Malaysian Journal of Mathematical Sciences 11(S) August: 121 - 138 (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 Attacks on Prime Power $N = p^r q$ Using Good Approximation of $\phi(N)$

Shehu, S.[1] and **Ariffin, M.R.K.**[2]

[1,2]*Al-Kindi Cryptography Research Laboratory, Institute for Mathematical Research, Universiti Putra Malaysia (UPM), Selangor, Malaysia*
[2]*Department of Mathematics, Faculty of Science, Universiti Putra Malaysia (UPM), Selangor, Malaysia*

*E-mail: *sadiqshehuzezi@gmail.com , rezal@upm.edu.my*
**Corresponding author*

ABSTRACT

This paper proposes three new attacks. Our first attack is based on the RSA key equation $ed - k\phi(N) = 1$ where $\phi(N) = p^{r-1}(p-1)(q-1)$. Let $q < p < 2q$ and $2p^{\frac{3r+2}{r+1}} \left| p^{\frac{r-1}{r+1}} - q^{\frac{r-1}{r+1}} \right| < \frac{1}{6}N^{\gamma}$ with $d = N^{\delta}$. If $\delta < \frac{1-\gamma}{2}$ we shows that $\frac{k}{d}$ can be recovered among the convergents of the continued fractions expansions of $\frac{e}{N-2N^{\frac{r}{r+1}}+N^{\frac{r-1}{r+1}}}$. We furthered our analysis on j prime power moduli $N_i = p_i^r q_i$ satisfying a variant of the above mentioned condition. We utilized the LLL algorithm on j prime power public keys (N_i, e_i) with $N_i = p_i^r q_i$ and we were able to factorize the j prime power moduli $N_i = p_i^r q_i$ simultaneously in polynomial time.

Keywords: Prime Power, Factorization, LLL algorithm, Simultaneous diophantine approximations, Continued fractions

1. Introduction

Apart from the basic RSA proposal several variants has been proposed in order to ensure computational efficiency while maintaining the acceptable level of security. One of such important variant is the prime power modulus. In the prime power the modulus is in the form $N = p^r q$ for $r \geq 2$. As in the standard RSA cryptosystem, the security of prime power modulus depend on the difficulty of factoring integers of the form $N = p^r q$.

Takagi (1998) proposes a cryptosystem 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.

As described in Boneh and Durfee (2000), schemes with modulus of the form $N = p^r q$ are more susceptible to attacks that leak bits of p than the original RSA-scheme. Using Coppersmith's method for solving univariate modular equations, they showed that it suffices to know a fraction of $\frac{1}{r+1}$ of the MSBs of p to factor the modulus.

May (2003) considered RSA-type schemes with modulus $N = p^r q$ for $r \geq 2$, and presented two new attacks for small secret exponent d. Both approaches are applications of Coppersmith's method for solving modular univariate polynomial equations. From these new attacks they directly derive partial key exposure attacks, that is attacks when the secret exponent is not necessarily small but when a fraction of the secret key bits is known to the attacker.

Asbullah and Ariffin (2015) 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 $N = p^r q$ for $r = 2$ in polynomial time.

Our contribution, as motivated from the recent result of Asbullah and Ariffin (2015), De Weger (2002), Nitaj (2011), Nitaj et al. (2014), Nitaj and Rachidi (2015), Wiener (1990). This paper, proposes three new attacks on the prime power modulus $N = p^r q$. In the first attack, we consider an instance of the prime power modulus $N = p^r q$ and public of exponent e satisfying the equation $ed - k\phi(N) = 1$ for some unknown integers $\phi(N)$, d,k. Applying continued fractions we show that $\frac{k}{d}$ can be recovered among the convergents of the continued fractions expansions of $\frac{e}{N - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}}}$. Hence one can factor the modulus $N = p^r q$ in polynomial time.

The second attack works with j instances (N_i, e_i) when there exist integer d and j integers k_i, satisfying $e_i d - k_i \phi(N_i) = 1$. We show that the j moduli N_i can be factored in polynomial time if $N = min_i\ N_i$ and

$$d < N^{\delta}, \quad k_i < N^{\delta}, \quad where \quad \delta = \frac{j - \beta j}{(j+1)}$$

In the third attack we show that the j moduli N_i can be factored in polynomial time, when the j instance (N_i, e_i) are such that there exist an integer k, and j integers d_i satisfying $e_i d_i - k\phi(N_i) = 1$ with $N = min_i\ N_i$, $min_i\ e_i = N^{\beta}$ and

$$d_i < N^{\delta}, \quad k < N^{\delta}, \quad where \quad \delta = \frac{\beta j - \gamma j}{(1+j)}$$

For the second and third attacks we transformed the equations into a simultaneous diophantine problem and apply lattice basis reduction techniques to find the parameters (d, k_i) or (k, d_i) which leads to factorization of j moduli N_i in polynomial time.

The rest of the paper is structured as follows. In section 2, we give a brief review of basic facts about the continued fractions, previous attacks using good approximation of $\phi(N)$, lattice basis reductions and simultaneous diophantine approximations with some useful results needed for the attack. In section 3, 4 and 5, we put forward the first, second and third attacks. We conclude this paper in section 6.

2. Preliminaries

We start with definitions and an important results concerning the continued fractions, lattice basis reduction techniques and simultaneous diophantine equations as will as some useful lemmas needed for the attacks.

2.1 Continued fractions

Definition 2.1 (Continued Fractions). *The continued fractions 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 number $a_0, a_1, a_2....$ are called the partial quotients. We use the notation $R = [a_0, a_1, a_2....]$. For $i \geq 1$ the rational $\frac{r_i}{s_i} = [a_0, a_1, a_2, ...]$ 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 expansions is finite.

Theorem 2.1 (Legendre). *Let $x = [a_0, a_1, a_2, ...a_m]$ be a continued fractions 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 Lattices

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

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

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

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 $b_1 ..., b_m$

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

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 $B = \langle b_1, ..., b_m \rangle$. The determinant of $\mathcal{L}$ is defined as

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

If $n = m$, we have

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

Theorem 2.2. *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*

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

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 $\alpha_1, ..., \alpha_n$ 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

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

A method to find simultaneous diophantine approximations to rational numbers was described by Lenstra et al. (1982). In their work, they considered a lattice with real entries. Below a similar result for a lattice with integer entries.

Theorem 2.3 (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*

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

Proof. See (Nitaj et al., 2014) (In Appendix A). □

Lemma 2.1. *Let $N = p^r q$ be a prime power modulus 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. Let $N = p^r q$ and suppose $q < p < 2q$. Then multiplying 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

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

Let $N = p^r q$ therefore using $\phi(N) = p^{r-1}(p-1)(q-1)$ we compute the approximation of $\phi(N)$ that is

$$\begin{aligned}\phi(N) &= p^{r-1}(pq - p - q + 1)\\ &= p^r q - p^r - p^{r-1} q + p^{r-1}\\ &= N - (p^r + p^{r-1} q - p^{r-1})\end{aligned}$$

The following result gives an interval for $N - \phi(N) = p^r + p^{r-1}q - p^{r-1}$ in terms of N. it shows that if $p \approx q$ then

$$\begin{aligned}N - \left((N^{\frac{1}{r+1}})^r + (N^{\frac{1}{r+1}})^{r-1} N^{\frac{1}{r+1}} - (N^{\frac{1}{r+1}})^{r-1}\right) &= N - \left(N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}} N^{\frac{1}{r+1}} - N^{\frac{r-1}{r+1}}\right)\\ &= N - \left(N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}+\frac{1}{r+1}} - N^{\frac{r-1}{r+1}}\right)\\ &= N - \left(N^{\frac{r}{r+1}} + N^{\frac{r}{r+1}} - N^{\frac{r-1}{r+1}}\right)\\ &= N - \left(2N^{\frac{r}{r+1}} - N^{\frac{r-1}{r+1}}\right)\end{aligned}$$

Which is a good approximation to $\phi(N)$. Also if $p \approx 2q$ then

$$\begin{aligned}&N - \left((2^{\frac{1}{r+1}} N^{\frac{1}{r+1}})^r + (2^{\frac{1}{r+1}} N^{\frac{1}{r+1}})^{r-1} N^{\frac{1}{r+1}} - 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}\right)\\ &= N - \left((2^{\frac{r}{r+1}} N^{\frac{r}{r+1}}) + (2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}}) N^{\frac{1}{r+1}} - 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}\right)\\ &= N - \left(2^{\frac{r}{r+1}} N^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}+\frac{1}{r+1}} - 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}\right)\\ &= N - \left(2^{\frac{r}{r+1}} N^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} N^{\frac{r}{r+1}} - 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}\right)\\ &= N - \left(\left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) N^{\frac{r}{r+1}} - 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}\right)\end{aligned}$$

Which is also a good approximation to $\phi(N)$.

□

Lemma 2.2. *Let $N = p^r q$ be a prime power modulus with $q < p < 2q$ and $\phi(N) = N - (p^r + p^{r-1}q - p^{r-1})$ then $\left|N - (2N^{\frac{r}{r+1}} - N^{\frac{r-1}{r+1}}) - \phi(N)\right| < 2p^{\frac{3r+2}{r+1}} \left|p^{\frac{r-1}{r+1}} - q^{\frac{r-1}{r+1}}\right|$*

Proof. Let $N = p^r q$ be a prime power modulus and suppose that $\phi(N) = p^{r-1}(p-1)(q-1) = p^r q - p^r - p^{r-1}q + p^{r-1} = N - (p^r + p^{r-1}q - p^{r-1})$ Then

$$
\begin{aligned}
&\left|N - \left(2N^{\frac{r}{r+1}} - N^{\frac{r-1}{r+1}}\right) - \phi(N)\right| \\
&= \left|N - \phi(N) - \left(2N^{\frac{r}{r+1}} - N^{\frac{r-1}{r+1}}\right)\right| \\
&= \left|p^r + p^{r-1}q - p^{r-1} - \left(2N^{\frac{r}{r+1}} - N^{\frac{r-1}{r+1}}\right)\right| \\
&= \left|p^r + p^{r-1}q - p^{r-1} - \left(2\left(p^r q\right)^{\frac{r}{r+1}} - \left(p^r q\right)^{\frac{r-1}{r+1}}\right)\right| \\
&= \left|p^r + p^{r-1}q - p^{r-1} - \left(2p^{\frac{r^2}{r+1}} q^{\frac{r}{r+1}} - p^{\frac{r^2-r}{r+1}} q^{\frac{r-1}{r+1}}\right)\right| \\
&= \left|p^r - 2p^{\frac{r^2}{r+1}} q^{\frac{r}{r+1}} - p^{r-1} + p^{r-1}q + p^{\frac{r^2-r}{r+1}} q^{\frac{r-1}{r+1}}\right| \\
&< \left|p^{\frac{r-1}{r+1}} - q^{\frac{r-1}{r+1}}\right| \times p^{\frac{r}{r+1}} \left(p^{\frac{3}{r+1}} + p^{\frac{2}{r+1}} q^{\frac{r-1}{r+1}} - p^{\frac{r^2-2r+1}{r+1}} q^{\frac{1}{r+1}} - p^{\frac{r^2-r}{r+1}}\right) \\
&< \left|p^{\frac{r-1}{r+1}} - q^{\frac{r-1}{r+1}}\right| \times p^{\frac{r}{r+1}} \left(p^{\frac{3}{r+1}} + p^{\frac{2}{r+1}} q^{\frac{r-1}{r+1}}\right) \\
&< \left|p^{\frac{r-1}{r+1}} - q^{\frac{r-1}{r+1}}\right| \times p^{\frac{r}{r+1}} \times 2p^2 \\
&= 2p^{\frac{3r+2}{r+1}} \left|p^{\frac{r-1}{r+1}} - q^{\frac{r-1}{r+1}}\right|
\end{aligned}
$$

Which terminate the proof. □

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

Let (N, e) be a public key satisfying an equation satisfying an equation $ed - k\phi(N) = 1$ for some unknown integers $\phi(N)$, d,k. In this section, we present a result based on continued fractions and show how to factor the prime power modulus $N = p^r q$

Theorem 3.1. *Let $N = p^r q$ be a prime power modulus with $q < p < 2q$. Let*

$1 < e < \phi(N) < N - \left(2N^{\frac{r}{r+1}} - N^{\frac{r-1}{r+1}}\right)$ *and* $ed - k\phi(N) = 1$ *for unknown integers* $(\phi(N), d, k)$*. If* $\delta < \frac{1-\gamma}{2}$*, then*

$$\left|\frac{e}{N - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}}} - \frac{k}{d}\right| < \frac{1}{2d^2}$$

where $\gamma \in (0.75, 0.8)$.

Proof. We transform the equation $ed - k\phi(N) = 1$ in to

$$ed - k(p^{r-1}(p-1)(q-1)) = 1$$

$$ed - k(p^{r-1}(pq - p - q + 1)) = 1$$
$$ed - k(p^{r-1}pq - p^{r-1}p - p^{r-1}q + p^{r-1}) = 1$$
$$ed - k(p^r q - p^r - p^{r-1}q + p^{r-1}) = 1$$
$$ed - k(N - (p^r + p^{r-1}q - p^{r-1})) = 1$$
$$ed - k(N - (N - \phi(N))) = 1$$

Since $N - \phi(N) = p^r + p^{r-1}q - p^{r-1}$ then

$$ed - k\left(N - (2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}}) + (2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}}) - (N - \phi(N))\right) = 1$$

$$ed - k\left(N - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}}\right) = 1 + k\left(N - \phi(N) - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}}\right)$$

Divide by $d(N - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}})$ we get

$$\begin{aligned}
\left|\frac{e}{N - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}}} - \frac{k}{d}\right| &= \left|\frac{e}{N - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}}} - \frac{e}{\phi(N)} + \frac{e}{\phi(N)} - \frac{k}{d}\right| \\
&\leq \left|\frac{e}{N - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}}} - \frac{e}{\phi(N)}\right| + \left|\frac{e}{\phi(N)} - \frac{k}{d}\right| \\
&\leq \left|\frac{e\phi(N) - e(N - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}})}{\phi(N)(N - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}})}\right| + \left|\frac{ed - k\phi(N)}{\phi(N)d}\right| \\
&\leq e\left|\frac{N - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}} - \phi(N)}{\phi(N)(N - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}})}\right| + \frac{1}{\phi(N)d} \\
&\leq \left|\frac{N - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}} - \phi(N)}{\phi(N)}\right| + \frac{1}{\phi(N)d}
\end{aligned}$$

Since $1 < e < \phi(N) < N - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}}$ and $ed - k\phi(N) = 1$. Since $\phi(N) > \frac{2}{3}N$ with $N > 6d$, then we have $\phi(N) > \frac{2}{3}N > \frac{2}{3} \times 6d > 4d$ and by hypothesis of the theorem $2p^{\frac{3r+2}{r+1}} \left| p^{\frac{r-1}{r+1}} - q^{\frac{r-1}{r+1}} \right| < \frac{1}{6}N^{\gamma}$ and $d = N^{\delta}$ then

$$\begin{aligned}
\left| \frac{N - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}} - \phi(N)}{\phi(N)} \right| + \frac{1}{\phi(N)d} &< \frac{2p^{\frac{3r+2}{r+1}} \left| p^{\frac{r-1}{r+1}} - q^{\frac{r-1}{r+1}} \right|}{\phi(N)} + \frac{1}{\phi(N)d} \\
&< \frac{\frac{1}{6}N^{\gamma}}{\frac{2}{3}N} + \frac{1}{4d^2} \\
&< \frac{1}{4}N^{\gamma-1} + \frac{1}{4}N^{-2\delta}
\end{aligned}$$

For the Theorem 2.1, to satisfy it is suffice to shows that if $\gamma - 1 < -2\delta$ then $\delta < \frac{1-\gamma}{2}$, that is if

$$\begin{aligned}
\frac{1}{4}N^{\gamma-1} + \frac{1}{4}N^{-2\delta} &< \frac{1}{4}N^{\gamma-1} + \frac{1}{4}N^{-2\times\frac{1-\gamma}{2}} \\
&< \frac{1}{4}N^{\gamma-1} + \frac{1}{4}N^{\gamma-1} \\
&< \frac{1}{2d^2}
\end{aligned}$$

Then $\frac{k}{d}$ is among the convergent of the continued fraction expansion of

$$\frac{e}{N - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}}}$$

□

Corollary 3.1. *Upon obtaining the secret exponent d, then the prime power modulus $N = p^r q$ can be factored in polynomial time.*

Proof. Observe that from Theorem 3.1, and the equation $ed - k\phi(N) = 1$ we get the relation $\frac{ed-1}{k} = \phi(N) = p^{r-1}(p-1)(q-1)$. Hence computing $gcd\left(N, \frac{ed-1}{k}\right)$ gives the prime factored p, which leads to the factorization of prime power modulus $N = p^r q$. □

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

Algorithm 1

Input: $N = p^r q$, with $q < p < 2q$ and public key (e, N) and Theorem 3.1.
Output: the prime factors p and q.
1: Compute the continued fraction expansion of $\frac{e}{N-2N^{\frac{r}{r+1}}+N^{\frac{r-1}{r+1}}}$.
2: For each convergent $\frac{k}{d}$ of $\frac{e}{N-2N^{\frac{r}{r+1}}+N^{\frac{r-1}{r+1}}}$, compute $\frac{ed-1}{k}$
3: Compute $p^{r-1} = gcd\left(N, \frac{ed-1}{k}\right)$
4: If $1 < p^{r-1} < N$, then $q = \frac{N}{p^r}$

Example 3.1. *As an example to illustrate our attack for $r = 3$, $d = 101$, $k = 65$, let us take for N and e the numbers*

$$N = 412850076201344480207$$

$$e = 265688720870514275 01$$

Suppose that N and e satisfy all the condition stated in Theorem 3.1, and Corollary 3.1, then $\frac{k}{d}$ is one of the convergent of the continued fraction of $\frac{e}{N-2N^{\frac{r}{r+1}}+N^{\frac{r-1}{r+1}}}$. Also the convergent of the continued fraction expansion of $\frac{e}{N-2N^{\frac{r}{r+1}}+N^{\frac{r-1}{r+1}}}$ are

$$\left[0, 1, \frac{1}{2}, \frac{2}{3}, \frac{9}{14}, \frac{65}{101}, \frac{10799}{16780}, ...\right]$$

Applying the factorization algorithm with the convergent $\frac{k}{d} = \frac{65}{101}$, we obtain

$$\frac{ed-1}{k} = \frac{(265688720870514275 01)(101) - 1}{65} = 412839397044952950 40$$

Hence we compute
$p = \sqrt{gcd\left(N, \frac{ed-1}{k}\right)} = \sqrt{gcd(412850076201344480207, 41283939704495295040)} =$ 82913. *Finally for $p = 82913$ we compute $q = \frac{N}{p^3} = 72431$, which leads to the factorization of N.*

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

For $j \geq 2$ and $r \geq 2$, let $N_i = p_i^r q_i$, $i = 1, ..., j$ be j moduli. This attack works upon j instances (N_i, e_i) when there exist an integer d and j integers k_i, satisfying $e_i d - k_i \phi(N_i) = 1$. We prove that the j moduli N_i for $i = 1, ..., j$, can be factored in polynomial time if $N = min\ N_i$ and

$$d < N^{\delta}, \quad k_i < N^{\delta}, \quad where \quad \delta = \frac{j - \gamma j}{(j+1)}$$

Theorem 4.1. *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 $N = min\ N_i$. Let e_i, $i = 1, ..., j$, be j public exponents. Define $\delta = \frac{j-\gamma j}{(j+1)}$ where $0 < \gamma \leq \frac{3}{4}$. Let $1 < e_i < \phi(N_i) < N_i - \nabla$ where $\nabla = 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}}$. If there exist an integer $d < N^{\delta}$ and j integers $k_i < N^{\delta}$ such that*

$$e_i d - k_i \phi(N_i) = 1$$

for $i = 1, ..., j$, then one can factor the j prime power moduli $N_1, ..., N_j$ in polynomial time.

Proof. We have

$$e_i d - k_i(N_i - (N_i - \phi(N_i))) = 1$$

$$e_i d - k_i(N_i - \nabla + \nabla - (N_i - \phi(N_i)) = 1$$

$$e_i d - k_i(N_i - \nabla) = 1 - k_i(N_i - \phi(N_i) - \nabla)$$

$$\left| \frac{e_i}{N_i - \nabla} d - k_i \right| = \frac{|1 - k_i(N_i - \phi(N_i) - \nabla)|}{N_i - \nabla} \tag{1}$$

Let $N = min\ N_i$, and suppose that $k_i < N^{\delta}$, and $|(N_i - \phi(N_i) - \nabla)| <$

$2p_i^{\frac{3r+2}{r+1}}\left|p_i^{\frac{r-1}{r+1}} - q_i^{\frac{r-1}{r+1}}\right|$. Then

$$\begin{aligned}
\frac{|1-k_i(N_i-\phi(N_i)-\nabla)|}{N_i-\nabla} &\leq \frac{|1+k_i(N_i-\phi(N_i)-\nabla)|}{N-\nabla} \\
&< \frac{1+N^{\delta}\left(N_i-(2N^{\frac{r}{r+1}}+N^{\frac{r-1}{r+1}})-\phi(N)\right)}{\phi(N)} \\
&< \frac{1+N^{\delta}\left(2p_i^{\frac{3r+2}{r+1}}\left|p_i^{\frac{r-1}{r+1}}-q_i^{\frac{r-1}{r+1}}\right|\right)}{\phi(N)} \\
&< \frac{N^{\delta}(\frac{1}{6}N^{\gamma})}{\frac{2}{3}N} \\
&< \frac{1}{4}N^{\delta+\gamma-1}
\end{aligned}$$

Plugging in to (1), we get

$$\left|\frac{e_i}{N_i-\nabla}d-k_i\right| < \frac{1}{4}N^{\delta+\gamma-1}$$

To show existence of the integer d and integers k_i, we let $\varepsilon = \frac{1}{4}N^{\delta+\gamma-1}$, with $\delta = \frac{j-\gamma j}{(j+1)}$. This will give us

$$N^{\delta}\varepsilon^{j} = \left(\frac{1}{4}\right)^{j} N^{\delta+\delta j+\gamma j-j} = \left(\frac{1}{4}\right)^{j}$$

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

$$\left|\frac{e_i}{N_i-\nabla}d-k_i\right| < \varepsilon, \qquad d < 2^{\frac{j(j-3)}{4}} \cdot 3^{j} \cdot \varepsilon^{-j}$$

The above satisfies the conditions of Theorem 2.3, and we can obtain d and k_i for $i = 1, ..., j$. Next, from the equation $e_i d - k_i\phi(N_i) = 1$ we will get

$$\frac{e_i d-1}{k_i} = \phi(N_i) = p^{r-1}(p-1)(q-1)$$

Finally, by computing $p_i^{r-1} = gcd\left(\frac{e_i d-1}{k_i}, N_i\right)$ we are able to factorize the j prime power moduli $N_i, ..., N_j$. $\square$

Example 4.1. *As an illustration to our attack on j moduli, we consider the following three prime power and three public exponents*

$$\begin{aligned}
N_1 &= 52456104821836006242720492026751134956368083625113730 71\\
N_2 &= 27597044534917989396329522413856367668097828325657469 33\\
N_3 &= 19825618334085902662953177350843279069779090114327269 47\\
e_1 &= 12457815005863813626036165033426745142157353903711616 0\\
e_2 &= 18922250860828721424743709159443326243810745952379342 4\\
e_3 &= 17778256615608588407644691708921479406934634813398463 7
\end{aligned}$$

We have

$$\begin{aligned}
N &= min(N_1, N_2, N_3)\\
&= 1982561833408590266295317735084327906977909011432726947.
\end{aligned}$$

Since $j = 3$ and $r = 3$ with $\gamma = 0.75$, we get $\delta = \frac{j-\gamma j}{(j+1)} = 0.1875$ and $\varepsilon = \frac{1}{4}N^{\delta+\gamma-1} = 0.0001010097596$. Using Theorem 2.3, with $n = j = 3$, we obtain

$$C = [3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1}] = 389046644000000000$$

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

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

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

$$K = \begin{bmatrix} -12119124277 & -132016987081 & -4774584152535 & -3499415255994 \\ 4447894238266 & -14913235108702 & 1040241488030 & 2293089452052 \\ -12344528858943 & 732396467579 & 9015337697435 & -15222622708846 \\ 29920299293636 & 5083100349908 & 58400924463802 & -7079938890808 \end{bmatrix}$$

Next we compute

$$K \cdot M^{-1} = \begin{bmatrix} -12119124277 & -252171353 & -9903953672 & -8026896964 \\ 4447894238266 & 92550540982 & 3634894524297 & 2945987510425 \\ -12344528858943 & -256861508584 & 10088158114994 & -8176189876022 \\ 29920299293636 & 622573230754 & 24451375469342 & 19817204120751 \end{bmatrix}$$

Then from the first row we have $d = 12119124277$, $k_1 = 252171353$, $k_2 = 9903953672$, $k_3 = 8026896964$. Next, by using d and k_i for $i = 1, 2, 3$, define $S_i = \frac{e_i d - 1}{k_i} = \phi(N_i) = p^{r-1}(p-1)(q-1)$

$$S_1 = 524561048218337468229078509366818271387718870441325514 4$$

$$S_2 = 2759704453491660108259154306202060341527530726659055360$$

$$S_3 = 1982561833408482377907837470407359583816783408205533440$$

Then, for $i = 1, 2, 3$ we compute $p_i = \sqrt{gcd\left(\frac{e_i d - 1}{k_i}, N_i\right)}$. That is

$$p_1 = 49244752761499, p_2 = 41738421927617, p_3 = 38281119331291$$

Finally, we can factor the 3 moduli to obtain

$$q_1 = 43925443427429, q_2 = 37953733129141, q_3 = 35340513648257$$

.

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

We consider the scenario when j moduli $N_i = p_i^r q$ for $j \geq 2$ and $r \geq 2$ satisfy j equations $e_i d_i - k\phi(N_i) = 1$ for $i = 1, ..., j$, and the parameters d_i and k, are suitably small.

Theorem 5.1. *For $j \geq 2$ and $r \geq 2$ let $N_i = p_i^r q_i$, $1 \leq i \leq k$ be j moduli with the same size N. Let e_i, $i = 1, ..., j$, be j public exponents with min $e_i = N^\beta$, $0 < \beta < 1$. Let $\delta = \frac{\beta j - \gamma j}{(1+j)}$ where $0 < \gamma \leq \frac{3}{4}$. If there exist an integer $k < N^\delta$ and j integers $d_i < N^\delta$ such that $e_i d_i - k\phi(N_i) = 1$ for $i = 1, ..., j$, then one can factor the j prime power moduli $N_1, ...N_j$ 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 $e_i d_i - k\phi(N_i) = 1$ can be rewritten as

$$\left| \frac{N_i - \nabla}{e_i} k - d_i \right| = \frac{|1 - k(N_i - \phi(N_i)) - \nabla|}{e_i} \tag{2}$$

Let $N = max\ N_i$, and suppose that $k < N^\delta$, $min\ e_i = N^\beta$ and $|(N_i - \phi(N_i) - \nabla)| < 2p_i^{\frac{3r+2}{r+1}} \left| p_i^{\frac{r-1}{r+1}} - q_i^{\frac{r-1}{r+1}} \right|$. Then

$$\begin{aligned}
\frac{|1 - k(N_i - \phi(N_i) - \nabla)|}{e_i} &\leq \frac{|1 + k(N_i - \phi(N_i) - \nabla)|}{N^\beta} \\
&< \frac{1 + N^\delta \left(2p_i^{\frac{3r+2}{r+1}} \left| p_i^{\frac{r-1}{r+1}} - q_i^{\frac{r-1}{r+1}} \right| \right)}{N^\beta} \\
&< \frac{N^\delta(\frac{1}{6}N^\gamma)}{N^\beta} \\
&< \frac{1}{6}N^{\delta+\gamma-\beta}
\end{aligned}$$

Plugging in to (2), to get

$$\left| \frac{N_i - \nabla}{e_i} k - d_i \right| < \frac{1}{6}N^{\delta+\gamma-\beta}$$

To show existence of the integer k and integers d_i, we let $\varepsilon = \frac{1}{6}N^{\delta+\gamma-\beta}$, with $\delta = \frac{\beta j - \gamma j}{(1+j)}$. This will give us

$$N^\delta \varepsilon^j = \left(\frac{1}{6}\right)^j N^{\delta+\delta j+\gamma j-\beta j} = \left(\frac{1}{6}\right)^j$$

Therefore since $\left(\frac{1}{6}\right)^j < 2^{\frac{j(j-3)}{4}} \cdot 3^j$ for $j \geq 2$, we get $N^\delta \varepsilon^j < 2^{\frac{j(j-3)}{4}} \cdot 3^j$. It follows that since $k < N^\delta$ then $k < 2^{\frac{j(j-3)}{4}} \cdot 3^j \cdot \varepsilon^{-j}$. Summarizing for $i = 1, ..., j$, we have

$$\left| \frac{N_i - \nabla}{e_i} k - d_i \right| < \varepsilon, \qquad k < 2^{\frac{j(j-3)}{4}} \cdot 3^j \cdot \varepsilon^{-j}$$

The above satisfies the conditions of Theorem 2.3, and we can obtain k and d_i for $i = 1, ..., j$. Next, from the equation $e_i d_i - k\phi(N_i) = 1$ we get

$$\frac{e_i d_i - 1}{k} = \phi(N_i) = p_i^{r-1}(p_i - 1)(q_i - 1)$$

Finally, by computing $p_i^{r-1} = \left(\frac{e_i d_i - 1}{k}, N_i\right)$ we are ableto factorize the j prime power moduli $N_i, ..., N_j$. $\square$

Example 5.1. *As an illustration to our attack on j moduli, we consider the* *following three prime power and three public exponents*

$$\begin{aligned} N_1 &= 5245610482172832806579932253813295674523806001827944067 \\ N_2 &= 2759704453496559510624258721238207637943024725075445661 \\ N_3 &= 5102916077472569763545373834401695235630054963793474563 \\ e_1 &= 4834972368487260164629839058964789220780346129889309529 \\ e_2 &= 2512166055084287840292458641460881111443081320778523525 \\ e_3 &= 5076479886888939189579571234397642340009946203049043035. \end{aligned}$$

We have

$$\begin{aligned} N &= max(N_1, N_2, N_3) \\ &= 5245610482172832806579932253813295674523806001827944067. \end{aligned}$$

Also $min(e_1, e_2, e_3) = N^{\beta}$ *with* $\beta = 0.97588$ *Since* $j = 3$ *and* $r = 3$ *with* $\gamma = 0.8$, *we get* $\delta = \frac{\beta j - \gamma j}{(1+j)} = 0.1319100000$ *and* $\varepsilon = \frac{1}{6} N^{\delta+\gamma-\beta} = 0.0006543638783$. *Using Theorem 2.3, with* $n = j = 3$, *we obtain*

$$C = [3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1}] = 220890863200000$$

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

$$M = \begin{bmatrix} 1 & -[C(N_1 - \nabla)/e_1] & -[C(N_2 - \nabla)/e_2] & -[C(N_3 - \nabla)/e_3] \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}$$

By applying the LLL algorithm to $\mathcal{L}$, *we obtain reduced basis from following matrix*

$$K = \begin{bmatrix} 2131123 & -882052 & -777312 & -2331090 \\ -31313998762 & -522598890312 & 78379448128 & 142981078460 \\ 613216935162 & -105896263288 & -584161169728 & 795476509540 \\ 2749849277163 & 902212864988 & 4085707904928 & 810178335710 \end{bmatrix}$$

Next we compute

$$K \cdot M^{-1} =$$
$$\begin{bmatrix} 2131123 & 2312121 & 2341115 & 2142221 \\ -31313998762 & -33973522003 & -34399550008 & -31477069011 \\ 613216935162 & 665297945423 & 673640782424 & 616410313276 \\ 2749849277163 & 2983396200296 & 3020807992080 & 2764169345633 \end{bmatrix}$$

Then from the first row we have $k = 2131123$, $d_1 = 2312121$, $d_2 = 2341115$, $d_3 = 2142221$. *Next, by using* d_i *and* k *for* $i = 1, 2, 3$, *define* $S_i = \frac{e_i d_i - 1}{k} = \phi(N_i) = p_i^{r-1}(p_i - 1)(q_i - 1)$

$$S_1 = 524561048217260686459866845548226330340382731272939208 0$$

$$S_2 = 275970445349642067925046058458554043254005954902387760 0$$

$$S_3 = 510291607747235152529456942153153608274062405832132824 8$$

Then for $i = 1, 2, 3$ *we compute* $p_i = \sqrt{gcd\left(\frac{e_i d_i - 1}{k}, N_i\right)}$. *That is*

$$p_1 = 49244752761481, p_2 = 41738421927641, p_3 = 48281119331239$$

Finally, we can factor the 3 moduli to obtain

$$q_1 = 43925443427387, q_2 = 37953733129141, q_3 = 45340513648277$$

.

6. Conclusion

This paper proposes three new attacks on the modulus $N = p^r q$. For the first attack, we used continued fractions expansions and show that $\frac{k}{d}$ can be recovered among the convergents of the continued fraction expansion of $\frac{e}{N - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}}}$. Hence, we can factor the prime power modulus $N = p^r q$ in polynomial time. For $j \geq 2$ and $r \geq 2$, we continued our attacks on j public keys (N_i, e_i) when there exist j relations of the form $e_i d - k_i \phi(N_i) = 1$ or of the form $e_i d_i - k\phi(N_i) = 1$ where the parameters d, d_i, k, k_i, are suitably small in terms of the prime factors of the moduli. We applied LLL algorithm in our approach which enable us to simultaneously factor the j prime power moduli N_i in polynomial time.

References

Asbullah, M. and Ariffin, M. (2015). New attacks on RSA with modulus $N = p^2 q$ using continued fractions. In *Journal of Physics: Conference Series*, volume 622, pages 12–19. IOP Publishing.

Boneh, D. and Durfee, G. (2000). Cryptanalysis of RSA with private key d less than $N^{0.292}$. *IEEE transactions on Information Theory*, 46(4):1339–1349.

De Weger, B. (2002). Cryptanalysis of RSA with small prime difference. *Applicable Algebra in Engineering, Communication and Computing*, 13(1):17–28.

Lenstra, A. K., Lenstra, H. W., and Lovász, L. (1982). Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534.

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

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

Nitaj, A., Ariffin, M. R. K., Nassr, D. I., and Bahig, H. M. (2014). New attacks on the RSA cryptosystem. In *International Conference on Cryptology in Africa*, pages 178–198. Springer.

Nitaj, A. and Rachidi, T. (2015). New Attacks on RSA with Moduli $N = p^r q$. In *International Conference on Codes, Cryptology, and Information Security*, pages 352–360. Springer.

Takagi, T. (1998). Fast RSA-type cryptosystem modulo $p^k q$. In *Advances in Cryptology-CRYPTO'98*, pages 318–326. Springer.

Wiener, M. J. (1990). Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information theory*, 36(3):553–558.