Journal of Algebra, Number Theory: Advances and Applications
Volume 18, Number 1-2, 2017, Pages 35-59
Available at http://scientificadvances.co.in
DOI: http://dx.doi.org/10.18642/jantaa_7100121854

NEW ATTACKS ON TAKAGI CRYPTOSYSTEM

MUHAMMAD REZAL KAMEL ARIFFIN[1], **SADIQ SHEHU**[2] **and M. A. ASBULLAH**[3]

[1,2,3]Al-Kindi Cryptography Research Laboratory
Institute for Mathematical Research
Universiti Putra Malaysia (UPM)
Selangor
Malaysia

[1,2]Department of Mathematics
Faculty of Science
Universiti Putra Malaysia (UPM)
Selangor
Malaysia
e-mail: rezal@upm.edu.my
sadiqshehuzezi@gmail.com
ma_asyraf@upm.edu.my

Abstract

This paper proposes three new attacks on RSA-Takagi cryptosystem. The first attack is based on the equation $eX - NY = (ap^r + bq^r)Z$ for suitable positive integers a, b. We show that $\frac{Y}{X}$ can be recovered among the convergents of the continued fractions expansion of $\frac{e}{N}$ and leads to successful factorization of the

---

2010 Mathematics Subject Classification: 11Y05.
Keywords and phrases: prime power modulo, factorization, LLL algorithm, simultaneous Diophantine approximations, continued fractions.
Received June 30, 2017

prime power modulus $N = p^r q$ in polynomial time. The second and third attack works upon j public keys (N_i, e_i) when there exist j relations of the shape $e_i x - N_i y_i = (ap_i^r + bq_i^r)z_i$ or of the shape $e_i x_i - N_i y = (ap_i^r + bq_i^r)z_i$, where the parameters x, x_i, y, y_i, z_i are suitably small in terms of the prime factors of the moduli. Applying the LLL algorithm, we show that our strategy enable us to simultaneously factor the j public key N_i in polynomial time.

1. Introduction

In recent years, modulus of the form $N = p^r q$ have found many applications in cryptography. In [3], Boneh et al. proposed an efficient algorithm for factoring modulus of the form $N = p^r q$ and showed that the algorithm runs in polynomial time when r is large $(r \approx \sqrt{\log p})$. Hence it is expected that the factoring of the modulus $N = p^r q$ will be intractable when the bound for r is small. Fujioka et al. [5], used the modulus $N = p^r q$ for $r = 2$ in an electronic cash scheme. Okamoto and Uchiyama [15], used $N = p^r q$ with $r = 2$ in designing an elegant public key system.

The cryptosystem developed by Takagi ushered in research in determining the security of the modulus $N = p^r q$. In [18], Takagi proposed a cryptosystem using modulus $N = p^r q$ based on the RSA cryptosystem. He chooses an appropriate modulus $N = p^r q$ which resists two of the fastest factoring algorithms, namely, the number field sieve and the elliptic curve method. Applying the fast decryption algorithm modulo p^r, he showed that the decryption process of the proposed cryptosystems is faster than the RSA cryptosystem using Chinese remainder theorem, known as the Quisquater-Couvreur method.

In [17], Sarkar proved that using the lattice reduction techniques, if the decryption exponent $d \leq N^{0.395}$, then one can factor the prime power modulus $N = p^r q$ in polynomial time. Asbullah and Ariffin [2] proved that by taking the term $N - (2N^{2/3} - N^{1/3})$ as a good approximation of $\phi(N)$ satisfying the RSA key equation $ed - k\phi(N) = 1$, one can yield the factorization of the prime power modulus $N = p^2 q$ in polynomial time (for more information, see [1], [16], [17]).

Our first proposed attack uses the Legendre theorem, which enables us to find the convergent of the continued fractions that leads to the factorization of the modulus $N = p^r q$ in polynomial time. The second and third attacks uses lattice bases reduction. We are interested in the so called reduced bases of a lattice so as to yield factorization of the j moduli $N_1, \ldots, N_j$ in polynomial time.

The remainder of this paper is organized as follows. In Section 2, we give introduction to continued fractions, lattice basis reduction with some previous results. In Section 3, we present the first attack and estimation of the size of the class of the exponents for which our attack applies. In Sections 4 and 5, we give the second and third attacks. We also provide numerical example for all our attacks. We conclude this paper in Section 6.

2. Preliminaries

We start with definitions and important theorems concerning the continued fractions, lattice basis reduction techniques and some theorem from the previous attacks as well as some useful lemmas.

2.1. Continued fractions

Definition 1 (Continued fractions)**.** A continued fraction is an expression of the form

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

where a_0 is an integer and a_n are positive integers for $n \geq 1$. The a_n are called the partial quotients of the continued fraction [12].

Definition 2 (Convergents)**.** Let $x \in \mathbb{R}$ with $x = [a_0, a_1, \ldots, a_m]$. For $0 \leq n \leq m$, the n-th convergent of the continued fraction expansion of x is $[a_0, a_1, \ldots, a_n]$.

Theorem 1 (Legendre)**.** *Let x be a real positive number. If X and Y are positive integers such that* $\gcd(X, Y) = 1$ *and*

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

then $\frac{Y}{X}$ is a convergent of the continued fraction expansion of x.

Definition 3 (Lattice basis reductions)**.** Let $m \leq n$ be two positive integers and $b_1, \cdots, b_m \in \mathbb{R}^n$ be n linearly independent vectors. A lattice $\mathcal{L}$ spanned by $\{b_1, \cdots, b_m\}$ is the set of all integer linear combinations of $b_1, \cdots, b_m$, that is,

$$\mathcal{L} = \mathcal{L}(b_1, \cdots, b_m) = \left\{ \sum_{i=1}^{m} \alpha_i b_i \middle| \alpha_i \in \mathbb{Z} \right\}.$$

The b_i are called basis vectors of $\mathcal{L}$ and $B = b_1, \cdots, b_m$ 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 the 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 $\dim(\mathcal{L}) = n$.

Theorem 2. *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*

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

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

As 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 be 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 [10]. In their work, they considered a lattice with real entries. Below a similar result for a lattice with integer entries.

Theorem 3 (Simultaneous Diophantine approximations, [8])**.** *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*

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

Lemma 1. *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 $N = p^r q$, then $q = \frac{N}{p^r}$ which in turn implies $2^{-\frac{r}{r+1}} N^{\frac{1}{r+1}} < q < N^{\frac{1}{r+1}}$. Hence $2^{-\frac{r}{r+1}} N^{\frac{1}{r+1}} < q < N^{\frac{1}{r+1}} < p < 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$ [14]. □

Lemma 2. *Let* $N = p^r q$ *be a prime power modulus with* $q < p < 2q$ *and* a, b *be suitably small integers such that* $\gcd(a, b) = 1$. *Also let* $S = (ap^r + bq^r)Z$, *where* $1 \leq Z < \frac{\frac{1}{2} N^{\frac{1}{2}}}{|ap^r - bq^r|}$, *then* $q^{r-1} abZ^2 = \left\lfloor \frac{S^2}{4N} \right\rfloor$.

Proof. Set $S = (ap^r + bq^r)Z$. Then observe that

$$\begin{aligned}
S^2 &= ((ap^r + bq^r)Z)^2 = (ap^r Z + bq^r Z)(ap^r Z + bq^r Z) \\
&= a^2 p^{2r} Z^2 + ap^r bq^r z^2 + abp^r q^r Z^2 + b^2 q^{2r} Z^2 \\
&= a^2 p^{2r} Z^2 + 2abp^r q^r Z^2 + b^2 q^{2r} Z^2 \\
&= a^2 p^{2r} Z^2 + 2abp^r q^r Z^2 - 2abp^r q^r Z^2 + 2abp^r q^r Z^2 + b^2 q^{2r} Z^2 \\
&= a^2 p^{2r} Z^2 - 2abp^r q^r Z^2 + b^2 q^{2r} Z^2 + 4abp^r q^r Z^2 \\
&= a^2 p^{2r} Z^2 - 2abp^r q^r Z^2 + b^2 q^{2r} \; Z^2 + 4abp^r q^{r-1} q Z^2 \\
&= a^2 p^{2r} Z^2 - 2abp^r q^r Z^2 + b^2 q^{2r} Z^2 - 4abNq^{r-1} Z^2 \\
&= (ap^r Z - bq^r Z)^2 + 4abNq^{r-1} Z^2.
\end{aligned}$$

Hence we obtain

$$S^2 - 4abNq^{r-1} Z^2 = (ap^r Z - bq^r Z)^2 > 0. \tag{1}$$

Then we divide (1) by $4N$, we get

$$\left|\frac{S^2}{4N} - q^{r-1}abZ^2\right| = \frac{|S^2 - 4abNq^{r-1}Z^2|}{4N}$$

$$= \frac{\left|(ap^rZ - bq^rZ)^2\right|}{4N}$$

$$= \frac{\left|(ap^r - bq^r)^2 Z^2\right|}{4N}$$

$$= \frac{(ap^r - bq^r)^2\left(\dfrac{\frac{1}{2}N^{\frac{1}{2}}}{|ap^r - bq^r|}\right)^2}{4N}$$

$$< \frac{\frac{1}{4}N}{4N} < \frac{N}{16N} = \frac{1}{16} < 1,$$

implies that

$$q^{r-1}Z^2ab = \left\lfloor \frac{S^2}{4N} \right\rfloor.$$

□

3. The First Attack on Prime Power Moduli $N = p^r q$

In this section, we present a result based on continued fractions and show how to factor the prime power modulus $N = p^r q$, if (N, e) is a public key satisfying an equation $eX - NY = (ap^r + bq^r)Z$ with small parameters X, Y, and Z, where a, b be a suitably small positive integer.

Lemma 3. *Let* $N = p^r q$ *be a prime power modulus with* $q < p < 2q$ *and* a, b *be integers such that* $\gcd(a, b) = 1$. *Let* e *be a public key satisfying the equation* $eX - NY = (ap^r + bq^r)Z$ *with* $\gcd(X, Y) = 1$, *if* $X < \frac{N}{2(ap^r + bq^r)Z}$, *then* $\frac{Y}{X}$ *is among the convergents of the continued fraction expansion of* $\frac{e}{N}$.

Proof. Suppose that e satisfies the equation $eX - NY = (ap^r + bq^r)Z$ with $X < \frac{N}{2(ap^r + bq^r)Z}$ and $\gcd(X, Y) = 1$.

Then from the equation $eX - NY = (ap^r + bq^r)Z$ when dividing by NX, we get

$$\left|\frac{e}{N} - \frac{Y}{X}\right| = \frac{|eX - NY|}{NX}$$

$$\leq \frac{|ap^r + bq^r|Z}{NX}.$$

Assume that if $X < \frac{N}{2(ap^r + bq^r)Z}$, then $\frac{|ap^r + bq^r|Z}{NX} < \frac{1}{2X^2}$ hold, that is,

$$\frac{2X^2(ap^r + bq^r)Z}{2XZ(ap^r + bq^r)} < \frac{NX}{2XZ(ap^r + bq^r)},$$

which implies

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

and by Theorem 1, we conclude that $\frac{Y}{X}$ is among the convergent of the continued fraction expansion of $\frac{e}{N}$. □

Theorem 4. *Let* $N = p^r q$ *be a prime power modulus with* $q < p < 2q$. *Let* a, b *be integers such that* $\gcd(a, b) = 1$ *and let e be a public key satisfying the equation* $eX - NY = (ap^r + bq^r)Z$ *with* $\gcd(X, Y) = 1$, *if* $1 \le Y < X < \dfrac{N}{2(ap^r + bq^r)Z}$ *and* $1 \le Z < \dfrac{\frac{1}{2}N^{\frac{1}{2}}}{|ap^r - bq^r|}$, *then* $N = p^r q$ *for* $r \ge 2$ *can be factored in polynomial time.*

Proof. Suppose that e satisfies an equation $eX - NY = (ap^r + bq^r)Z$ with $\gcd(X, Y) = 1$, let X and Z satisfy the condition in Lemma 3, then $\dfrac{Y}{X}$ is among the convergent of the continued fraction expansion of $\dfrac{e}{N}$.

Hence using X and Y, we define $S = eX - NY$ and Lemma 2 shows that $q^{r-1}Z^2ab = \left\lfloor \dfrac{S^2}{4N} \right\rfloor$. It follows that $q = \gcd\left(\left\lfloor \dfrac{S^2}{4N} \right\rfloor, N\right)$. □

The following algorithm is designed to recover the prime factors for prime power modulus $N = p^r q$ in polynomial time.

Algorithm 1

Input: The public key pair (e, N) satisfying $N = p^r q$, $q < p < 2q$ and Theorem 4.

Output: The two prime factors p and q.

(1) Compute the continued fraction expansion of $\dfrac{e}{N}$.

(2) For each convergent $\dfrac{Y}{X}$ of $\dfrac{e}{N}$, compute $S = eX - NY$.

(3) Compute $\left\lfloor \dfrac{S^2}{4N} \right\rfloor$.

(4) $q = \gcd\left(\left\lfloor \dfrac{S^2}{4N} \right\rfloor, N\right)$.

(5) If $1 < q < N$, then $p^r = \dfrac{N}{q}$.

Example 1. The following shows an illustration of our attack for $r = 3$, $X = 49$, $Y = 38$, $Z = 3$, $a = 2$, $b = 3$, given N and e as

$$N = 36788825128956632489,$$

$$e = 28530237308691190057.$$

Suppose that the public key (e, N) satisfy all the condition as stated in the Theorem 4, from 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

$$\left[0, 1, \frac{3}{4}, \frac{7}{9}, \frac{38}{49}, \frac{4529}{5840}, \frac{9096}{11729}, \frac{1378025}{1776919}, \frac{2765146}{3565567}, \frac{4143171}{5342486}, \frac{6908317}{8908053}, \frac{149217828}{192411599}, \ldots\right].$$

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

$$S = eX - NY = 37544738478948 62761,$$

and

$$\left\lfloor \frac{S^2}{4N} \right\rfloor = 95790459637642658.$$

Hence

$$\gcd\left(\left\lfloor \frac{S^2}{4N} \right\rfloor, N\right) = (95790459637642658, 36788825128956632489).$$

$$= 1$$

Also the convergent $\frac{7}{9}$, gives S and $\left\lfloor \frac{S^2}{4N} \right\rfloor$ with $\gcd\left(\left\lfloor \frac{S^2}{4N} \right\rfloor, N\right) = 1.$

Therefore, we need to try for the next convergent $\frac{38}{49}$, we obtain

$$S = eX - NY = 6273225516278211,$$

and

$$\left\lfloor \frac{S^2}{4N} \right\rfloor = 267427392966.$$

We compute the

$$\gcd\left(\left\lfloor \frac{S^2}{4N} \right\rfloor, N\right) = (267427392966,\ 3678882512895663 2489)$$

$$= 70373.$$

Finally with $q = 70373$, we compute $p = \sqrt[3]{\frac{N}{q}} = 80557$, which leads to the factorization of N.

3.1. Estimation of the number of e's satisfying $eX - NY = (ap^r + bq^r)Z$

We give an estimation of the number of the exponents $e < N$ for which our attacks can be applied. Let a, b be integers such that $\gcd(a, b) = 1$. Let $(ap^r + bq^r) < N^{\frac{2}{3}+\alpha}$ with $0 < \alpha < \frac{1}{2}$.

Lemma 5. *Let $N = p^r q$ be a prime power modulus with $q < p < 2q$. Let a, b be integers such that $\gcd(a, b) = 1$ and suppose that e is a public exponent satisfying $e < N$ and two equation $eX_1 - NY_1 = (ap^r + bq^r)Z_1$ and $eX_2 - NY_2 = (ap^r + bq^r)Z_2$ with $\gcd(X_i, Y_i) = 1$, for $i = 1, 2$, $1 \le Y_i \le X_i < \frac{N}{2(ap^r + bq^r)Z}$, then $X_1 = X_2$, $Y_1 = Y_2$.*

Proof. Assume that the exponent e satisfying the two equation $eX_1 - NY_1 = (ap^r + bq^r)Z_1$ and $eX_2 - NY_2 = (ap^r + bq^r)Z_2$ with $\gcd(X_i, Y_i) = 1$, for $i = 1, 2, 1 \leq Y_i \leq X_i < \frac{N}{2(ap^r + bq^r)Z}$. Therefore equating the term $(ap^r + bq^r)Z$, we get

$$eX_1 - NY_1 = eX_2 - NY_2, \tag{2}$$

implies

$$eX_1 - NY_1 = eX_2 - NY_2,$$

$$e(X_1 - X_2) = N(Y_1 - Y_2),$$

$$\frac{e(X_1 - X_2)}{N} = (Y_1 - Y_2).$$

Since we assume $e < N$ and $Y < X$, then

$(X_1 - X_2) < |X_1 + X_2| < \frac{2N}{2(ap^r + bq^r)Z} < \frac{N}{(ap^r + bq^r)} < N$ therefore with $e < N$, $\gcd(e, N) = 1$ and $X_1 - X_2 < N$ we obtain $X_1 = X_2$, $Y_1 = Y_2$.

□

Theorem 5. *Let $N = p^r q$ be a prime power modulus with $q < p < 2q$. Let a, b be suitably small integers such that $\gcd(a, b) = 1$, and $(ap^r + bq^r) < N^{\frac{2}{3}+\alpha}$. The number of the exponents e of the form $e \equiv (ap^r + bq^r)X^{-1} (\mathrm{mod}\, N)$ with $\gcd(X, ap^r + bq^r) = 1$ and $X < \frac{1}{2} N^{\frac{1}{3}-\alpha}$ is at least $N^{\frac{1}{3}-\epsilon}$, where $\epsilon > 0$ is arbitrarily small for suitably large N.*

Proof. Let a, b be suitably small integers such that $\gcd(a, b) = 1$, and $(ap^r + bq^r) < N^{\frac{2}{3}+\alpha}$ and let $X_0 = \left\lfloor \frac{1}{2} N^{\frac{1}{3}-\alpha} \right\rfloor$. Let ξ denote the number of the exponents e satisfying $e \equiv (ap^r + bq^r)X^{-1} \pmod{N}$ with $\gcd(X, ap^r + bq^r) = 1$ and $X < \frac{1}{2} N^{\frac{1}{3}-\alpha}$

$$\xi = \sum_{\substack{X=1 \\ \gcd(X, ap^r+bq^r)=1}}^{X_0} 1. \tag{3}$$

Using the following result (see Nitaj [15], Lemma 3.3) with $n = ap^r + bq^r$ and $m = X_0$, we get

$$X_0 \frac{\phi(ap^r + bq^r)}{ap^r + bq^r} - 2^{\omega(ap^r+bq^r)} < \xi > X_0 \frac{\phi(ap^r + bq^r)}{ap^r + bq^r} + 2^{\omega(ap^r+bq^r)}. \tag{4}$$

Therefore, $2^{\omega(ap^r+bq^r)}$ is the number of square free divisors of $ap^r + bq^r$ which is upper bounded by the total number $\tau(ap^r + bq^r)$ of divisors of $ap^r + bq^r$. Hence using the identity that $\tau(n)$ satisfies $\tau(n) = \mathcal{O}(\log\log n)$ (see Hardy and Wright [6], Theorems 430-431). It follows that the dominant term in (4) is $X_0 \frac{\phi(ap^r + bq^r)}{ap^r + bq^r}$. Substituting this with $n = ap^r + bq^r$ and $X_0 = \left\lfloor \frac{1}{2} N^{\frac{1}{3}-\alpha} \right\rfloor$ gives

$$\xi = X_0 \frac{\phi(ap^r + bq^r)}{ap^r + bq^r} \leq \frac{1}{2} N^{\frac{1}{3}-\alpha} \frac{\phi(ap^r + bq^r)}{N^{\frac{2}{3}+\alpha}}$$

$$< \mathcal{O}\left(N^{-\frac{1}{3}-2\alpha} \phi(ap^r + bq^r)\right).$$

Also on the other hand, for $n \geq 2,$ we have the following identity (see Hardy and Wright [6], Theorem 328)

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

where c is a positive constant. Taking $n = ap^r + bq^r = N^{\frac{2}{3}+\alpha}$ implies that

$$\xi = \mathcal{O}\left(N^{-\frac{1}{3}-2\alpha} \frac{cN^{\frac{2}{3}+\alpha}}{\log \log N^{\frac{2}{3}+\alpha}}\right)$$

$$= \mathcal{O}(N^{\frac{1}{3}-\epsilon}),$$

where $\epsilon = \alpha + \epsilon_1$ satisfies $N^{\epsilon} = \log \log N$ and is arbitrarily small for suitably large N. □

Remark 1.1. From the two distinct n-bit prime (p, q), the resultant modulus $N = p^r q$ is $(r+1)$ n-bit integer. Then, we can observe that the number of exponents satisfying our attack is $N^{\frac{1}{3}-\epsilon} \approx 2^{(\frac{r+1}{3})n-(r+1)\epsilon}$. This proves that there are exponentially many exponents that satisfy our conditions in the Theorem 5.

4. The Second Attack on j Prime Power Moduli $N_i = p_i^r q_i$

In this section, for $j \geq 2, r \geq 2$ moduli $N_i = p_i^r q_i$ with the same size N. We suppose in this scenario that the prime power moduli satisfying the j equations $e_i x - N_i y_i = (ap_i^r + bq_i^r) z_i$. We proved that it is possible to factor the moduli N_i if the unknown parameters $x, y_i,$ and z_i are suitably small.

Theorem 6. *For* $j \geq 2$, *let* $N_i = p_i^r q_i$, $1 \leq i \leq j$ *be* j *moduli. Let* $N = \min N_i$. *Let* e_i, $i = 1, \ldots, j$, *be* j *public exponents. Define* $\delta = \frac{j(r-1) - 2\alpha j(r+1)}{2(r+1)}$, *where* $0 < \alpha \leq \frac{1}{3}$. *Let* a, b *be suitably small integers such that* $ap_i^r + bq_i^r < N^{\frac{r}{r+1}+\alpha}$. *If there exist an integer* $x < N^{\delta}$ *and* j *integers* $y_i < N^{\delta}$ *and* $|z_i| < \frac{1}{2}N^{\frac{1}{2}}$ *such that* $e_i x - N_i y_i = (ap_i^r + bq_i^r)z_i$ *for* $i = 1, \ldots, j$, *then one can factor the* j *moduli* $N_1, \ldots, N_j$ *in polynomial time.*

Proof. For $j \geq 2$ and $r \geq 2$, let $N_i = p_i^r q_i$, $1 \leq i \leq j$ be j moduli. Let $N = \min N_i$, and suppose that $y_i < N^{\delta}$, and $|ap_i^r + bq_i^r| < N^{\frac{r}{r+1}+\alpha}$, then the equation $e_i x - N_i y_i = (ap_i^r + bq_i^r)z_i$ can be rewritten as

$$\left|\frac{e_i}{N_i}x - y_i\right| = \frac{|(ap_i^r + bq_i^r)z_i|}{N_i}. \tag{5}$$

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

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

Substitute in to (5), to get

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

Hence to shows the existence of the integer x, we let $\varepsilon = \frac{1}{2}N^{\frac{1}{r+1}+\alpha-\frac{1}{2}}$, with $\delta = \frac{j(r-1)-2\alpha j(r+1)}{2(r+1)}$, then we have

$$N^{\delta}\varepsilon^{j} = \left(\frac{1}{2}\right)^{j} N^{\frac{j}{r+1}+\delta+\alpha j-\frac{j}{2}} = \left(\frac{1}{2}\right)^{j}.$$

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

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

Hence it satisfy the conditions of Theorem 3, and we can obtain x and y_i for $i = 1, \ldots, j$.

Next using the equation $e_i x - N_i y_i = (ap_i^r + bq_i^r)z_i$. Since $|z_i| < \frac{1}{2}N^{\frac{1}{2}}$. Then Lemma 2 implies that $q_i^{r-1}z_i^2 ab = \left\lceil \frac{S_i^2}{4N_i} \right\rceil$ with $S_i = e_i x - N_i y_i$ for $i = 1, \ldots, j$, we compute $q_i = \gcd\left(N_i, \left\lceil \frac{S_i^2}{4N_i} \right\rceil\right)$. Which leads to factorization of j moduli $N_i, \ldots, N_j$. □

Example 2.2. As an illustration to our attack on j prime power moduli $N_i = p_i^r q_i$, we consider the following three prime power and three public exponents:

$$N_1 = 17045097945895618685155952441339893600689182583574082 21,$$

$$e_1 = 33849575291641579016778267980488779906142169932227998 8,$$

$$N_2 = 33719247071717691458191412567482962078715432369622918 9,$$

$$e_2 = 15828169124830058511963055060542574333652195793017649 6,$$

$$N_3 = 34148126779162067538572619688979041794249503583268925 3,$$

$$e_3 = 39647198399758278340940098400026445259840074660851452 3.$$

Then $N = \min(N_1, N_2, N_3) =$ 337192470717176914581914125674 8296207871543236962291 89. Since $j = 3$ and $r = 3$ $a = 2$, $b = 3$, with $\alpha = 0.2$, we get $\delta = \frac{j(r-1) - 2\alpha j(r+1)}{2(r+1)} = 0.15$ and $\varepsilon = \frac{1}{2} N^{\frac{1}{r+1}+\alpha-\frac{1}{2}}$ $= 0.001053358274$. Using Theorem 3, with $n = j = 3$, we obtained

$$C = [3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1}] = 32896567070000.$$

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:

$$K = \begin{bmatrix} -114011317 & 6055627 & 73217384 & 90488217 \\ -4867213808 & -9691416752 & -30568298384 & 19143379408 \\ 27668984032 & -55826375792 & 16618205936 & 25266163568 \\ -51875747251 & -45872210819 & -19741736248 & -46322992049 \end{bmatrix}.$$

Next we compute

$$K \cdot M^{-1} = \begin{bmatrix} -114011317 & -22641317 & -53518111 & -132371223 \\ -4867213808 & -966571860 & -2284721339 & -5651009578 \\ 27668984032 & 5494737321 & 12988112037 & 32124681583 \\ -51875747251 & -10301917994 & -24351021220 & -60229600783 \end{bmatrix}.$$

Then from the first row we obtained $x = 114011317$, $y_1 = 22641317$, $y_2 = 53518111$, $y_3 = 132371223$. Hence using x and y_i for $i = 1, 2, 3$, define $S_i = e_i x - N_i y_i$ we get

$$S_1 = 4506429282145174322765316975531700445571 39,$$

$$S_2 = 127282857626254792126010153333292333063253,$$

$$S_3 = 136982941525724752298529650018124382290372.$$

And Lemma 2 implies that $q_i^{r-1} z_i^2 ab = \left\lfloor \frac{S_i^2}{4N_i} \right\rfloor$ for $i = 1, 2, 3$, which gives

$$\left\lfloor \frac{S_1^2}{4N_1} \right\rfloor = 29785550278790743767615058584,$$

$$\left\lfloor \frac{S_2^2}{4N_2} \right\rfloor = 120116307839314965105877816 56,$$

$$\left\lfloor \frac{S_3^2}{4N_3} \right\rfloor = 13737449194790479890699360984.$$

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

$$q_1 = 35228746712729,\ q_2 = 22371513493663,\ q_3 = 23924751126179.$$

Finally for $i = 1, 2, 3,$ we find $p_i = \sqrt[3]{\frac{N_i}{q_i}}$, hence $p_1 = 36439082724349$, $p_2 = 24701737414787$, $p_3 = 24257152513543$, which leads to the factorization of three moduli N_1, N_2, and N_3.

5. The Third Attack on *j* Prime Power Moduli $N_i = p_i^r q_i$

We present an attack on the prime power moduli $N_i = p_i^r q_i$. For $j \geq 2$ and $r \geq 2$, we consider the scenario when the j moduli satisfy j equations of the form $e_i x_i - N_i y = (ap_i^r + bq_i^r) z_i$ for $i = 1, \ldots, j$, with suitably small unknown parameters $x_i y$ and z_i. Applying the LLL algorithm we show that our approach enable us to factor the prime power moduli N_i in polynomial time.

Theorem 7. *For* $j \geq 2$ *and* $r \geq 2$, *let* $N_i = p_i^r q_i, 1 \leq i \leq j$ *be* j *moduli with the same size N. Let* $e_i, i = 1, \ldots, j$, *be* j *public exponents with* $\min\ e_i = N^{\beta}, 0 < \beta < 1$. *Let* $\delta = \frac{jr(2\beta - 2\alpha - 1) + j(2\beta - 2\alpha - 3)}{2(r+1)}$, *where* $0 < \alpha \leq \frac{1}{3}$. *Let* a, b *be suitably integers such that* $ap_i^r + bq_i^r < N^{\frac{r}{r+1}+\alpha}$. *If there exist an integer* $y < N^{\delta}$ *and* j *integers* $x_i < N^{\delta}$ *such that* $e_i x_i - N_i y = (ap_i^r + bq_i^r) z_i$ *for* $i = 1, \ldots, j$, *then one can factor the* j *moduli* $N_1, \ldots, N_j$ *in polynomial time.*

Proof. For $j \geq 2$ and $r \geq 2$, let $N_i = p_i^r q_i$, $1 \leq i \leq j$ be j moduli. Then the equation $e_i x_i - N_i y = (ap_i^r + bq_i^r)z_i$ can be rewritten as

$$\left|\frac{N_i}{e_i} y - x_i\right| = \frac{|(ap_i^r + bq_i^r)z_i|}{e_i}. \tag{6}$$

Let $N = \max N_i$, and suppose that $y < N^{\delta}$, $|z_i| < \frac{1}{2} N^{\frac{1}{2}}$, $\min e_i = N^{\beta}$ and $ap_i^r + bq_i^r < N^{\frac{r}{r+1}+\alpha}$, then

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

Plugging in to (6), to get

$$\left|\frac{N_i}{e_i} y - x_i\right| < \frac{1}{2} N^{\frac{1}{r+1}+\frac{1}{2}+\alpha-\beta}.$$

Hence to shows the existence of the integer y and integers x_i, we let $\varepsilon = \frac{1}{2} N^{\frac{1}{r+1}+\frac{1}{2}+\alpha-\beta}$, with $\delta = \frac{jr(2\beta - 2\alpha - 1) + j(2\beta - 2\alpha - 3)}{2(r+1)}$, we get

$$N^{\delta}\varepsilon^j = \left(\frac{1}{2}\right)^j N^{\delta+\frac{j}{r+1}+\frac{j}{2}+\alpha j-\beta j} = \left(\frac{1}{2}\right)^j.$$

Therefore since $\left(\frac{1}{2}\right)^j < 2^{\frac{j(j-3)}{4}} \cdot 3^j$ for $j \geq 2$, we get $N^{\delta}\varepsilon^j < 2^{\frac{j(j-3)}{4}} \cdot 3^j$.

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

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

Hence it satisfy the conditions of Theorem 3, and we can obtain y and x_i for $i = 1, \ldots, j$.

Next from the equation $e_i x_i - N_i y = (ap_i^r + bq_i^r)z_i$. Since $|z_i| < \frac{1}{2} N^{\frac{1}{2}}$. Then Lemma 2 implies that $q_i^{r-1} z_i^2 ab = \left[\frac{S_i^2}{4N_i}\right]$ with $S_i = e_i x_i - N_i y$ for $i = 1, \ldots, j$, we compute $q_i = \gcd\left(N_i, \left[\frac{S_i^2}{4N_i}\right]\right)$. Which leads to factorization of j moduli $N_i, \ldots, N_j$. □

Example 3.3. As an illustration to our attack on j prime power moduli $N_i = p_i^r q_i$, we consider the following three prime power and three public exponents:

$N_1 = 94986711397407221711007482750056210640371957949407155 7,$

$e_1 = 968704891042970066369652928957481456246576606936674853,$

$N_2 = 262275319092318010637574979619075550506568907989717923,$

$e_2 = 263538429122381233357593267961398695157179502108793860,$

$N_3 = 211089221682124580503194910838862462545904186015524098 3,$

$e_3 = 197673468102366477854424092341591867271847201535648968 0.$

Then $N = \max(N_1, N_2, N_3) =$ 21108922168212458050319491083886246254590418601552409 83. Also $\min(e_1, e_2, e_3) = N^{\beta}$ with $\beta = 0.983342$. Since $j = 3$ and $r = 3$, $a = 2, b = 3$, with $\alpha = 0.2$, we get $\delta = \frac{jr(2\beta - 2\alpha - 1) + j(2\beta - 2\alpha - 3)}{2(r+1)} = 0.1000260000$ and $\varepsilon = \frac{1}{2} N^{\frac{1}{r+1} + \frac{1}{2} + \alpha - \beta}$ $= 0.00772117964 5$. Using Theorem 3, with $n = j = 3$, we obtained

$$C = [3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1}] = 11395159140.$$

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:

$$K = \begin{bmatrix} 123725 & 20785 & 92080 & 13080 \\ -30294472 & 104786860 & 37687768 & -145129860 \\ -15483984 & -180263460 & 72564276 & -77804220 \\ 139136373 & -16873995 & 166858032 & -114784320 \end{bmatrix}.$$

Next we compute

$$K \cdot M^{-1} = \begin{bmatrix} 123725 & 121319 & 123132 & 132122 \\ -30294472 & -29705355 & -30149274 & -32350505 \\ -15483984 & -15182877 & -15409771 & -16534855 \\ 139136373 & 136430678 & 138469508 & 148579316 \end{bmatrix}.$$

Then from the first row we obtained $y = 123725$, $x_1 = 121319$, $x_2 = 123132$, $x_3 = 132122$. Hence using x and y_i for $i = 1, 2, 3$, define $S_i = e_i x_i - N_i y$ we get

$$S_1 = 41995591565568564617557822240404645310128 2,$$

$$S_2 = 159653209917252821645668588312632155546345,$$

$$S_3 = 643244295848175425091990005465222938879285.$$

And Lemma 2 implies that $q_i^{r-1} z_i^2 ab = \left[\frac{S_i^2}{4N_i}\right]$ for $i = 1, 2, 3$, which gives

$$\left[\frac{S_1^2}{4N_1}\right] = 46417801105971176693248343574,$$

$$\left[\frac{S_2^2}{4N_2}\right] = 24296174269366246412626731366,$$

$$\left[\frac{S_3^2}{4N_3}\right] = 49003357542846686156958208326.$$

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

$$q_1 = 29318746722359,\ q_2 = 21211533493277,\ q_3 = 30124235826437.$$

Finally for $i = 1, 2, 3$, we find $p_i = \sqrt[3]{\frac{N_i}{q_i}}$, hence $p_1 = 31879082726747$, $p_2 = 23123937435199$, $p_3 = 41227152517619$, which leads to the factorization of three moduli N_1, N_2, and N_3.

6. Conclusion

We proposed the first attack based on the equation $eX - NY = (ap^r + bq^r)Z$ for suitable positive integers a, b. Using continued fraction, we show that $\frac{Y}{X}$ can be recovered among the convergents of the continued fractions 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 $N^{\frac{1}{3}-\varepsilon}$, where $\varepsilon \geq 0$ is arbitrarily small for suitably large N. Hence one can factor the prime power modulus $N = p^r q$ in polynomial time. For $j \geq 2$, $r \geq 2$, we then present second and third attacks on the prime power moduli $N_i = p_i^r q_i$ for $i = 1, \ldots, j$. The attacks work when j public keys (N_i, e_i) are such that there exist j relations of the shape $e_i x - N_i y_i = (ap_i^r + bq_i^r)z_i$ or of the shape $e_i x_i - N_i y = (ap_i^r + bq_i^r)z_i$, where the parameters x, x_i, y, y_i, z_i are suitably small in terms of the prime factors of the moduli. Based on LLL algorithm, we show that our approach enable us to simultaneously factor the j prime power moduli N_i in polynomial time.

References

[1] M. R. K. Ariffin and S. Shehu, New attacks on prime power RSA modulus $N = p^r q$, Asian Journal of Mathematics and Computer Research (2016), 77-90.

[2] M. A. Asbullah and M. R. K. Ariffin, New attacks on RSA with modulus $N = p^2 q$ using continued fractions, Journal of Physics, Conference Series, Volume 622, No. 1, IOP Publishing, 2015.

[3] D. Boneh, G. Durfee and N. Howgrave-Graham, Factoring $N = p^r q$ for large r, Advances in Cryptology CRYPTO'99, Lecture Notes in Computer Science 1592 (1999), 326-337.

[4] J. Blomer and A. May, A generalized Wiener attack on RSA, In Public Key Cryptography - PKC 2004, Lecture Notes in Computer Science 2947 (2004), 1-13.

[5] A. Fujioka, T. Okamoto and S. Miyaguchi, ESIGN: An efficient digital signature implementation for smart cards, Advances in Cryptology EURO-CRYPT 91, Springer-Verlag (1991), 446-457.

[6] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, London, 1975.

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

[8] N. Howgrave-Graham and J. P. Seifert, Extending wieners attack in the presence of many decrypting exponents, In Secure Networking-CQRE (Secure)'99, 1740 (1999), 153-166.

[9] A. K. Lenstra, H. W. Lenstra and L. Lovasz, Factoring polynomials with rational coefficients, Mathematische Annalen 261 (1982), 513-534.

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

[11] A. Nitaj, Diophantine and lattice cryptanalysis of the RSA cryptosystem, Artificial Intelligence, Evolutionary Computing and Metaheuristics, Springer Berlin, Heidelberg (2013), 139-168.

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

[13] A. Nitaj, M. R. K. Ariffin, D. I. Nassr and H. M. Bahig, New attacks on the RSA cryptosystem, Progress in Cryptology-AFRICACRYPT 2014, Springer International Publishing (2014), 178-198.

[14] A. Nitaj, A New Vulnerable Class of Exponents in RSA, 2011.

[15] T. Okamoto and S. Uchiyama, A new public-key cryptosystem as secure as factoring, Advances in Cryptology-EUROCRYPT'98, Springer-Verlag (1998), 308-318.

[16] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21(2) (1978), 120-126.

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

[18] T. Takagi, Fast RSA-type cryptosystem modulo $p^k q$, In Advances in Cryptology-Crypto'98, Springer (1998), 318-326.

[19] M. Wiener, Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory 36 (1990), 553-558.

■