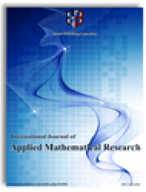
International Journal of Applied Mathematical Research, *5 (4) (2016) 167-175*

International Journal of Applied Mathematical Research

Website: www.sciencepubco.com/index.php/IJAMR
doi: 10.14419/ijamr.v5i4.6494
Research paper



Cryptanalysis on prime power RSA modulus of the form $N = p^r q$

Muhammad Rezal Kamel Ariffin[1*] **and Sadiq Shehu**[2]

[1]*Al-Kindi Cryptography Research Laboratory, Institute for Mathematical Research*
[1]*Department of Mathematics, Faculty of Science, Universiti Putra Malaysia (UPM), Selangor, Malaysia*
[2]*Al-Kindi Cryptography Research Laboratory, Institute for Mathematical Research,Universiti Putra Malaysia, Selangor, Malaysia*
[*]*rezal@upm.edu.my and sadiqshehuzezi@gmail.com*

Abstract

Let $N = p^r q$ be an RSA prime power modulus for $r \geq 2$ and $q < p < 2q$. This paper propose three new attacks. In the first attack we consider the class of public exponents satisfying an equation $eX - NY = up^r + \frac{q^r}{u} + Z$ for suitably small positive integer u. Using continued fraction we show that $\frac{Y}{X}$ can be recovered among the convergents of the continued fraction expansion of $\frac{e}{N}$ and leads to the successful factorization of $N = p^r q$. Moreover we show that the number of such exponents is at least $N^{\frac{r+3}{2(r+1)} - \varepsilon}$ where $\varepsilon \geq 0$ is arbitrarily small for large N. The second and third attacks works when k RSA public keys (N_i, e_i) are such that there exist k relations of the shape $e_i x - N_i y_i = p_i^r u + \frac{q_i^r}{u} + z_i$ or of the shape $e_i x_i - N_i y = p_i^r u + \frac{q_i^r}{u} + z_i$ where the parameters x, x_i, y, y_i, z_i are suitably small in terms of the prime factors of the moduli. We apply the LLL algorithm, and show that our strategy enable us to simultaneously factor the k prime power RSA moduli.

Keywords: *Continued fraction, Diophantine approximations, Factorization, LLL algorithm, RSA prime power, Simultaneous.*

1. Introduction

Invented by Rivest, Shamir and Adleman in 1978, the RSA cryptosystem is most commonly used for providing privacy and ensuring authenticity of digital data. It is one of the most popular and accepted public key cryptosystem systems in use today [14]. In the RSA cryptosystem, the modulus $N = pq$ is a product of two primes of equal bit-size. Let e and d be two positive integers satisfying $ed \equiv 1 \pmod{\phi(N)}$ where $\phi(N) = (p-1)(q-1)$ is Euler's totient function. Commonly, N is called the RSA modulus, e the encryption exponent and d the decryption exponent. The modular equation $ed \equiv 1 \pmod{\phi(N)}$ is sometimes interpreted as the equation $ed - k\phi(N) = 1$, where k is some positive integer and is called the RSA key equation.
In 1990, Wiener showed that RSA is insecure if $d < \frac{1}{3}N^{0.25}$ [17]. Later Boneh and Durfee improved the bound to $d < N^{0.292}$ [1]. Similarly, 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 are based on the RSA key equation

$$ed - k\phi(N) = 1$$

where k is a positive integer. In 2004, Blomer and May [2] combined both Wiener method with Boneh and Durfee method to show that RSA is insecure if the public exponent e satisfies an equation

$$ex - k\phi(N) = y$$

Applying the continued fraction algorithm and Coppersmith's method [14], they showed that the RSA modulus can be factored in polynomial time if the parameters x and y satisfy

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

Additionally, Blomer and May proved that the number of such weak exponents is at least $N^{\frac{3}{4}-\varepsilon}$.
Concurrent to these efforts 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 $ed \equiv 1 \pmod{(p-1)(q-1)}$ [16],. As in the standard RSA cryptosystem, the security of the Prime Power RSA depends on the difficulty of factoring integers of the form $N = p^r q$.

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 $\max N_i$ [5]. Very recently in 2014, with k RSA public keys (N_i, e_i), Nitaj, et al presented a method that factor 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 [9].

Our contribution, in this paper, we propose three new attacks on the Prime Power RSA with a modulus $N = p^r q$, as motivated from the recent result of [9] and [13]. 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 $eX - NY = up^r + \frac{q^r}{u} + Z$ for suitable positive integer u. 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 $N^{\frac{r+3}{2(r+1)} - \varepsilon}$ where $\varepsilon \geq 0$ is arbitrarily small for large N. Hence one can factor the modulus $N = p^r q$ in polynomial time.

The second attack works for $k \geq 2$, $r \geq 2$ moduli $N_i = p_i^r q_i$, $i = 1, ..., k$ when k instances (N_i, e_i) are such that there exit an integer x, k integers y_i, and k integers z_i satisfying $e_i x - N_i y_i = p_i^r u + \frac{q_i^r}{u} + z_i$. We show that the k RSA moduli N_i can be factored in polynomial time if $N = min_i\ N_i$ and $x < N^{\delta}$, $y_i < N^{\delta}$, $|z_i| < \frac{p_i^r u - \frac{q_i^r}{u}}{3(p_i^r u + \frac{q_i^r}{u})} N^{\frac{1}{r+1}}$ where $\delta = \frac{k(1-\alpha r-\alpha)}{(r+1)}$

The third attack works 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 $e_i x_i - N_i y = p_i^r u + \frac{q_i^r}{u} + z_i$. Also we show that the k RSA moduli N_i can be factored in polynomial time if min_i $N = min_i\ N_i$, $e_i = N^{\beta}$ and $x_i < N^{\delta}$, $y < N^{\delta}$, $|z_i| < \frac{p_i^r u - \frac{q_i^r}{u}}{3(p_i^r u + \frac{q_i^r}{u})} N^{\frac{1}{r+1}}$ where $\delta = \frac{\beta k(r+1) - k(r+\alpha r+\alpha)}{(r+1)}$
Both second and third attacks 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 present the first attack and estimation of the number of exponents for which our attack works. In section 4 and 5,we give the second and third attack with numerical example respectively. We conclude this paper in section 6.

2. Preliminaries

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

2.1. Continued fraction

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

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

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 expansion is finite.
Theorem 1. (Legendre). Let a, b, x, y be an integers such that $gcd(a, b) = gcd(x, y) = 1$. Suppose that

$$\left| \frac{a}{b} - \frac{x}{y} \right| < \frac{1}{2y^2}$$

Then $\frac{x}{y}$ is a convergent of the continued fraction expansion of $\frac{a}{b}$.

2.2. Lattice

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

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

is a lattice. The b_i are called basis vectors of $\mathscr{L}$ and $B = b_1, ..., b_m$ is called a lattice basis for $\mathscr{L}$. 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 $dim(\mathscr{L})$, 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 $dim(\mathscr{L}) = n$.[6]
A lattice $\mathscr{L}$ 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 $\mathscr{L}$ is the determinant.

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

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

If $n = m$, we have

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

Theorem 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

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

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 [7] 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). 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 [9] Appendix A.
Lemma 1. Let $N = pq$ be an RSA modulus with $q < p < 2q$. Them

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

Proof. suppose $N = pq$. then multiplying by p we get $pq < p^2 < 2pq$ which implies $N < p^2 < 2N\,N^{\frac{1}{2}} < p < 2^{\frac{1}{2}}N^{\frac{1}{2}}$ Also since $N = pq$, then $q = \frac{N}{p}$ which in turn implies $2^{-\frac{1}{2}}N^{\frac{1}{2}} < q < N^{\frac{1}{2}}$ □

Lemma 2. Let $N = p^r q$ be an RSA modulus prime power with $q < p < 2q$ and u be a suitably small integer. let $\left|up^r - \frac{q^r}{u}\right| < N^{\frac{1}{2}}$. Let S be an approximation of $\left|up^r + \frac{q^r}{u}\right|$ such that $\left|up^r + \frac{q^r}{u} - S\right| < \frac{\left|up^r - \frac{q^r}{u}\right|}{3\left|up^r + \frac{q^r}{u}\right|}N^{\frac{1}{r+1}}$
Then

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

Proof. Let $S = up^r + \frac{q^r}{u} + w$ with $w < \frac{\left|up^r - \frac{q^r}{u}\right|}{3\left|up^r + \frac{q^r}{u}\right|}N^{\frac{1}{r+1}}$

Observe that

$$\begin{aligned}
(up^r - \frac{q^r}{u})^2 &= (up^r - \frac{q^r}{u})(up^r - \frac{q^r}{u}) \\
&= u^2p^{2r} - \frac{p^r q^r u}{u} - \frac{p^r q^r u}{u} + \frac{q^{2r}}{u^2} \\
&= u^2p^{2r} - 2p^r q^r + \frac{q^{2r}}{u^2} \\
&= u^2p^{2r} - 2p^r q^r + 2p^r q^r - 2p^r q^r + \frac{q^{2r}}{u^2} \\
&= u^2p^{2r} + 2p^r q^r + \frac{q^{2r}}{u^2} - 4p^r q^r \\
&= u^2p^{2r} + 2p^r q^r + \frac{q^{2r}}{u^2} - 4p^r q^{r-1} q \\
&= u^2p^{2r} + 2p^r q^r + \frac{q^{2r}}{u^2} - 4Nq^{r-1} \\
&= (up^r + \frac{q^r}{u})^2 - 4Nq^{r-1}
\end{aligned}$$

Hence we obtain

$$(up^r - \frac{q^r}{u})^2 = (up^r + \frac{q^r}{u})^2 - 4Nq^{r-1} \tag{1}$$

Now consider

$$\begin{aligned}
&S^2 - 4Nq^{r-1} \\
&= \left(up^r + \frac{q^r}{u} + w\right)^2 - 4Nq^{r-1} \\
&= \left(up^r + \frac{q^r}{u} + w\right)\left(up^r + \frac{q^r}{u} + w\right) - 4Nq^{r-1} \\
&= u^2p^{2r} + 2p^r q^r + 2up^r w + \frac{2q^r w}{u} + \frac{q^{2r}}{u^2} + w^2 - 4Nq^{r-1} \\
&= u^2p^{2r} + 2p^r q^r + \frac{q^{2r}}{u^2} + 2w\left(up^r + \frac{q^r}{u}\right) + w^2 - 4Nq^{r-1} \\
&= \left(up^r + \frac{q^r}{u}\right)^2 - 4Nq^{r-1} + 2w\left(up^r + \frac{q^r}{u}\right) + w^2
\end{aligned}$$

Hence using (1) we can rewrite the above as

$$S^2 - 4Nq^{r-1} = \left(up^r - \frac{q^r}{u}\right)^2 + 2w\left(up^r + \frac{q^r}{u}\right) + w^2 \tag{2}$$

Suppose that $\left|up^r - \frac{q^r}{u}\right| < N^{\frac{1}{2}}$ and $w < \frac{\left|up^r - \frac{q^r}{u}\right|}{3\left|up^r + \frac{q^r}{u}\right|}N^{\frac{1}{r+1}} < N^{\frac{1}{r+1}}$

Then (2) becomes

$$\begin{aligned}
\left|S^2 - 4Nq^{r-1}\right| &= \left|\left(up^r - \frac{q^r}{u}\right)^2 + 2w\left(up^r + \frac{q^r}{u}\right) + w^2\right| \\
&< (N^{\frac{1}{2}})^2 + 2(up^r + \frac{q^r}{u})\frac{\left|up^r - \frac{q^r}{u}\right|}{3\left(up^r + \frac{q^r}{u}\right)}N^{\frac{1}{r+1}} + (N^{\frac{1}{r+1}})^2 \\
&< N + \frac{2}{3}\left|up^r - \frac{q^r}{u}\right|N^{\frac{1}{r+1}} + N^{\frac{2}{r+1}} \\
&< N + \frac{2}{3}N^{\frac{1}{2}+\frac{1}{r+1}} + N^{\frac{2}{r+1}} \\
&< N + \frac{2}{3}N^{\frac{3+r}{2(r+1)}} + N^{\frac{2}{r+1}} \\
&< 2N
\end{aligned}$$

Therefore it follows that the left hand side of (2) satisfies $\left|S^2 - 4Nq^{r-1}\right| < 2N$, dividing by $4N$, we get

$$\begin{aligned}
\left|\frac{S^2}{4N} - q^{r-1}\right| &= \frac{\left|S^2 - 4Nq^{r-1}\right|}{4N} \\
&= \frac{\left|\left(up^r - \frac{q^r}{u}\right)^2 + 2w\left(up^r + \frac{q^r}{u}\right) + w^2\right|}{4N} \\
&< \frac{2N}{4N} = \frac{1}{2}
\end{aligned}$$

Which implies that

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

□

Lemma 3. Let $N = p^r q$ be an RSA modulus prime power with $q < p < 2q$ and u be a suitably small integer. let S be a positive integer such that

$$\left|up^r + \frac{q^r}{u} - S\right| < \frac{\left|up^r - \frac{q^r}{u}\right|}{3\left|up^r + \frac{q^r}{u}\right|}N^{\frac{1}{r+1}}$$

$\sqrt{S^2 - 4Nq^{r-1}}$ is an approximation of $\left|up^r - \frac{q^r}{u}\right|$
Then

$$\left|\left|up^r - \frac{q^r}{u}\right| - \sqrt{S^2 - 4Nq^{r-1}}\right| < N^{\frac{1}{r+1}}$$

Where $\nabla = S^2 - 4Nq^{r-1}$

Proof. let us consider

$$\left|\left(up^r - \frac{q^r}{u}\right)^2 - \nabla\right|$$
$$= \left|\left(up^r - \frac{q^r}{u}\right)^2 - (S^2 - 4Nq^{r-1})\right|$$
$$\leq \left(up^r - \frac{q^r}{u}\right)\left(up^r - \frac{q^r}{u}\right) - (S^2 - 4Nq^{r-1})$$
$$= u^2p^{2r} - \frac{p^rq^ru}{u} - \frac{p^rq^ru}{u} + \frac{q^{2r}}{u^2} - S^2 + 4Nq^{r-1}$$
$$= u^2p^{2r} - 2p^rq^r + \frac{q^{2r}}{u^2} - S^2 + 4Nq^{r-1}$$
$$= u^2p^{2r} - 2p^rq^r + 4Nq^{r-1} + \frac{q^{2r}}{u^2} - S^2$$
$$= u^2p^{2r} - 2p^rq^r + 4p^rqq^{r-1} + \frac{q^{2r}}{u^2} - S^2$$
$$= u^2p^{2r} - 2p^rq^r + 4p^rq^r + \frac{q^{2r}}{u^2} - S^2$$
$$= u^2p^{2r} + 2p^rq^r + \frac{q^{2r}}{u^2} - S^2$$
$$= \left(up^r + \frac{q^r}{u}\right)^2 - S^2$$

Therefore

$$\left|\left(up^r - \frac{q^r}{u}\right)^2 - \nabla\right| = \left|\left(up^r + \frac{q^r}{u}\right)^2 - S^2\right| \tag{3}$$

Hence we can rewrite the left hand side of (3) as

$$\left|\left(up^r - \frac{q^r}{u}\right)^2 - \nabla\right|$$
$$= \left|\left(up^r - \frac{q^r}{u}\right)^2 - \sqrt{\nabla}\left(up^r - \frac{q^r}{u}\right) + \sqrt{\nabla}\left(up^r - \frac{q^r}{u}\right) - \nabla\right|$$
$$= \left|\left(up^r - \frac{q^r}{u}\right) - \sqrt{\nabla}\right|\left(\left(up^r - \frac{q^r}{u}\right) + \sqrt{\nabla}\right)$$

Which shows that

$$\left|\left(up^r - \frac{q^r}{u}\right) - \sqrt{\nabla}\right| = \frac{\left|\left(up^r - \frac{q^r}{u}\right)^2 - \nabla\right|}{\left(\left(up^r - \frac{q^r}{u}\right) + \sqrt{\nabla}\right)}$$
$$= \frac{\left|\left(up^r + \frac{q^r}{u}\right)^2 - S^2\right|}{\left(\left(up^r - \frac{q^r}{u}\right) + \sqrt{\nabla}\right)}$$
$$\leq \frac{\left|\left(up^r + \frac{q^r}{u}\right)^2 - S^2\right|}{\left|up^r - \frac{q^r}{u}\right|}$$

That is

$$\left|\left(up^r - \frac{q^r}{u}\right) - \sqrt{\nabla}\right| \leq \frac{\left|\left(up^r + \frac{q^r}{u}\right)^2 - S^2\right|}{\left|up^r - \frac{q^r}{u}\right|} \tag{4}$$

Also we rewrite $\left|\left(up^r + \frac{q^r}{u}\right)^2 - S^2\right|$ as

$$\left|\left(up^r + \frac{q^r}{u}\right)^2 - S^2\right|$$
$$= \left|\left(up^r + \frac{q^r}{u}\right)^2 - S\left(up^r + \frac{q^r}{u}\right) + S\left(up^r + \frac{q^r}{u}\right)S^2\right|$$
$$= \left|\left(up^r + \frac{q^r}{u}\right) - S\right|\left(\left(up^r + \frac{q^r}{u}\right) + S\right)$$
$$= \left|up^r + \frac{q^r}{u} - S\right|\left(up^r + \frac{q^r}{u} + S\right)$$

Therefore (4) becomes

$$\left|\left(up^r - \frac{q^r}{u}\right) - \sqrt{\nabla}\right| \leq \frac{\left|up^r + \frac{q^r}{u} - S\right|\left(up^r + \frac{q^r}{u} + S\right)}{\left|up^r - \frac{q^r}{u}\right|} \tag{5}$$

Suppose that

$$\left|up^r + \frac{q^r}{u} - S\right| < \frac{\left|up^r - \frac{q^r}{u}\right|}{3\left|up^r + \frac{q^r}{u}\right|}N^{\frac{1}{r+1}}$$

Then

$$S < up^r + \frac{q^r}{u} + \frac{\left|up^r - \frac{q^r}{u}\right|}{3\left|up^r + \frac{q^r}{u}\right|}N^{\frac{1}{r+1}}$$

And

$$up^r + \frac{q^r}{u} + S < \left(up^r + \frac{q^r}{u}\right) + \left(up^r + \frac{q^r}{u}\right) + \frac{\left|up^r - \frac{q^r}{u}\right|}{3\left|up^r + \frac{q^r}{u}\right|}N^{\frac{1}{r+1}}$$
$$< \left(up^r + \frac{q^r}{u}\right) + \left(up^r + \frac{q^r}{u}\right) + \frac{\left|up^r - \frac{q^r}{u}\right|}{3\left|up^r + \frac{q^r}{u}\right|}N^{\frac{1}{r+1}}$$
$$< \left(up^r + \frac{q^r}{u}\right) + \left(up^r + \frac{q^r}{u}\right) + \frac{\left(up^r + \frac{q^r}{u}\right)}{3\left(up^r + \frac{q^r}{u}\right)}N^{\frac{1}{r+1}}$$
$$< 2\left(up^r + \frac{q^r}{u}\right) + \frac{1}{3}N^{\frac{1}{r+1}}$$
$$< 3\left(up^r + \frac{q^r}{u}\right)$$

Putting back in to (5) we get

$$\left|\left(up^r - \frac{q^r}{u}\right) - \sqrt{\nabla}\right| \leq \frac{\left|up^r + \frac{q^r}{u} - S\right|\left(up^r + \frac{q^r}{u}\right)}{\left|up^r - \frac{q^r}{u}\right|}$$
$$\leq \frac{3\left(up^r + \frac{q^r}{u}\right)\left|up^r - \frac{q^r}{u}\right|}{\left|up^r - \frac{q^r}{u}\right|3\left(up^r + \frac{q^r}{u}\right)}N^{\frac{1}{r+1}}$$
$$< N^{\frac{1}{r+1}}$$

□

3. The First Attack on Prime Power RSA with Moduli $N = p^rq$

In this section, we present a result based on continued fractions and show how to factor the Prime Power RSA modulus N if (N,e) is a public key satisfying an equation $eX - NY = up^r + \frac{q^r}{u} + Z$ with small parameters X, Y and Z where u be a suitably small positive integer.

Lemma 4. Let $N = p^r q$ be an RSA modulus prime power with $q < p < 2q$ and u be a suitably small integer. let e be a public key satisfying the equation

$$eX - NY = up^r + \frac{q^r}{u} + Z$$

with $gcd(X,Y) = 1$, if $X < \frac{N}{3\left(\left(up^r + \frac{q^r}{u}\right)\right.}$ and $Z < \frac{\left|up^r - \frac{q^r}{u}\right|}{3\left(up^r + \frac{q^r}{u}\right)} N^{\frac{1}{r+1}}$

Then $\frac{Y}{X}$ is among the convergent of the continued fraction expansion of $\frac{e}{N}$.

Proof. Assume that $Z < \frac{\left|up^r - \frac{q^r}{u}\right|}{3\left(up^r + \frac{q^r}{u}\right)} N^{\frac{1}{r+1}}$ thus $Z < N^{\frac{1}{r+1}}$ and let $X < \frac{N}{3\left(\left(up^r + \frac{q^r}{u}\right)\right.}$, then from the equation $eX - NY = up^r + \frac{q^r}{u} + Z$ when dividing by NX we get

$$\begin{aligned}
\left|\frac{e}{N} - \frac{Y}{X}\right| &= \frac{|eX - NY|}{NX} \\
&= \frac{\left|up^r + \frac{q^r}{u} + Z\right|}{NX} \\
&\leq \frac{\left|up^r + \frac{q^r}{u}\right| + |Z|}{NX} \\
&\leq \frac{\left|up^r + \frac{q^r}{u}\right|}{NX} + \frac{|Z|}{NX} \\
&\leq \frac{\left|up^r + \frac{q^r}{u}\right| + N^{\frac{1}{r+1}}}{NX}
\end{aligned}$$

If the condition $\frac{\left|up^r + \frac{q^r}{u}\right| + N^{\frac{1}{r+1}}}{NX} < \frac{1}{2X^2}$ hold, which is equivalent to

$$\frac{2X^2 \left|up^r + \frac{q^r}{u}\right| + N^{\frac{1}{r+1}}}{2X\left|up^r + \frac{q^r}{u}\right| + N^{\frac{1}{r+1}}} < \frac{NX}{2X\left|up^r + \frac{q^r}{u}\right| + N^{\frac{1}{r+1}}}$$

Which implies

$$X < \frac{N}{2(up^r + \frac{q^r}{u}) + N^{\frac{1}{r+1}}}$$

Then by theorem (1), we conclude that $\frac{Y}{X}$ is among the convergent of the continued fraction expansion of $\frac{e}{N}$. Hence according to lemma (3) such condition is satisfies if $X < \frac{N}{3(up^r + \frac{q^r}{u})}$. □

Theorem 4. Let $N = p^r q$ be an RSA modulus prime power with $q < p < 2q$. let u be a suitably small integer and suppose that e is a public key exponent satisfying the equation

$$eX - NY = up^r + \frac{q^r}{u} + Z$$

with $gcd(X,Y) = 1$, if $X < \frac{N}{3(up^r + \frac{q^r}{u})}$ and $|Z| < \frac{\left|up^r - \frac{q^r}{u}\right|}{3(up^r + \frac{q^r}{u})} N^{\frac{1}{r+1}}$ then N can be factored in polynomial time.

Proof. suppose that e satisfies the equation

$$eX - NY = up^r + \frac{q^r}{u} + Z$$

with $gcd(X,Y) = 1$, let X and Z satisfy the condition in lemma (4), then $\frac{Y}{X}$ is among the convergent of the continued fraction expansion of $\frac{e}{N}$. Therefore using the value of X and Y, we define $S = eX - NY$ Then S is an approximation of $\left|up^r + \frac{q^r}{u}\right|$ satisfying

$$\left|up^r + \frac{q^r}{u} - S\right| < Z < \frac{\left|up^r - \frac{q^r}{u}\right|}{3(up^r + \frac{q^r}{u})} N^{\frac{1}{r+1}}$$

And by lemma (2) this implies that

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

It follows that $gcd\left(\left\lfloor \frac{S^2}{4N} \right\rfloor, N\right) = q$ □

Algorithm 1

```
Input: an RSA modulus prime power $N = p^r q$,with $q < p < 2q$ and public key $(e,N)$ and Theorem (4).
Output: the prime factors $p$ and $q$.
Compute the continued fraction expansion of $\frac{e}{N}$.
For each convergent $\frac{Y}{X}$ of $\frac{e}{N}$, compute $S = eX - NY$.
    Compute $\left\lfloor \frac{S^2}{4N} \right\rfloor$
    $q = gcd\left(\left\lfloor \frac{S^2}{4N} \right\rfloor, N\right)$
    If $1 < q < N$, then $p^r = \frac{N}{q}$
    End if.
End for.
```

-

Example 1. The following shows an illustration of our attack for $r = 3$, given N and e as

$$N = 32136260228777526617$$

$$e = 24662734946793681455$$

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

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

$$\left[0, 1, \frac{3}{4}, \frac{10}{13}, \frac{33}{43}, \frac{24265}{31618}, \frac{24298}{31661}, \frac{218649}{284906}, \frac{2210788}{2880721}, \frac{4640225}{6046348}, \frac{6851013}{8927069}, \cdots\right]$$

Therefore omitting the first and second entry and try for the next convergent $\frac{33}{43}$, we obtain

$$S = eX - NY = 1015162469924204$$

And

$$\left[\frac{S^2}{4N}\right] = 8017071938$$

We compute $gcd\left(\left[\frac{S^2}{4N}\right], N\right) = (8017071938, 32136260228777526617) = 63313$

Finally with $q = 63313$ we compute $p = \sqrt[3]{\frac{N}{q}} = 79769$, which leads to the factorization of N.

3.1 Estimation of the Number of $e^{\prime s}$ Satisfying $eX - NY = up^r + \frac{q^r}{u} + Z$

We give an estimation of the number of the exponents $e < N$ for which our attacks can be applied. Let u be a suitably small integer. Define α by $\left(up^r + \frac{q^r}{u}\right) = N^{\frac{2}{3}+\alpha}$ with $0 < \alpha < \frac{1}{3}$

Lemma 5. Let $N = p^r q$ be an RSA modulus prime power with $q < p < 2q$. let $\left|up^r - \frac{q^r}{u}\right| < N^{\frac{1}{2}}$ and Suppose that e is a public key exponent satisfying $e < N$ and two equation

$$eX_1 - NY_1 = up^r + \frac{q^r}{u} + Z_1$$

And

$$eX_2 - NY_2 = up^r + \frac{q^r}{u} + Z_2$$

with $gcd(X_i,Y_i)=1$, for $i=1,2$
$1\le Y_i\le X_i<\frac{N}{3(up^r+\frac{q^r}{u})}$ and $|Z_i|<\frac{\left|up^r-\frac{q^r}{u}\right|}{3(up^r+\frac{q^r}{u})}N^{\frac{1}{r+1}}$
Then $X_1=X_2$, $Y_1=Y_2$ and $Z_1=Z_2$.

Proof. Assume that the exponent e satisfying the two equation

$$eX_1-NY_1=up^r+\frac{q^r}{u}+Z_1$$

And

$$eX_2-NY_2=up^r+\frac{q^r}{u}+Z_2$$

with $gcd(X_i,Y_i)=1$, for $i=1,2$
$1\le Y_i\le X_i<\frac{N}{3(up^r+\frac{q^r}{u})}$ and $|Z_i|<\frac{\left|up^r-\frac{q^r}{u}\right|}{3(up^r+\frac{q^r}{u})}N^{\frac{1}{r+1}}$
Then $X_1=X_2$, $Y_1=Y_2$ and $Z_1=Z_2$
Therefore we have

$$e=\frac{up^r+\frac{q^r}{u}+Z_1+NY_1}{X_1}$$

And

$$e=\frac{up^r+\frac{q^r}{u}+Z_2+NY_2}{X_2}$$

Equating e we get

$$X_2(up^r+\frac{q^r}{u}+Z_1+NY_1)=X_1(up^r+\frac{q^r}{u}+Z_2+NY_2)$$

$$(up^r+\frac{q^r}{u})X_2+Z_1X_2+NY_1X_2=(up^r+\frac{q^r}{u})X_1+Z_2X_1+NY_2X_1$$

$$(up^r+\frac{q^r}{u})(X_2-X_1)+Z_1X_2-Z_2X_1=N(Y_2X_1-Y_1X_2) \tag{6}$$

Let $\left|up^r-\frac{q^r}{u}\right|<\left|up^r+\frac{q^r}{u}\right|$ and $\left|up^r+\frac{q^r}{u}\right|>p^r>N^{\frac{r}{r+1}}$. Then the right hand of(6) becomes

$$\begin{aligned}
&\left|(up^r+\frac{q^r}{u})(X_2-X_1)+Z_1X_2-Z_2X_1\right|\\
&\le\left|up^r+\frac{q^r}{u}\right|(|X_2-X_1|)+|Z_1X_2-Z_2X_1|\\
&\le\left|up^r+\frac{q^r}{u}\right|(|X_2|+|X_1|)+|Z_1X_2|+|Z_2X_1|\\
&<\frac{2N(up^r+\frac{q^r}{u})}{3(up^r+\frac{q^r}{u})}+\frac{2(up^r-\frac{q^r}{u})}{9(up^r+\frac{q^r}{u})^2}N^{\frac{r+2}{r+1}}\\
&<\frac{2N}{3}+\frac{2N^{\frac{r+2}{r+1}}}{9N^{\frac{r}{r+1}}}<\frac{2N}{3}+\frac{2}{3}N^{\frac{r+2}{r+1}-\frac{r}{r+1}}\\
&<\frac{2N}{3}+\frac{2}{3}N^{\frac{r+2-r}{r+1}}\\
&<\frac{2N}{3}+\frac{2}{3}N^{\frac{2}{r+1}}\\
&<N
\end{aligned}$$

Therefore from the right hand side of (6) we get $Y_2X_1-Y_1X_2=0$. since the $gcd(X_1,Y_1)=1=gcd(X_2,Y_2)$ which leads to $X_1=X_2$ and $Y_1=Y_2$ and $Z_1=Z_2$. □

Theorem 5. Let $N=p^rq$ be an RSA modulus prime power with $q<p<2q$. let the number of exponents $e<N$ satisfying an equation

$$eX_1-NY_1=up^r+\frac{q^r}{u}+Z_1$$

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

Proof. Suppose that the exponent e satisfying an equation

$$eX-NY=up^r+\frac{q^r}{u}+Z$$

with $gcd(X,Y)=1$ and $X<\frac{N}{3(up^r+\frac{q^r}{u})}$, $|Z|<\frac{\left|up^r-\frac{q^r}{u}\right|}{3(up^r+\frac{q^r}{u})}N^{\frac{1}{r+1}}$
Hence we can express e as $e=\frac{up^r+\frac{q^r}{u}+Z+NY}{X}$ with the conditions given in the theorem bellow

$$\xi=\sum_{Z=1}^{A_1}\sum_{\substack{X=1\\ gcd\left(X,up^r+\frac{q^r}{u}+Z\right)=1}}^{A_2}1 \tag{7}$$

Where $A_1=\left\lfloor\frac{\left|up^r-\frac{q^r}{u}\right|}{3(up^r+\frac{q^r}{u})}N^{\frac{1}{r+1}}\right\rfloor$ and $A_2=\left\lfloor\frac{N}{3(up^r+\frac{q^r}{u})}\right\rfloor$
Using the given identity (See [13]) Let m and n be positive integers then.

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

Where c is a positive constant. Now from the above identity with $m=A_2$ and $n=up^r+\frac{q^r}{u}+Z$ we get

$$\sum_{\substack{X=1\\ gcd(X,up^r+\frac{q^r}{u}+Z)=1}}^{A_2}1>\frac{cA_2}{(\log\log\left|up^r+\frac{q^r}{u}+Z\right|)^2}>\frac{cA_2}{(\log\log N)^2} \tag{8}$$

Where c is a positive constant. Substituting (8) into (7) we get

$$\xi=\frac{c}{(\log\log N)^2}\sum_{Z=1}^{A_1}A_2 \tag{9}$$

Now we have

$$\begin{aligned}
\sum_{Z=1}^{A_1}A_2&=2A_2A_1\\
&>2\left\lfloor\frac{\left|up^r-\frac{q^r}{u}\right|}{3\left|up^r+\frac{q^r}{u}\right|}N^{\frac{1}{r+1}}\right\rfloor\left\lfloor\frac{N}{3(up^r+\frac{q^r}{u})}\right\rfloor\\
&>\frac{2}{3}N^{\frac{1}{r+1}}\times\frac{N}{3(up^r+\frac{q^r}{u})}\\
&>\frac{2}{9(up^r+\frac{q^r}{u})}N^{\frac{r+2}{r+1}}
\end{aligned}$$

Substituting back into (9) we get

$$\begin{aligned}
\xi&>\frac{2c}{9(up^r+\frac{q^r}{u})(\log\log N)^2}N^{\frac{r+2}{r+1}}\\
&>\frac{2c}{9(\log\log N)^2}N^{\frac{r+2}{r+1}-\frac{1}{2}}\\
&>\frac{2c}{9(\log\log N)^2}N^{\frac{2(r+2)-(r+1)}{2(r+1)}}\\
&>\frac{2c}{9(\log\log N)^2}N^{\frac{r+3}{2(r+1)}}\\
&>N^{\frac{r+3}{2(r+1)}-\varepsilon}
\end{aligned}$$

Where we used $\left|up^r+\frac{q^r}{u}\right|>N^{\frac{1}{2}}$ with $\left|up^r-\frac{q^r}{u}\right|<\left|up^r+\frac{q^r}{u}\right|$ and we set $N^{-\varepsilon}=\frac{2c}{9(\log\log N)^2}$, with $\varepsilon>0$ is arbitrarily small for suitably large N. □

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

In this section for $k \geq 2$, $r \geq 2$ moduli $N_i = p_i^r q_i$ with the same size N. We suppose that the prime power RSA moduli satisfying the k equations $e_i x - N_i y_i = p_i^r u + \frac{q_i^r}{u} + z_i$. 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 6. 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, $i = 1, ..., k$, be k public exponents. Define $\delta = \frac{k(1-\alpha r-\alpha)}{r+1}$. Let u, be a suitably small integer such that $p_i^r u + \frac{q_i^r}{u} < N^{\frac{r}{r+1}+\alpha}$. If there exist an integer $x < N^\delta$ and k integers $y_i < N^\delta$ and $|z_i| < \frac{p_i^r u - \frac{q_i^r}{u}}{3(p_i^r u + \frac{q_i^r}{u})} N^{\frac{1}{r+1}}$ such that $e_i x - N_i y_i = p_i^r u + \frac{q_i^r}{u} + z_i$ for $i = 1, ..., k$, then one can factor the k RSA moduli $N_1, ...N_k$ 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 $\left| p_i^r u + \frac{q_i^r}{u} \right| < N^{\frac{r}{r+1}+\alpha}$. Then the equation $e_i x - N_i y_i = p_i^r u + \frac{q_i^r}{u} + z_i$ can be rewrite

$$\left| \frac{e_i}{N_i} x - y_i \right| = \frac{\left| p_i^r u + \frac{q_i^r}{u} + z_i \right|}{N_i} \tag{10}$$

Let $N = min_i\ N_i$, and suppose that $y_i < N^\delta$, $|z_i| < N^{\frac{1}{r+1}}$ and $\left| q_i^r + p_i^r u \right| < N^{\frac{r}{r+1}+\alpha}$. Then

$$\begin{aligned} \frac{\left| p_i^r u + \frac{q_i^r}{u} + z_i \right|}{N_i} &\leq \frac{\left| z_i + p_i^r u + \frac{q_i^r}{u} \right|}{N} \\ &< \frac{N^{\frac{1}{r+1}} + N^{\frac{r}{r+1}+\alpha}}{N} \\ &< \frac{2N^{\frac{r}{r+1}+\alpha}}{N} \\ &< 2N^{\frac{r}{r+1}+\alpha-1} \end{aligned}$$

Substitute in to (10), to get

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

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

$$N^\delta \varepsilon^k = 2^k N^{\delta+\alpha k+\frac{kr}{r+1}-k} = 2^k$$

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 $x < N^\delta$, then $x < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \varepsilon^{-k}$ Summarizing for $i = 1, ..., k$, we have

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

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

Next from the equation $e_i x - N_i y_i = p_i^r u + \frac{q_i^r}{u} + z_i$ we get

$$(e_i x - N_i y_i) - (p_i^r u + \frac{q_i^r}{u}) = z_i$$

Since $|z_i| < N^{\frac{1}{r+1}}$ and $S_i = e_i x - N_i y_i$ is an approximation of $p_i^r u + \frac{q_i^r}{u}$ with an error term of at most $N^{\frac{1}{r+1}}$. Hence using lemma 2, implies that $q_i^{r-1} u = \left[\frac{S_i^2}{4N_i} \right]$ with $S_i = e_i x - N_i y_i$ for $i = 1, ..., k$, we compute $q_i = gcd\left(N_i, \left[\frac{S_i^2}{4N_i} \right] \right)$. Which leads to factorization of k RSA moduli $N_i, ..., N_k$.

□

Example 2. Consider the following three RSA prime power and three public exponents

$N_1 = 396811998723440490898179183106862445436637438710601543$

$e_1 = 280777539730432248989866685726800370419697516012778750$

$N_2 = 1761935453709475892062197083923840534809604834405267667$

$e_2 = 1245774494551468759343140040367253853071721343254285057$

$N_3 = 275806371570006052291797098323622579947913608064631787$

$e_3 = 201231552592489032873517705662876856104469684640666708$

Then

$$\begin{aligned} N &= max(N_1, N_2, N_3) \\ &= 1761935453709475892062197083923840534809604834405267667 \end{aligned}$$

Since $k = 3$ and $r = 3$ with $\alpha < \frac{1}{3}$ we get $\delta = \frac{k(1-\alpha r-\alpha)}{r+1} = 0.25$ and $\varepsilon = 2N^{\frac{r}{r+1}+\alpha-1} = 0.003879095716$. Using equation (11) of Theorem 3 with $n = k = 3$, we obtained.

$$C = [3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1}] = 178868160100$$

Consider the lattice $\mathscr{L}$ 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 $\mathscr{L}$, we obtain the reduced basis with following matrix

$$K = \begin{bmatrix} -4401137 & -4090836 & -4015793 & -922985 \\ -180914422 & 41062584 & 324166242 & -724251010 \\ -663465796 & 704521412 & 51957556 & -199450580 \\ 559311153 & 145935984 & -572548483 & -845009935 \end{bmatrix}$$

Next we compute

$$K \cdot M^{-1} = \begin{bmatrix} -4401137 & -3114171 & -3111819 & -3211121 \\ -180914422 & -128012022 & -127915340 & -131997277 \\ -663465796 & -469457311 & -469102750 & -484072400 \\ 559311153 & 395759226 & 395460326 & 408079955 \end{bmatrix}$$

Then from the first row we obtained $x = 4401137$, $y_1 = 3114171$, $y_2 = 3111819$, $y_3 = 3211121$. Hence using x and y_i for $i = 1, 2, 3$, define $S_i = e_i x - N_i y_i$ we get

$$S_1 = 41641330784512073299977617385100311672897$$

$$S_2 = 128095260343012991955826751291968746653536$$

$$S_3 = 32567304381947595300133101408261464743769$$

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

$$\left[\frac{S_1^2}{4N_1} \right] = 1092457155456172672658538818$$

$$\left[\frac{S_2^2}{4N_2} \right] = 2328177755859188806036633058$$

$$\left[\frac{S_3^2}{4N_3} \right] = 961389423918013737009006002$$

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

$q_1 = 23371533491153, q_2 = 34118746722727, q_3 = 21924751126501$

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

$p_1 = 25701937447111, p_2 = 37239082724141, p_3 = 23257152513583$

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 present an attack on the Prime Power RSA, For $k \geq 2$, and $r \geq 2$, we consider the scenario when the k RSA moduli satisfy k equations of the form $e_i x_i - N_i y = p_i^r u + \frac{q_i^r}{u} + z_i$ for $i = 1, ..., k$, with suitably small unknown parameters x_i y and z_i.

Theorem 7. 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, $i = 1, ...k$, be k public exponents with $min_i\ e_i = N^{\beta}$. Let $\delta = \frac{\beta k(r+1) - k(r + \alpha r + \alpha)}{(r+1)}$. Let u, be a suitably small integer such that $p_i^r u + \frac{q_i^r}{u} < N^{\frac{r}{r+1} + \alpha}$. If there exist an integer $y < N^{\delta}$ and k integers $x_i < N^{\delta}$ such that $e_i x_i - N_i y = p_i^r u + \frac{q_i^r}{u} + z_i$ for $i = 1, ..., k$, then one can factor the k RSA moduli $N_1, ...N_k$ 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 $e_i x_i - N_i y = p_i^r u + \frac{q_i^r}{u} + z_i$ can be rewrite as

$$\left| \frac{N_i}{e_i} y - x_i \right| = \frac{\left| p_i^r u + \frac{q_i^r}{u} + z_i \right|}{e_i} \tag{11}$$

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

$$\begin{aligned} \frac{\left| p_i^r u + \frac{q_i^r}{u} + z_i \right|}{e_i} &\leq \frac{\left| z_i + p_i^r u + \frac{q_i^r}{u} \right|}{N^{\beta}} \\ &< \frac{N^{\frac{1}{r+1}} + N^{\frac{r}{r+1} + \alpha}}{N^{\beta}} \\ &< \frac{2N^{\frac{r}{r+1} + \alpha}}{N^{\beta}} \\ &< 2N^{\frac{r}{r+1} + \alpha - \beta} \end{aligned}$$

Substitute in to (11), to get

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

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

$$N^{\delta} \varepsilon^k = 2^k N^{\delta + \frac{rk}{r+1} + \alpha k - \beta k} = 2^k$$

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 $i = 1, ..., k$, we have

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

Hence it satisfy the conditions of Theorem 3 and we can obtain y and x_i for $i = 1, ..., k$.
Next from the equation $e_i x_i - N_i y = p_i^r u + \frac{q_i^r}{u} + z_i$ we get

$$(e_i x_i - N_i y) - (p_i^r u + \frac{q_i^r}{u}) = z_i$$

Since $|z_i| < N^{\frac{1}{r+1}}$ and $S_i = e_i x_i - N_i y$ is an approximation of $p_i^r u + \frac{q_i^r}{u}$ with an error term of at most $N^{\frac{1}{r+1}}$. Hence using lemma 2, implies that $q_i^{r-1} u = \left[\frac{S_i^2}{4N_i} \right]$ with $S_i = e_i x_i - N_i y$ for $i = 1, ..., k$, we compute $q_i = gcd\left(N_i, \left[\frac{S_i^2}{4N_i} \right] \right)$. Which leads to factorization of k RSA moduli $N_i, ..., N_k$. □

Example 3. Consider the following three RSA prime power and three public exponents

$$\begin{aligned} N_1 &= 3165542718957158938384232970528258463353837742447148 71 \\ e_1 &= 30662975302805379736707040753751257120840979424750164758 \\ N_2 &= 1070522932772407842320618757272826193993836676945090657 \\ e_2 &= 15625738431404765502888647177342514979698505778142537031 1 \\ N_3 &= 1288107615235882059075831083904889457607931668623096287 \\ e_3 &= 35718894214786453506357951535370606505124981687937380988 6 \end{aligned}$$

Then

$$\begin{aligned} N &= max(N_1, N_2, N_3) \\ &= 1288107615235882059075831083904889457607931668623096287 \end{aligned}$$

Also $min(e_1, e_2, e_3) = N^{\beta}$ with $\beta = 0.989144$ Since $k = 3$ and $r = 3$ with $\alpha < \frac{1}{3}$ we get $\delta = \frac{\beta k(r+1) - k(r + \alpha r + \alpha)}{(r+1)} = 0.217432$ and $\varepsilon = 2N^{\frac{r}{r+1} + \alpha - \beta} = 0.0002394886628$. Using equation (11) of Theorem 3, with $n = k = 3$, we obtained.

$$C = [3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1}] = 12311619560000000$$

Consider the lattice $\mathscr{L}$ 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 $\mathscr{L}$, we obtain the reduced basis with following matrix

$$K = \begin{bmatrix} -31124545811 & -23784506307 & -25893307909 & -25594266408 \\ 299409812239 & -599057443457 & 825420120041 & -625605806008 \\ -743267379069 & 3382700381747 & 366761735189 & -2574560326232 \\ -5132867992791 & 893683621433 & 3683419949471 & 1703935452152 \end{bmatrix}$$

Next we compute

$$K \cdot M^{-1} = \begin{bmatrix} -31124545811 & -321319371 & -213234979 & -112242457 \\ 299409812239 & 3091006472 & 2051263508 & 1079742438 \\ -743267379069 & -7673243111 & 5092141904 & -2680397566 \\ -5132867992791 & -52990007465 & -35165396639 & -18510333242 \end{bmatrix}$$

Then from the first row we obtained $y = 31124545811$, $x_1 = 321319371$, $x_2 = 213234979$, $x_3 = 112242457$. Hence using x and y_i for $i = 1, 2, 3$, define $S_i = e_i x_i - N_i y$ we get

$$\begin{aligned} S_1 &= 334051363804872573957480389548451144718 37 \\ S_2 &= 881413864362746300203561065437429887206 42 \\ S_3 &= 103124273676106945098670323757365660026145 \end{aligned}$$

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

$$\begin{aligned} \left[\frac{S_1^2}{4N_1} \right] &= 8812889571164680321912754 42 \\ \left[\frac{S_2^2}{4N_2} \right] &= 1814277808787576652532459442 \\ \left[\frac{S_3^2}{4N_3} \right] &= 2063999873814339973363338482 \end{aligned}$$

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

$q_1 = 20991533497061, q_2 = 30118746726811, q_3 = 32124755826421$

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

$p_1 = 24705937445171, p_2 = 32879082726283, p_3 = 34227152573563$

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

6. Conclusion

Let $N = p^r q$ be an RSA prime power modulus 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 $\frac{e}{N}$. Further more we show that the set of such weak exponents is relatively large, namely that their number is at least $N^{\frac{r+3}{2(r+1)}-\varepsilon}$ 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 $i = 1, ..., k$. The attacks work when k RSA public keys (N_i, e_i) are such that there exist k relations of the shape $e_i x - N_i y_i = p_i^r u + \frac{q_i^r}{u} + z_i$ or of the shape $e_i x_i - N_i y = p_i^r u + \frac{q_i^r}{u} + z_i$ where the parameters x, x_i, y, y_i, z_i are suitably small in terms of the prime factors of the moduli. Using LLL algorithm we show that our approach enable us to simultaneously factor the k Prime Power RSA moduli N_i.

References

[1] Boneh, D., Durfee, G., *Cryptanalysis of RSA with private key d less than* $N^{0.292}$, Advances in Cryptology - Eurocrypt'99, Lecture Notes in Computer Science Vol. 1592, Springer-Verlag, (1999), 1–11.

[2] Blomer, J., May, A., *A generalized Wiener attack on RSA*, In Public Key Cryptography - PKC 2004, volume 2947 of Lecture Notes in Computer Science, Springer-Verlag (2004), 1–13.

[3] Howgrave-Graham, N., Seifert, J. P., *Extending Wieners attack in the presence of many decrypting exponents*, In Secure Networking- CQRE (Secure)'99, LNCS 1740, Springer-Verlag (1999), 153–166.

[4] Hardy, G.H., Wright, E. M., *An Introduction to the Theory of Numbers*, Oxford University Press, London (1975).

[5] Hinek, J., *On the Security of Some Variants of RSA*, Phd. Thesis, Waterloo, Ontario, Canada (2007)

[6] Hinek, M. Jason, *Lattice attacks in cryptography: A partial overview*, School of Computer Science, University of Waterloo, Canada (2004).

[7] Lenstra, A.K. , Lenstra, H.W., L. Lovasz, L., *Factoring polynomials with rational coefficients*, Mathematische Annalen, Vol. 261, (1982), 513–534.

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

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

[10] Nitaj, Abderrahmane, *Diophantine and Lattice Cryptanalysis of the RSA Cryptosystem*. Artificial Intelligence, Evolutionary Computing and Metaheuristics. Springer Berlin Heidelberg, (2013), 139–168.

[11] Nitaj, Abderrahmane, *Cryptanalysis of RSA Using the Ratio of the Primes*, Progress in Cryptology-AFRICACRYPT 2009. Springer Berlin Heidelberg, (2009), 98–115.

[12] Nitaj, Abderrahmane, and Tajjeeddine Rachidi, *New Attacks on RSA with Moduli* $N = p^r q$. Codes, Cryptology, and Information Security. Springer International Publishing, (2015), 352–360.

[13] Nitaj, Abderrahmane, *A New Vulnerable Class of Exponents in RSA*. (2011).

[14] Rivest, R., Shamir, A., Adleman, L., *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM 21.2 (1978), 120–126.

[15] Sarkar, S., *Small secret exponent attack on RSA variant with modulus* $N = p^r q$, Designs, Codes and Cryptography, Volume 73, Issue 2, (2015), 383–392.

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

[17] Wiener, M., *Cryptanalysis of short RSA secret exponents*, IEEE Transactions on Information Theory, Vol. 36, (1990), 553–558.