1: Compute the continued fraction expansion of $\frac{e}{N}$.
2: For every convergent $\frac{Y}{X}$ of $\frac{e}{N}$, compute $S = N - \frac{eX}{Y}$.
3: Compute $[\frac{S^2}{4N}]$.
4: Compute $q = \gcd([\frac{S^2}{4N}], N)$.
5: If $1 < q < N$, then $p^r = \frac{N}{q}$.
6: End if.
7: End for.

3.1. Estimation of the weak exponent

Lemma 3.4 *Let $N = p^r q$ be an RSA modulus prime power with $q < p < 2q$. Let a, b be suitably small integers with $\gcd(a, b) = 1$ and $|ap^r - bq^r| < N^{\frac{1}{r}}$. Suppose that e is a public key exponent satisfying the two equations*

$$eX' - NY' + (ap^r + bq^r)Y' = Z', \quad eX - NY + (ap^r + bq^r)Y = Z$$

with $\gcd(X, Y) = 1 = \gcd(X', Y')$, $1 \le Y \le X < \frac{N^{\frac{1}{2}}}{2(ap^r+bq^r)^{\frac{1}{2}}}$ and $|Z, Z'| < \frac{|ap^r-bq^r|}{3(ap^r+bq^r)} N^{\frac{1}{r^2}} Y$. Then $X = X'$, $Y = Y'$ and $Z = Z'$.

Proof Suppose that e satisfies the two equations

$$eX' - NY' + (ap^r + bq^r)Y' = Z', \quad eX - NY + (ap^r + bq^r)Y = Z$$

with $1 \le Y \le X < \frac{N^{\frac{1}{2}}}{2(ap^r+bq^r)^{\frac{1}{2}}}$ and $|Z|$, $|Z'| < \frac{|ap^r-bq^r|}{3(ap^r+bq^r)} N^{\frac{1}{r^2}} Y$. Then, from

$$eX - NY + (ap^r + bq^r)Y = Z,$$

we have

$$e = \frac{NY + Z - (ap^r + bq^r)Y}{X}.$$

Also from $eX' - NY' + (ap^r + bq^r)Y' = Z'$, we get

$$e = \frac{NY' + Z' - (ap^r + bq^r)Y'}{X'}.$$

Equating the term e yields

$$\frac{NY + Z - (ap^r + bq^r)Y}{X} = \frac{NY' + Z' - (ap^r + bq^r)Y'}{X'},$$

$$NYX' + ZX' - (ap^r + bq^r)YX' = NY'X + Z'X - (ap^r + bq^r)Y'X,$$

$$(ap^r + bq^r)(Y'X - YX') + ZX' - Z'X = N(Y'X - YX'). \tag{3}$$

Next we assume that $X, X' < \frac{N^{\frac{1}{2}}}{2(ap^r+bq^r)^{\frac{1}{2}}}$ and $|Z, Z'| < \frac{|ap^r-bq^r|}{3(ap^r+bq^r)} N^{\frac{1}{r^2}} Y$. Then the left hand

side of (3) becomes

$$\begin{aligned}
&|(ap^r + bq^r)(Y'X - YX') + ZX' - Z'X| \\
&< (ap^r + bq^r)|(Y'X - YX')| + |ZX' - Z'X| \\
&< (ap^r + bq^r)(|Y'X| + |YX'|) + |ZX'| + |Z'X| \\
&< (ap^r + bq^r)\frac{N^{\frac{2}{r}}}{2(ap^r + bq^r)} + \frac{N^{\frac{1}{r}}}{6(ap^r + bq^r)^2} \times N^{\frac{1+2r}{r^2}} \\
&< \frac{1}{2}N^{\frac{2}{r}} + \frac{N^{\frac{1}{r}+\frac{1+2r}{r^2}}}{6(ap^r + bq^r)^2} < \frac{1}{2}N^{\frac{2}{r}} + \frac{N^{\frac{3r+1}{r^2}}}{6(ap^r + bq^r)^2} \\
&< N.
\end{aligned}$$

Hence from the right hand side of (3) we deduce that $Y'X - YX' = 0$. Since $\gcd(X, Y) = \gcd(X', Y') = 1$, it follows that $X' = X$, $Y' = Y$ and $Z' = Z$. □

Theorem 3.5 *Let $N = p^r q$ be an RSA modulus prime power with $q < p < 2q$. Let a, b be suitably small integers with $\gcd(a, b) = 1$. Suppose that $e < N$ is a public key exponent satisfying the equation*

$$eX - NY + (ap^r + bq^r)Y = Z$$

with $\gcd(X, Y) = 1$, $1 \leq Y \leq X < \frac{N^{\frac{1}{2}}}{2(ap^r+bq^r)^{\frac{1}{2}}}$ and $|Z, Z'| < \frac{|ap^r-bq^r|}{3(ap^r+bq^r)}N^{\frac{1}{r^2}}Y$ is at least $N^{\frac{2}{(r+1)}-\varepsilon}$ where $\varepsilon > 0$ is arbitrarily small for suitably large N.

Proof Suppose that the exponent e satisfies an equation

$$eX - NY + (ap^r + bq^r)Y = Z$$

with $\gcd(X, Y) = 1$ and $1 \leq Y \leq X < \frac{N^{\frac{1}{2}}}{2(ap^r+bq^r)^{\frac{1}{2}}}$, $|Z, Z'| < \frac{|ap^r-bq^r|}{3(ap^r+bq^r)}N^{\frac{1}{r^2}}Y$. Let ξ denote the number of the exponent e satisfying

$$e \equiv \frac{Z - (ap^r + bq^r)Y}{X} \bmod N.$$

With the condition given in the theorem, we have

$$\xi = \sum_{Y=1}^{\omega_1} \sum_{\substack{X=1 \\ \gcd(X,Y)=1}}^{Y-1} \sum_{|Z|=1}^{\omega_2} 1, \tag{4}$$

where $\omega_1 = \lfloor \frac{N^{\frac{1}{2}}}{2(ap^r+bq^r)^{\frac{1}{2}}} \rfloor$ and $\omega_2 = \lfloor \frac{|ap^r-bq^r|}{3(ap^r+bq^r)}N^{\frac{1}{r^2}} \rfloor$. Observe that

$$\sum_{|Z|=1}^{\omega_2} 1 = 2\omega_2 > \frac{ap^r - bq^r}{3(ap^r + bq^r)}N^{\frac{1}{r^2}} > \frac{N^{\frac{r}{r^2}}}{3(ap^r + bq^r)} > N^{\frac{1}{r+1}}. \tag{5}$$

Substituting (5) into (4), we get

$$\xi > N^{\frac{1}{r+1}} \sum_{X=1}^{\omega_1} \sum_{\substack{Y=1 \\ \gcd(X,Y)=1}}^{X-1} 1. \tag{6}$$

Also by considering the following identity for $1 < Y < N$, we have [15, Theorem 328]

$$\sum_{\substack{X=1 \\ \gcd(X,Y)=1}}^{Y-1} 1 = \phi(Y) > \frac{CY}{\log\log Y} > \frac{CY}{\log\log N}, \tag{7}$$

where c is a positive constant. Substituting (7) into (6), we get

$$\xi > N^{\frac{1}{r+1}} \times \frac{C}{\log\log N} \sum_{Y=1}^{\omega_1} Y. \tag{8}$$

Then for $\sum_{Y=1}^{\omega_1} Y$, we have

$$\sum_{Y=1}^{\omega_1} Y = \frac{\omega_1(\omega_1+1)}{2} > \frac{N}{8(ap^r+bq^r)}.$$

Substituting into (8) gives

$$\xi > N^{\frac{1}{r+1}} \times \frac{C}{\log\log N} \times \frac{N}{8(ap^r+bq^r)},$$

$$\xi > \frac{C}{8\log\log N} \times \frac{N^{\frac{1}{r+1}} \times N}{(ap^r+bq^r)}. \tag{9}$$

Next we assume that $ap^r + bq^r < 2ap^r$, then using the result from Lemma 2.3, we have

$$(ap^r+bq^r) < (2ap^r) < (2a(2^{\frac{1}{r+1}} N^{\frac{1}{r+1}})^r) < 2a(2^{\frac{r}{r+1}} N^{\frac{r}{r+1}}).$$

Substituting the above result into (10), we get

$$\begin{aligned}
\xi &> \frac{C}{16\log\log N} \times \frac{N^{\frac{1}{r+1}} \times N}{a2^{\frac{r}{r+1}} N^{\frac{r}{r+1}}} = \frac{C}{16\log\log N} \times \frac{N^{\frac{r+2}{(r+1)}}}{a2^{\frac{r}{r+1}} N^{\frac{r}{r+1}}} \\
&= \frac{C}{16a2^{\frac{r}{r+1}}\log\log N} N^{\frac{r+2-r}{(r+1)}} = \frac{C}{16a2^{\frac{r}{r+1}}\log\log N} N^{\frac{2}{(r+1)}} \\
&= N^{\frac{2}{(r+1)}-\varepsilon},
\end{aligned}$$

where we set $N^{-\varepsilon} = \frac{C}{16a2^{\frac{r}{r+1}}\log\log N}$ and $\varepsilon > 0$ is arbitrarily small for large N. □

4. The second attack on k prime power RSA with moduli $N_i = p_i^r q_i$

Suppose that the prime power RSA moduli $N_i = p_i^r q_i$ with the same size N, satisfies the k equations of the form $e_i x - N_i y_i + (ap_i^r + bq_i^r)y_i = z_i$. In this section for $k \geq 2$, $r \geq 2$ we show that it is possible to factor the RSA moduli N_i if the unknown parameters x, y_i, and z_i are suitably small.

Theorem 4.1 *For $k \geq 2$, $r \geq 2$, let $N_i = p_i^r q_i$, $1 \leq i \leq k$ be k RSA moduli. Let $N = \min_i N_i$. Let e_i, $i = 1, \ldots, k$, be k public exponents. Define $\delta = \frac{k - kr^2 - \alpha k r^2}{r^2(1+k)}$. Let a, b be suitably small integers with $\gcd(a,b) = 1$ such that $ap_i^r + bq_i^r < N^{\frac{r}{r+1}+\alpha}$. If there exist an integer $x < N^{\delta}$ and k integers $y_i < N^{\delta}$ and $|z_i| < \frac{ap_i^r - bq_i^r}{3(ap_i^r+bq_i^r)} N^{\frac{1}{r^2}} y_i$ such that $e_i x - N_i y_i + (ap_i^r + bq_i^r)y_i = z_i$ 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 $r \geq 2$, let $N_i = p_i^r q_i$, $1 \leq i \leq k$ be k RSA moduli. Let $N = \min_i N_i$ and

suppose that $y_i < N^{\delta}$ and $|ap_i^r + bq_i^r| < N^{\frac{r}{r+1}+\alpha}$. Then the equation $e_i x - N_i y_i + (ap_i^r + bq_i^r)y_i = z_i$ can be rewritten as

$$\left|\frac{e_i}{N_i}x - y_i\right| = \frac{|z_i - (ap_i^r + bq_i^r)y_i|}{N_i}. \tag{10}$$

Let $N = \min_i N_i$, and suppose that $y_i < N^{\delta}$, $|z_i| < N^{\frac{1}{r^2}} y_i$ and $|ap_i^r + bq_i^r| < N^{\frac{r}{r+1}+\alpha}$. Then

$$\begin{aligned}\frac{|z_i - (ap_i^r + bq_i^r)y_i|}{N_i} &\leq \frac{|z_i + (ap_i^r + bq_i^r)y_i|}{N} < \frac{N^{\frac{1}{r^2}} \cdot N^{\delta} + N^{\frac{r}{r+1}+\alpha} \cdot N^{\delta}}{N} \\ &< \frac{N^{\frac{1}{r^2}+\delta} + N^{\delta+\frac{r}{r+1}+\alpha}}{N} < \frac{2N^{\frac{1}{r^2}+\delta+\alpha}}{N} \\ &< 2N^{\frac{1}{r^2}+\delta+\alpha-1} < 2N^{\delta+\alpha-\frac{1-r^2}{r^2}}.\end{aligned}$$

Substituting into (11) gives

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

Hence to show the existence of the integer x, we let $\varepsilon = 2N^{\delta+\alpha-\frac{1-r^2}{r^2}}$ with $\delta = \frac{k-kr^2-\alpha kr^2}{r^2(1+k)}$. Then we have $N^{\delta}\varepsilon^k = 2^k N^{\delta+\delta k+\alpha k-\frac{k-kr^2}{r^2}} = 2^k$. Therefore since $2^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k$ for $k \geq 2$, we get $N^{\delta}\varepsilon^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k$. 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

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

Hence it satisfies the conditions of [9], and we can obtain x and y_i for $i = 1, \ldots, k$. Next from the equation $e_i x - N_i y_i = z_i - (ap_i^r + bq_i^r)y_i$, we get $(ap_i^r + bq_i^r) - (N_i - \frac{e_i x}{y_i}) = \frac{z_i}{y_i}$. Since $|z_i| < N^{\frac{1}{r^2}} y_i$ and $S_i = N_i - \frac{e_i x}{y_i}$ is an approximation of $ap_i^r + bq_i^r$ with an error term of at most $N^{\frac{1}{r^2}}$, using Lemma 2.4 implies that $abq_i^{r-1} = [\frac{S_i^2}{4N_i}]$ with $S_i = N_i - \frac{e_i x}{y_i}$. For $i = 1, \ldots, k$, we compute $q_i = \gcd(N_i, [\frac{S_i^2}{4N_i}])$, which leads to factorization of k RSA moduli $N_i, \ldots, N_k$. □

Example 4.2 As an illustration to our second attack on k prime power RSA, we consider the following three RSA prime power and three public exponents

$$\begin{aligned}N_1 &= 19591352994040260303167470156568646095770569250721626 1,\\ N_2 &= 16997922295000448137122376596209111277641348240692628 41,\\ N_3 &= 32937970222047577181060217629570052947019437843961947 9,\\ e_1 &= 12996240341579036835209361475676488425396893023 03,\\ e_2 &= 24975977316909591477014987638482535355381489609233,\\ e_3 &= 32771125955079641000884923182329513369784895666742.\end{aligned}$$

Then $N = \max(N_1, N_2, N_3) = 16997922295000448137122376596209111277641348240692628 41$. Since $k = 3$ and $r = 3$ with $\alpha < \frac{1}{3}$, we get $\delta = \frac{k-kr^2-\alpha kr^2}{r^2(1+k)} = 0.29166666$ and $\varepsilon = 2N^{\delta+\alpha-\frac{1-r^2}{r^2}} = 0.00001068145463$. Using [14, Eq. (11)], with $n = k = 3$, we obtain

$$C = [3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1}] = 3111239348000000000000.$$

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

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

Therefore applying the LLL algorithm to $\mathcal{L}$, we obtain the reduced basis with following matrix

$$K = \begin{bmatrix} 213211211837 & 632821697847507 & 1241289918735056 & 13478586491738418 \\ 5446677911782793 & -8118714952379577 & -4474991019541616 & 5620827954759402 \\ 5441774053910541 & 2034705429745149 & -12690482991353808 & -5161303690478674 \\ 13755566028807787 & 5229506896157957 & -5232739515531344 & -4243530005173282 \end{bmatrix}.$$

Next we compute

$$K \cdot M^{-1} = \begin{bmatrix} 213211211837 & 1414371 & 3132829 & 21213121 \\ 5446677911782793 & 36131417379 & 80031018860 & 541908826441 \\ -5441774053910541 & -36098886846 & -79958963793 & -541420924658 \\ 13755566028807787 & 91249768303 & 202118058404 & 1368588847080 \end{bmatrix}.$$

Then from the first row we obtain $x = 213211211837$, $y_1 = 1414371$, $y_2 = 3132829$, $y_3 = 21213121$. Hence, using x and y_i for $i = 1, 2, 3$, and defining $S_i = N_i - \frac{e_i x}{y_i}$, we get

$$S_1 = 2817073984679857305109891001272304341 3860,$$

$$S_2 = 216450726906431579918076792924822175513927,$$

$$S_3 = 67266921312851019748440655807702140329434$$

and Lemma 2.4 implies that $abq_i^{r-1} = [\frac{S_i^2}{4N_i}]$ for $i = 1, 2, 3$, which gives

$$[\frac{S_1^2}{4N_1}] = 10126796548423903859820960 06,$$

$$[\frac{S_2^2}{4N_2}] = 68906829265984400004695573 34,$$

$$[\frac{S_3^2}{4N_3}] = 34343636480979289779373613 34.$$

Therefore for $i = 1, 2, 3$, we compute $q_i = \gcd([\frac{S_i^2}{4N_i}], N_i)$, that is

$$q_1 = 12991533491999,\ q_2 = 33888746722667,\ q_3 = 23924755826333.$$

Finally for $i = 1, 2, 3$, we find $p_i = \sqrt[3]{\frac{N_i}{q_i}}$, hence

$$p_1 = 24705937446979,\ p_2 = 36879082724147,\ p_3 = 23967152513467$$

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

5. The third attack on k prime power RSA with moduli $N_i = p_i^r q_i$

In this section, we consider the scenario when the k RSA moduli $N_i = p_i^r q$ for $k \geq 2$, and $r \geq 2$ satisfy k equations $e_i x_i - N_i y + (ap_i^r + bq_i^r)y = z_i$ for $i = 1, \ldots, k$, with suitably small unknown parameters x_i, y and z_i.

Theorem 5.1 *For $k \geq 2$, and $r \geq 2$ let $N_i = p_i^r q_i$, $1 \leq i \leq k$ be k RSA moduli with the same size N. Let e_i, $i = 1, \ldots, k$, be k public exponents with $\min_i$, $e_i = N^\beta$. Let $\delta = \frac{\beta k r^2 - \alpha k r^2 - k}{r^2(1+k)}$. Let a, b be suitably small integers with $\gcd(a, b) = 1$ such that $ap_i^r + bq_i^r < N^{\frac{r}{r+1}+\alpha}$. If there exist an integer $y < N^\delta$ and k integers $x_i < N^\delta$ such that $e_i x_i - N_i y + (ap_i^r + bq_i^r)y = z_i$ 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 $r \geq 2$, let $N_i = p_i^r q_i$, $1 \leq i \leq k$ be k RSA moduli. Then the equation $e_i x_i - N_i y + (ap_i^r + bq_i^r)y = z_i$ can be rewritten as

$$\left|\frac{N_i}{e_i} y - x_i\right| = \frac{|z_i - (ap_i^r + bq_i^r)y|}{e_i}. \tag{11}$$

Let $N = \max_i N_i$, $|z_i| < N^{\frac{1}{r^2}} y_i$ and suppose that $y < N^\delta$, $\min_i$, $e_i = N^\beta$ and $|ap_i^r + bq_i^r| < N^{\frac{r}{r+1}+\alpha}$. Then

$$\begin{aligned}
\frac{|z_i - (ap_i^r + bq_i^r)y|}{e_i} &\leq \frac{|z_i + (ap_i^r + bq_i^r)y|}{N^\beta} < \frac{N^{\frac{1}{r^2}} \cdot N^\delta + N^{\frac{r}{r+1}+\alpha} \cdot N^\delta}{N^\beta} \\
&= \frac{N^{\frac{1}{r^2}+\delta} + N^{\delta+\frac{r}{r+1}+\alpha}}{N^\beta} < \frac{2N^{\frac{1}{r^2}+\delta+\alpha}}{N^\beta} \\
&< 2N^{\frac{1}{r^2}+\delta+\alpha-\beta}.
\end{aligned} \tag{12}$$

Substituting into (12) yields $|\frac{N_i}{e_i} y - x_i| < 2N^{\frac{1}{r^2}+\delta+\alpha-\beta}$. Hence to show the existence of the integer y and integers x_i, we let $\varepsilon = 2N^{\frac{1}{r^2}+\delta+\alpha-\beta}$, with $\delta = \frac{\beta k r^2 - \alpha k r^2 - k}{r^2(1+k)}$. Then we have

$$N^\delta \varepsilon^k = 2^k N^{\delta+\delta k+\frac{k}{r^2}+\alpha k-\beta k} = 2^k.$$

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

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

Hence it satisfies the conditions of [14], and we can obtain y and x_i for $i = 1, \ldots, k$. Next from the equation $e_i x_i - N_i y = z_i - (ap_i^r + bq_i^r)y$, we get

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

Since $S_i = N_i - \frac{e_i x_i}{y}$ is an approximation of $ap_i^r + bq_i^r$ with an error term of at most $N^{\frac{1}{r^2}}$, using Lemma 2.4 implies that $abq_i^{r-1} = [\frac{S_i^2}{4N_i}]$ with $S_i = N_i - \frac{e_i x_i}{y}$. For $i = 1, \ldots, k$, we compute $q_i = \gcd(N_i, [\frac{S_i^2}{4N_i}])$, which leads to factorization of k RSA moduli $N_i, \ldots, N_k$. □

Example 5.2 As an illustration to our third attack on k prime power RSA, we consider the following three RSA prime power and three public exponents

$$\begin{aligned}
N_1 &= 29478007378617097023406572417037943925952729414310412 37, \\
N_2 &= 36973929473317994523347604230786274707808979855050683 41, \\
N_3 &= 14012288952291923813798515482903600779563305771278258 33, \\
e_1 &= 31903636395113698903813783442029745231839939984541508 51841,
\end{aligned}$$

$$e_2 = 341626248149130063399185868689644809069995027400936261283 0,$$

$$e_3 = 126583325939372177796238521956982355885583276234437084100 1.$$

Then $N = \max(N_1, N_2, N_3) = 369739294733179945233476042307862747078089798550506834 1$. Also $\min(e_1, e_2, e_3) = N^\beta$ with $\beta = 0.994871$. Since $k = 3$ and $r = 3$ with $\alpha < \frac{1}{3}$, we get $\delta = \frac{\beta k r^2 - \alpha k r^2 - k}{r^2(1+k)} = 0.2878199168$ and $\varepsilon = 2N^{\frac{1}{r^2}+\delta+\alpha-\beta} = 0.00001163556867$. Using [14, Eq. (11)], with $n = k = 3$, we obtain

$$C = [3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1}] = 2209553741000000000000.$$

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

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

Therefore applying the LLL algorithm to $\mathcal{L}$, we obtain the reduced basis with following matrix

$$M = \begin{bmatrix} 12142354517 & -2333587136850290 & -2655014285575194 & -2972297581182437 \\ -1016896438021615 & 3395215855002550 & 8132820287728430 & -8244621735525985 \\ 1883362666735622 & 11499575960505860 & -7006895107637804 & -854668408378342 \\ 13230083976811097 & -7127477806244890 & 4998010273833246 & -132246744939817 \end{bmatrix}.$$

Next we compute

$$K \cdot M^{-1} = \begin{bmatrix} 12142354517 & 11219173 & 13141571 & 13441121 \\ -1016896438021615 & -939581943953 & -1100578699230 & -1125665376413 \\ 1883362666735622 & 1740170866389 & 2038348013065 & 2084810277532 \\ 13230083976811097 & 12224202540996 & 14318811699479 & 14645195816308 \end{bmatrix}.$$

Then from the first row we obtain $y = 12142354517$, $x_1 = 11219173$, $x_2 = 13141571$, $x_3 = 13441121$. Hence, by using x and y_i for $i = 1, 2, 3$, and defining $S_i = N_i - \frac{e_i x_i}{y}$, we get

$$S_1 = 2774962940151247013792266443297632811348 95,$$

$$S_2 = 3380739575946992970804135391137624161145 76,$$

$$S_3 = 1402367538923303966427022168334040825585 25$$

and Lemma 2.4 implies that $abq_i^{r-1} = [\frac{S_i^2}{4N_i}]$ for $i = 1, 2, 3$, which gives

$$[\frac{S_1^2}{4N_1}] = 6530647764202866046495021254,$$

$$[\frac{S_2^2}{4N_2}] = 7728012847959674598896447094,$$

$$[\frac{S_3^2}{4N_3}] = 3508767769708551665573768166.$$

Therefore for $i = 1, 2, 3$ we compute $q_i = \gcd([\frac{S_i^2}{4N_i}], N_i)$, that is

$$q_1 = 32991533672047,\ q_2 = 35888746722707,\ q_3 = 24182527334519$$

and finally for $i = 1, 2, 3$, we find $p_i = \sqrt[3]{\frac{N_i}{q_i}}$, hence

$$p_1 = 44705937443491,\ p_2 = 46879082724167,\ p_3 = 38696272470943$$

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

6. Conclusion

This paper shows three new attacks on RSA-type modulus of $N = p^r q$ for $r \geq 2$ and $q < p < 2q$. For the first attack, using continued fraction we show that $\frac{Y}{X}$ can be recovered among the convergents of the continued fraction expansion of $\frac{e}{N}$. Furthermore we show that the set of such weak exponents is relatively large, namely that their number is at least $N^{\frac{2}{(r+1)}-\varepsilon}$ where $\varepsilon \geq 0$ is arbitrarily small for suitably large N. Hence one can factor the prime power RSA modulus $N = p^r q$ in polynomial time. For $k \geq 2$, $r \geq 2$, we present second and third attacks on the prime power RSA with moduli $N_i = p_i^r q_i$ for $i = 1, \ldots, k$. The attacks work when k RSA public keys (N_i, e_i) are such that there exist k relations of the shape $e_i x - N_i y_i + (ap_i^r + bq_i^r)y_i = z_i$ or of the shape $e_i x_i - N_i y + (ap_i^r + bq_i^r)y = z_i$ where the parameters x, x_i, y, y_i, z_i are suitably small in terms of the prime factors of the moduli. Applying LLL algorithm, we show that our approach enables us to simultaneously factor the k prime power RSA moduli N_i.

References

[1] A. NITAJ. *Diophantine and Lattice Cryptanalysis of the RSA Cryptosystem. Artificial Intelligence, Evolutionary Computing and Metaheuristics*. Springer Berlin Heidelberg, 2013.

[2] A. NITAJ. *A new vulnerable class of exponents in RSA*. JP J. Algebra Number Theory Appl., 2011, **21**(2): 203–220.

[3] M. WIENER. *Cryptanalysis of short RSA secret exponents*. IEEE Trans. Inform. Theory, 1990, **36**(3): 553–558.

[4] D. BONEH, G. DURFEE. *Cryptanalysis of RSA with Private Key d Less than $N^{0.292}$*. Springer, Berlin, 1999.

[5] J. BLOMER, A. MAY. *A generalized Wiener Attack on RSA*. Springer, Berlin, 2004.

[6] R. RIVEST, A. SHAMIR, L. ADLEMAN. *A method for obtaining digital signatures and public-key cryptosystems*. Comm. ACM, 1978, **21**(2): 120–126.

[7] N. HOWGRAVE-GRAHAM, J. P. SEIFERT. *Extending Wieners Attack in the Presence of Many Decrypting Exponents*. Springer-Verlag, 1999.

[8] A. NITAJ. *Cryptanalysis of RSA Using the Ratio of the Primes*. Springer, Berlin, 2009.

[9] T. TAKAGI. *Fast RSA-Type Cryptosystem Modulo $p^k q$*. Springer, Berlin, 1998.

[10] S. SARKAR. *Small secret exponent attack on RSA variant with modulus $N = p^r q$*. Des. Codes Cryptogr., 2014, **73**(2): 383–392.

[11] A. MAY. *New RSA Vulnerabilities Using Lattice Reduction Methods*. Ph.D. Thesis, University of Paderborn, 2003.

[12] M. J. HINEK. *Lattice attacks in cryptography: A partial overview*. School of Computer Science, University of Waterloo, Canada, 2004.

[13] J. HINEK. *On the Security of Some Variants of RSA*. Ph.D. Thesis, Waterloo, Ontario, Canada, 2007.

[14] A. NITAJ, M. R. K. ARIFFIN, D. I. NASSR, et al. *New Attacks on the RSA Cryptosystem*. Springer, Cham, 2014.

[15] G. H. HARDY, E. M. WRIGHT. *An Introduction to the Theory of Numbers*. Oxford University Press, London, 1965.

[16] A. K. LENSTRA, H. W. LENSTRA, L. LOVASZ. *Factoring polynomials with rational coefficients*. Math. Ann., 1982, **261**(4): 515–534.