Caliphate Journal of Science & Technology (CaJoST)

**ISSN:** 2705-313X (**PRINT**); 2705-3121 (**ONLINE**)

Research Article

Open Access Journal available at: https://cajost.com.ng/index.php/files and https://www.ajol.info/index.php/cajost/index

DOI: https://dx.doi.org/10.4314/cajost.v5i1.1

**Article Info**

Received: 24th January 2021

Revised: 15th July 2022

Accepted: 20th July 2022

# Public Key Exponent Attacks on Multi-Prime Power Modulus Using Continued Fraction Expansion Method

Zaid Ibrahim*, Sadiq Shehu and Saidu I. Abubakar

Department of Mathematics, Sokoto State University, Nigeria

***Corresponding author's email:**

malamzaid2@gmail.com

**Cite this:** *CaJoST*, 2023, 1, 1-9

This paper proposes three public key exponent attacks of breaking the security of the prime power modulus $N = p^2q^2$ where $p$ and $q$ are distinct prime numbers of the same bit size. The first approach shows that the RSA prime power modulus $N = p^2q^2$ for $\mathrm{q} < p < 2\mathrm{q}$ using key equation $ed - k\phi(N) = 1$ where $\phi(N) = p^2q^2(p-1)(q-1)$ can be broken by recovering the secret keys $\frac{k}{d}$ from the convergents of the continued fraction expansion of $\frac{\mathrm{e}}{N-2N^{\frac{3}{4}}+N^{\frac{1}{2}}}$. The paper also reports the second and third approaches of factoring $n$ multi-prime power moduli $N_i = p_i^2\, q_i^2$ simultaneously through exploiting generalized system of equations $e_i d - k_i\varphi(N_i) = 1$ and $e_i d_i - k\varphi(N_i) = 1$ respectively. This can be achieved in polynomial time through utilizing Lenstra Lenstra Lovasz (LLL) algorithm and simultaneous Diophantine approximations method for $i = 1, 2, \ldots, n$.

**Keywords:** Public key exponent attacks, Multi-prime power, Factorization, LLL algorithm, Simultaneous Diophantine Approximations, Continued fractions.

## 1. Introduction

The public key cryptosystem invented by Rivest, Shamir and Adleman popularly known as RSA is one of the most popular and accepted cryptosystem in the history of cryptology, (Rivest et al., 1978). It is based on the dramatic difference between the ease of finding large prime numbers and computing modular powers on one hand, and the difficulty of factoring a product of large prime numbers as well as inverting the modular exponentiation on the other hand, (Nitaj, 2009). Other research works that exploited the security of the standard RSA cryptosystem and some of its variants can be found in (B. de Weger, 2002; Maitara & Sarkar, 2008; Chen et al., 2009 ; Nitaj, 2011;Nitaj, 2013; Nitaj et al., 2014). As in the standard RSA cryptosystem, so also the security of the prime power modulus depends on the difficulty of factoring the modulus $N = p^2q^2$ into prime factors $p$ and $q$.

In order to ensure computational efficiency while maintaining the acceptable level of security, many variants of RSA have been proposed. One of such important variants is the multi-prime power modulus. It was first developed by (Takagi, 1998) where he proposed the multi-prime power modulus $N = p^rq$ for $r \geq 2$. He chose an appropriate modulus $N = p^rq$ which resisted two of the fastest factoring algorithms namely: the Number Field Sieve and the Elliptic Curve Methods. Applying the fast decryption algorithm modulo $p^r$, he showed that the decryption process of the proposed cryptosystem is faster than the standard RSA cryptosystem using Chinese Remainder Theorem. Other reported works that attacked Takagi's scheme using different techniques can be found in (Nitaj & Rachidi, 2015; Sarkar, 2015) etc.

However, (Lim et al., 2000) extended the work of Takagi's cryptosystem by using the moduli of the form $N = p^rq^l$ where $r, l \geq 2$. They showed that the choice of either $p^{r+1}q^r$, $p^{r+1}q^{r-1}$or $p^{r+2}q^{r-2}$ gives optimal efficiency under some assumptions that the sum of the exponents are to be fixed. They also claimed that their cryptosystem with modulus $N = p^3q^2$ using 8192-bits is 15-times faster in decryption process than the standard RSA modulus $N = pq$. Another research work on multi-prime power moduli $N = p^rq^l$ was reported by (Lu et al., 2017) where the authors used Coppersmith technique in making the cryptosystem insecure.

Moreover, (May, (2003) considered an RSA-type scheme with modulus $N = p^rq$ for $r \geq 2$ where he presented two attacks using small secret exponent $d$. Both attacks were based on Coppersmith method for solving modular univariate polynomial equations. He also used partial key exposure technique (that is mounting an attack when a fraction of the secret key bits is known to the attacker). Also, (Asbullah et al., 2015) proved that by taking the term $N-(2N^{\frac{2}{3}}-N^{\frac{1}{3}})$ as a good approximation of $\phi(N)$ satisfying key equation $ed-k\phi(N)=1$, one can factor the prime power modulus $N=p^rq$ for $r=2$ in polynomial time.

After thorough review on reported research works on the security of RSA-like modulus of the form$N=p^rq^l$ for $(r,l)\geq 2$, there were only few researches on the scheme and no one applied the concept of continued fraction expansion method to break the security of the moduli $N=p^rq^l$ where $r,l\geq 2$. While in our paper, we develop three approaches that use continued fractions expansion method and lattice basis reduction technique which lead to successful factorization of the multi-prime power moduli $N=p^2q^2$ and its generalized form $N_i=p_i^2\,q_i^2$ for $i=1,2,\dots,n$ in polynomial time without any prior information known to the attacker. In the first approach, the paper shows that given a public exponent $e$ satisfying key equation $ed-k\phi(N)=1$, then $\frac{k}{d}$ can be recovered among the convergents of the continued fractions expansion of $\frac{\mathrm{e}}{N-2N^{\frac{3}{4}}+N^{\frac{1}{4}}}$. The second approach proves that for public key pair $(N_i,e_i)$ and known integer $h_i$ there exist private integer $d$ and $n$ integers $k_i$ satisfying generalized key equation $e_id-k_i\phi_i(N)=1$, where $n$ moduli $N_i$ can be factored in polynomial time provided $N=min\{N_i\}$ for $i=1,2,\dots n,$ and unknown parameters $(d,k_i)<N^{\delta}\ where\ \delta=\frac{n(1-\gamma)}{n+1}$. Our third approach shows that $n$ moduli $N_i$ can also be factored efficiently given public key pair $(N_i,e_i)$ and known integer $h_i$ there exists unknown integer $k$ and $n$ integers $d_i$ satisfying generalized key equation $e_id_i-k\phi_i(N)=1$ where $\min\{e_i\}=N^{\beta}$ and $(d_i,k)<N^{\omega}\ for\ \omega=\frac{n(\beta-\gamma)}{n+1}$.

In both second and third approaches, we transform the system of equations into simultaneous Diophantine approximation problem and apply lattice reduction technique to find the parameters $(d,k_i)$ and $(d_i,k)$ which lead to the factorization of $n$ moduli $N_i$ in polynomial time for $i=1,2,\dots n.$

The rest of the paper is organized as follows. In section 2, we give a brief review of basic terms about continued fractions and theorems related to lattice basis reduction and simultaneous Diophantine approximations. In section 3, we present the findings of this research work. We conclude the paper in section 4.

## 2. Preliminaries

In this section, we give definitions as well as some important theorems concerning continued fraction, lattice basis reduction technique and simultaneous Diophantine approximation method.
**Definition 2.1**(Continued Fraction). A continued fraction of a real number $\mathbb{R}$ is an expression of the form

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

where$a_0\in\mathbb{Z}$ is an integer. The numbers$\{a_0,a_1,a_2,a_3\}$ are called the partial quotients. It can be denoted by$R=\{a_0,a_1,a_2,a_3\}$. For $i\geq 1$, the rational $\frac{r_i}{s_i}=\{a_0,a_1,a_2,a_3\}$ are called the convergents of the continued fraction expansion of $\mathbb{R}$. If $\mathbb{R}=\frac{r}{s}$ is a rational number such that the $\gcd(r,s)=1$, then the continued fraction is finite (Nitaj, 2013).

**Theorem 2.2.** *(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 among the convergents of the continued fraction expansion of $x$ (Nitaj, 2013).

**Theorem 2.3.** *Let L be a lattice of dimension $\tau$ with a basis $v_1,\dots,v_\tau$. The LLL algorithm produces a reduced basis $b_1,\dots,b_\omega$ satisfying*

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

*for all* $1\leq i\leq\tau$ *and* $L$ *is the lattice (*Lenstra et al., 1982).

**Theorem 2.4.** (Simultaneous Diophantine Approximations). There is a polynomial time algorithm, for given rational numbers $\beta_1,\dots,\beta_n$and $0<\varepsilon<1$, to compute integers $p_1,\dots,p_n$ and a positive integer $q$ such that

$$\max|q\beta_i-p_i|<\varepsilon\ and\ q\leq 2^{\frac{n(n-3)}{4}}$$

Proof. See Appendix A in (Nitaj, 2011).

## 3. Results

This section discusses the major findings of this research work into three approaches. The first part presents cryptanalysis attack of factoring prime power moduli $N=p^2q^2$ using continued fractions method through approximation of $\phi(N)$, and the remaining two parts present two instances of factoring $n$ multi-prime power moduli $N_i = p_i^2 q_i^2$ for $i = 1,\ 2, \ldots,\ n$ through exploiting two generalized key equations.

### 3.1 First Attack on Prime Power Modulus $N = p^2q^2$

This section presents first approach which is based on continued fraction expansion method that shows how to factor the multi-prime power modulus $N = p^2q^2$ by exploiting the security of the modulus through key equation $ed - k\varphi(N) = 1$ where $\varphi(N),\ d \, and\ \ k$ are unknown parameters and $(N, e)$ are public key pair using approximation of $\varphi(N) = N - (2N^{\frac{3}{4}} - N^{\frac{1}{2}})$.

**Lemma 3.1**. *Let* $N = p^2q^2$ be a prime power modulus where $p$ and $q$ are distinct positive prime numbers of same bit size such that $q < p < 2q$. *If* $q^2 < p^2 < 2q^2$, *then*

$$2^{-1/4}N^{1/4} < q < N^{1/4} < p < 2^{1/4}N^{1/4}$$

*and*

$$\varphi(N) = N - (2N^{\frac{3}{4}} - N^{\frac{1}{2}})$$

Proof. Since $N = p^2q^2$ where $q < p < 2q$ and suppose $q^2 < p^2 < 2q^2$. Then multiplying the inequality by $p^2$ we get $p^2q^2 < p^4 < 2p^2q^2$ which implies $N < p^4 < 2N$ , that is $N^{\frac{1}{4}} < p < 2^{1/4}N^{1/4}$. Since $N = p^2q^2$ is the modulus, then $q^2 = \frac{N}{p^2}$ which implies $2^{-1/4}N^{\frac{1}{4}} < q < N^{1/4}$. Hence,

$$2^{-1/4}N^{1/4} < q < N^{1/4} < p < 2^{1/4}N^{1/4}.$$

By definition of $\varphi(N)$, we can write

$\varphi(N) = p^{2-1}q^{2-1}(p-1)(q-1)$ and compute the approximation of $\varphi(N)$as follows:

$$\begin{aligned}\varphi(N) &= p^{2-1}q^{2-1}(pq - p - q + 1)\\ &= p^2q^2 - p^2q - pq^2 + pq\\ &= N - (p^2q + pq^2 - pq)\\ &= N + pq - (p^2q + pq^2)\end{aligned}$$

From the above, we can obtain the following result and gives an interval for $N - \phi(N) = (p^2q + pq^2)$ in terms of $N$. Taking $p \approx q \approx N^{\frac{1}{4}}$ gives

$$\begin{aligned}&N - \left(\left(N^{\frac{1}{4}}\right)^2 N^{\frac{1}{4}} + N^{\frac{1}{4}}\left(N^{\frac{1}{4}}\right)^2 - N^{\frac{1}{4}}N^{\frac{1}{4}}\right)\\ &\quad = N - \left(N^{\frac{2}{4}}N^{\frac{1}{4}} + N^{\frac{1}{4}}N^{\frac{2}{4}} - N^{\frac{1}{2}}\right)\\ &\quad = N - \left(N^{\frac{3}{4}} + N^{\frac{3}{4}} - N^{\frac{1}{2}}\right)\\ &\quad = N - \left(2N^{\frac{3}{4}} - N^{\frac{1}{2}}\right)\end{aligned}$$

This is a good approximation of $\varphi(N)$ because it output the correct convergents $\frac{k}{d}$

**Theorem 3.2.** Let $N = p^2q^2$ be multi-prime power modulus where $p$ and $q$ are positive prime numbers such that $q < p < 2q$ and $q^2 < p^2 < 2q^2$ and known integer $h_2$. Let $1 < e < \varphi(N) < N - \left(2N^{\frac{3}{4}} - N^{\frac{1}{2}}\right)$ satisfies an equation $ed - k\varphi(N) = 1$ for some private integers $\varphi(N),\ d \, and\ \ k.$ If $d < \frac{1}{2}\left(N - 2N^{\frac{3}{4}} + N^{\frac{1}{2}}\right)$, then

$$\left|\frac{e}{N - 2N^{\frac{3}{4}} + N^{\frac{1}{2}}} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

*Proof.* From equation $ed - k\varphi(N) = 1$, we can rewrite it as:

$$\begin{aligned}ed - k(p^{2-1}q^{2-1}(p-1)(q-1)) &= 1\\ ed - k\big(pq(pq - p - q + 1)\big) &= 1\\ ed - k(p^2q^2 - p^2q - pq^2 + pq) &= 1\\ ed - k\big(N - (p^2q + pq^2 - pq)\big) &= 1\\ ed - k\big(N + pq - (p^2q + pq^2)\big) &= 1\\ ed - k(N - \big(N - \phi(N)\big) &= 1.\end{aligned}$$

Since $N - \phi(N) = p^2q + pq^2 - pq$, then

$$ed - k\left(N - 2N^{\frac{3}{4}} + N^{\frac{1}{2}}\right) = 1$$

Dividing by $d\left(N - 2N^{\frac{3}{4}} + N^{\frac{1}{2}}\right)$ and taking the absolute value gives

$$\left|\frac{e}{N - 2N^{\frac{3}{4}} + N^{\frac{1}{2}}} - \frac{k}{d}\right| = \left|\frac{1}{d\left(N - 2N^{\frac{3}{4}} + N^{\frac{1}{2}}\right)}\right| < \frac{1}{2d^2}.$$

Therefore, since

$$\frac{1}{d\left(N - 2N^{\frac{3}{4}} + N^{\frac{1}{2}}\right)} < \frac{1}{2d^2}$$

then

$$d < \frac{1}{2}\left(N - 2N^{\frac{3}{4}} + N^{\frac{1}{2}}\right).$$

Hence $\frac{k}{d}$ is among the convergrnts of the continued fraction expansion of $\frac{e}{N - 2N^{\frac{3}{4}} + N^{\frac{1}{2}}}$.

**Corollary 3.3.** Assume that the Theorem 3.2 revealed the secret exponent $d$, then the multi-prime power modulus $N = p^2q^2$ can be factored in polynomial time

Proof. Observe that from Theorem 3.2, and equation $ed - k\varphi(N) = 1$ we get a relation

$\frac{ed-1}{k} = \phi(N) = p^2q^2(p-1)(q-1)$.Hence, computing the $\gcd\left(N, \frac{ed-1}{k}\right) = pq$ can lead to the factorization of the multi-prime power modulus $N = p^2q^2$.

**Algorithm 1**

**Input:**$N = p^2q^2$ as modulus such that $q < p < 2q$ and $q^2 < p^2 < 2q^2$, public key $(e, N)$ and a known integer $h_2 = (p-1)(q-1)$ satisfying Theorem 3.2.

**Output:** The prime factors $p$ and $q$.

1: Compute the continued fraction expansion of $\frac{e}{N-2N^{\frac{3}{4}}+N^{\frac{1}{2}}}$

2: For each convergent $\frac{k}{d}$ of $\frac{e}{N-2N^{\frac{3}{4}}+N^{\frac{1}{2}}}$, compute $\varphi(N) = \frac{ed-1}{k}$

3: Compute $h_1 = \gcd\left(N, \frac{ed-1}{k}\right)$ and

4: Compute $h_3 = h_1 - h_2 + 1$

5. Solve quadratic equation $x^2 - h_3x + h_1 = 0$

6. Return prime factors $(p,\ q)$

**Example 3.1.** As an example to illustrate our attack for $N = p^2q^2$, Let the public keys$(e, N)$ be as follows:

$$N = 401874364437987855692007131194778093102301722124035041$$

$$e = 14330350374582654596582701324634687776221266623000385$$

Also, let the known integer be

$$h_2 = 6339356153726647320684587 52$$

Taking the continued fraction expansion of $\frac{e}{N-2N^{\frac{3}{4}}+N^{\frac{1}{2}}}$ gives the following convergents by applying Algorithm 1

$$\left[0; \frac{1}{2}; \frac{5}{14}; \frac{41}{115}; \frac{46}{129}; \frac{2065}{5791}; \frac{4176}{11711}; \frac{10417}{29213}; \frac{243767}{683610}; \frac{497951}{1396433}; \frac{2733522}{7665775}\right]$$

Applying the Algorithm 1 with the convergent $\frac{k}{d} = \frac{2733522}{7665775}$, we obtain $\frac{ed-1}{k} = 40187436443795348652807168644280702217784448102825139 2$.

Hence, using Algorithm 1 we get the following:

$$h_1 = 6339356153727189476119650 71$$

$$h_3 = 54215543506320.$$

Finally, solving $x^2 - h_3x + h_1 = 0$, leads to the factorization of $N$ efficiently and yield the prime factors as follows $p = 37152455623183$ and $q = 17063087883137$.

### 3.2 Second Attack on n Multi-prime Power Moduli $N_i = p_i^2q_i^2$

Let $N_i = p_i^2q_i^2$ be n multi-prime power moduli for $i = 1,2,\dots,n$. The attack works upon $n$ instances of public key pair $(e_i, N_i)$ and unknown integers $d, k_i$ satisfying $e_id - k_i\phi(N) = 1$.

**Theorem 3.3** Let $N_i = p_i^2q_i^2$ be $n$ multi-prime power moduli where $p$ and $q$are distinct positive prime numbers of the same bit-size. Let $(e_i, N_i)$ be $n$ public exponents, $h_{2i,} = (p_i - 1)(q_i - 1)$ be a known positive integer and $N = \max\{N_i\}$, such that $1 < e_i < \phi(N_i) < N_i - \xi$ where $\xi = 2N^{\frac{3}{4}} + N^{\frac{1}{2}}$. If there exists integer $d < N^{\delta}$ and $n$ integers $k_i < N^{\delta}$ such that $e_Id - k_I\phi(N_I) = 1$ holds for $i = 1, \dots n$, then one can factor $n$ prime power moduli $N_1, \dots, N_n$ in polynomial time where $\delta = \frac{n(1-\gamma)}{n+1}$ and $0 < \gamma < \frac{3}{4}$.

Proof. Since the modulus $N_i = p_i^2q_i^2, for\ 1 \le i \le n$ and $N = \max\{N_i\}$, if $k_i < N^{\delta}$ then we can rewrite $e_id - k_i\phi(N_i) = 1$ as follows:

$$e_id - k_i(N_i - (N_i - \phi(N_i))) = 1$$

$$e_id - k_i\big(N_i - \xi + \xi - (N_i - \phi(N_i)\big) = 1$$

$$e_id - k_i(N_i - \xi) = 1 + k_i(N_i - \phi(N_i) - \xi)$$

$$\left|\frac{e_i}{N_i - \xi}d - k_i\right| = \frac{\left|1 + k_i\big(\xi - N_i - \phi(N_i)\big)\right|}{N_i - \xi} \quad (1)$$

Suppose that $N = \max\{N_1,\ N_2,\ N_3\}$, $k_i < N^{\delta}$and $1 < e_I < \phi(N_I) < N_i - \xi < \frac{3}{4}N$, then taking the absolute value of the inequalities gives

$$\frac{\left|1 + k_i\big(\xi - N_i - \phi(N_i)\big)\right|}{N_i - \xi} = \frac{\left|1 + k_i\left(4N^{\frac{3}{4}} + 2N^{\frac{1}{2}}\right)\right|}{N_i - \xi}$$

$$< \frac{1 + N^{\delta}\left(\frac{1}{2}N^{\gamma}\right)}{\frac{3}{4}N} < \frac{2}{3}N^{\delta+\gamma-1}.$$

Equation (1) becomes

$$\left|\frac{e_i}{N_i - \xi}d - k_i\right| < \frac{2}{3}N^{\delta+\gamma-1}.$$

Hence, to show the existence of integer $d$, we define $\epsilon = \frac{2}{3}N^{\delta+\gamma-1}$ where $\delta = \frac{n(1-\gamma)}{n+1}$, then

$$N^{\delta}\epsilon^n = (\tfrac{2}{3})^nN^{\delta+\delta n+\gamma n-n} = (\tfrac{2}{3})^n.$$

For $\left(\frac{2}{3}\right)^n < 2^{\frac{n(n-3)}{4}} \times 3^n$ with $n \ge 2$, we get $N^{\delta}\epsilon^n < 2^{\frac{n(n-3)}{4}} \times 3^n$. It follows that if $d < N^{\delta}$, then

$d < 2^{\frac{n(n-3)}{4}} \times 3^n \times \epsilon^{-n}$. Summarizing for $i = 1, \dots, n$, we have

$$\left|\frac{e_i}{N_i-\xi}d - k_i\right| < \epsilon,\ d < 2^{\frac{n(n-3)}{4}} \times 3^n \times \epsilon^{-n}$$

Hence, this satisfied Theorem 2.8, we can obtain d and $k_i$ for $i = 1, \dots, n$.

Next from $e_i d - k_i \phi(N_i) = 1$ we get

$$\frac{e_i d - 1}{k_i} = \phi(N_i) = p_i^2 q_i^2 (p_i - 1)(q_i - 1) = J_i$$

$$h_{1i} = \gcd(N_i, J_i)$$

$$h_{3I} = h_{1i} - h_{2i} + 1.$$

Therefore, by finding the roots of the equation $x^2 + h_{3i}x + h_{1i} = 0$,the prime factors $p_i$ and $q_i$ can be revealed, which leads to the factorization of the n moduli $N_i, \dots, N_n$.This completes the proof.

**Algorithm 2**

```
Initialization: The public key $(e_i, N_i)$ satisfying Theorem 3.4.
Choose $\gamma, \delta, N = \max\{N_m\}$ where $0 < \gamma, \delta < 1$
For **any** $(\gamma, \delta, N)$**do**
    $\epsilon = \frac{2}{3} N^{\delta+\gamma-1}$
    $C = 2^{\frac{(n+1)(n-4)}{4}} \times 3^{n+1} \times \epsilon^{-n-1}$
**end for**
Consider the lattice $L$ spanned by the matrix $M$ as stated above
Applying the $LLL$ algorithm to $L$ yields the reduced basis matrix $K$,
For **any**$(M, K)$**do**
    Compute $U := M^{-1}$ and $W = U K$
**end for**
Produce $d, k_i$ from $W$
For **each**$(d, k_i, e_i)$ **do**
    $J_i = \frac{e_i d - 1}{k_i}$ for $i = 1, \dots, n$
    Compute $h_{1i} = \gcd(N_i, J_i)$
    Compute $h_{3I} = h_{1i} - h_{2i} + 1$
**end for**
Solve quadratic equation $x^2 + h_{3i}x + h_{1i} = 0$
    Return prime factors $(p_i, q_i)$.
```

**Example 3.2.** As an illustration to our attack on n moduli we consider the following three prime power and their three public exponents respectively.

$$N_1 = 117195790933145924077611992188529827447399655012644846432609$$
$$N_2 = 54208925846394398923442489853432606247191350107623867506569$$
$$N_3 = 70396116810398900802458798657807287144507078495664229622489$$
$$e_1 = 34125362325331459683339353041340550043768596833924700401017$$
$$e_2 = 41923966193053456521870291921339512335922518116793291416 97$$
$$e_3 = 23103727061250185647267144188662944497535641508429048858105$$

Given the following

$$h_{21} = 3423387079094987611834738570 08$$
$$h_{22} = 23282810364385536143544080 2728$$
$$h_{23} = 26532266546678262005322410 9568.$$

Then

$$N = max(N_1, N_2, N_3) = 117195790933145924077611992188529827447399655012644846432609$$

$n = 3\ with\ \epsilon = 0.77$ we get $\delta = \frac{n(1-\gamma)}{n+1} = 0.1725000000$ and $\epsilon = \frac{2}{3} N^{\delta+\gamma-1} = 0.0002675754719.$

Using Theorem 2.5, we obtain $C = 2^{\frac{(n+1)(n-4)}{4}} \times 3^{n+1} \times \epsilon^{-n-1} = 7900777350000000.$

Consider the lattice $L$ spanned by the matrix

$$H = \begin{bmatrix} 1 & -[Ce_1\backslash N_1 - \xi] & -[Ce_2\backslash N_2 - \xi] & -[Ce_3\backslash N_3 - \xi] \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}$$

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

$$K = \begin{bmatrix} -72884895817 & -36311686582 & 82928249801 & 128963933610 \\ -259346487775 & 62995137350 & -23319035425 & -23319035425 \\ -273572463545 & 1319884261930 & -777609404615 & 752521859850 \\ -1020027489801 & -3058158417846 & -3486963901047 & 748365276330 \end{bmatrix}$$

Next, we compute and obtain

$$W = \begin{bmatrix} -72884895817 & -21222805512 & -5636754207 & -23920534486 \\ -259346487775 & -75517156313 & -20057275100 & -85116491354 \\ -273572463545 & 79659511373 & -21157480127 & -89785400326 \\ -1020027489801 & -297014145253 & -78886635975 & -334768987085 \end{bmatrix}$$

Then, from the first row of $W$, we obtain $d = 72884895817, k_1 = 21222805512$

$k_2 = 5636754207, k_3 = 23920534486$. Hence, using $d\ and\ k_i$ for $i = 1,2,3$, we compute and obtain $\frac{e_i d-1}{k_i} = \phi(N_i) = p_i^2 q_i^2 (p_i - 1)(q_i - 1) = J_i, h_{1i}, h_{3i}$ as follows:

$$J_1 = 1171957909331455168740522243671159023509949305281499504678 24$$

$$J_2 = 542089258463941265783891472185706946453217778123844682846 64$$

$$J_3 = 703961168103985717383762691128445925742655516592168823229 44$$

$$h_{11} = 342338707909499950659131618353$$

$$h_{12} = 232828103643856531161298980163$$

$$h_{13} = 265322665466783860294354472933$$

$$h_{31} = 1189475657761346,\ h_{32} = 1169725858177436, h_{33} = 1240241130363366$$

Finally, we solve quadratic equation $x^2 + h_{3i}x + h_{1i} = 0$, for $i = 1, 2, 3$ which produces prime factors as follows:

$p_1 = 701388554111197$, $p_2 = 915372448132237$, $p_3 = 965412977340517$

$q_1 = 488087103650149$, $q_2 = 254353410045199$, $q_3 = 274828153022849$.

This leads to the factorization of the three moduli $N_1, N_2$ and $N_3$ in polynomial time.

### 3.3 Third Attack on n Multi-prime Power Moduli $N_i = p_i^2 q_i^2$

In this section, the attack works upon $n$ instances of public key pair $(e_i, N_i)$ satisfying generalized key equation $e_i d_i - k\phi(N_i) = 1$ where $d_i$ and $k$ are private exponents.

**Theorem 3.4** Let $N_i = p_i^2 q_i^2$ be $n$ prime-power moduli where $p$ and $q$ are positive prime numbers having same bit size. Let $e_i$ be $n$ public exponents with $e_i = N^\beta$ and $N = \max\{N_i\}\ for\ 0 < \beta < 1$. Also, define $\delta = \frac{n(\beta-\gamma)}{n+1}$ where $0 < \gamma < \frac{4}{5}$ and let $h_{2i} = (p_i - 1)(q_i - 1)$ be a known positive integers. If there exists unknown positive integers $(k, d_i) < N^\beta$ such that generalized key equation $e_i d_i - k\phi(N_i) = 1$ holds for $i = 1, \ldots n$, then one can factor $n$ prime power moduli $N_1, \ldots, N_i$ efficiently.

Proof. Since $N_i = p_i^2 q_i^2$ is defined to be $n$ prime power moduli for $1 \le i \le n$. The generalized key equation $e_i d_i - k\phi(N_i) = 1$ can be rewritten as :

$$\left|\frac{N_i - \xi}{e_i} k - d_i\right| = \frac{|1 + k(N_i - \phi(N_i) - \xi)|}{e_i} \qquad (2)$$

Also,suppose $N = \max\{N_i\}, k < N^\delta$ and $\min\{e_i\} = N^\beta$, then

$$\begin{aligned} \frac{|1 + k(N_i - \phi(N_i) - \xi)|}{e_i} & \\ &\le \frac{\left|1 + k\left(2N^{\frac{3}{4}} + N^{\frac{1}{2}} + 2N^{\frac{3}{4}} + N^{\frac{1}{2}}\right)\right|}{N^\beta} \\ &< \frac{1 + N^\delta\left(4N^{\frac{3}{4}} + 2N^{\frac{1}{2}}\right)}{N^\beta} < \frac{N^\delta(N^\gamma)}{2N^\beta} \\ &= \frac{1}{2}N^{\delta+\gamma-\beta}. \end{aligned}$$

Using equation (2), we get

$$\left|\frac{N_i - \xi}{e_i} k - d_i\right| < \frac{1}{2}N^{\delta+\gamma-\beta}$$

For the existence of unknown integers $(k, d_i)$, we define $\epsilon = \frac{1}{2}N^{\delta+\gamma-\beta}$ where $\delta = \frac{n(\beta-\gamma)}{n+1}$. Then we have

$N^\delta \epsilon^n = (\frac{1}{2})^n N^{\delta+\delta n+\gamma n-\beta n} = (\frac{1}{2})^n$.

Therefore, since $(\frac{1}{2})^n < 2^{\frac{n(n-3)}{4}} \times 3^n$ with $n \ge 3$, this implies $N^\delta \epsilon^n < 2^{\frac{n(n-3)}{4}} \times 3^n$ . This means that if $k < N^\delta$, then $k < 2^{\frac{n(n-3)}{4}} \times 3^n \times \epsilon^{-n}$ . This can be expressed as

$$\left|\frac{N_i - \xi}{e_i} k - d_i\right| < \epsilon,$$

where

$$k < 2^{\frac{n(n-3)}{4}} \times 3^n \times \epsilon^{-n}.$$

This clearly satisfied the condition stated in Theorem 2.5. We can now proceed to get the values of the unknown integers $(k, d_i)$ for $i = 1, \ldots, n$.

Next, the generalized key equation

$e_i d_i - k\phi(N_i) = 1$ can be transformed into:

$$\frac{e_i d_i - 1}{k} = \phi(N_i) = p_i^2 q_i^2 (p_i - 1)(q_i - 1).$$

Define:

$$\phi(N_i) = p_i^2 q_i^2 (p_i - 1)(q_i - 1) = J_i$$

$$h_{1i} = \gcd(N_i, J_i)$$

$$h_{3i} = h_{1i} - h_{2i} + 1.$$

Therefore, by finding the roots of $x^2 + h_{3i} + h_{1i} = 0,$ the prime factors $p_i$ and $q_i$ can be revealed, which gives us the factorization of n moduli $N_i, \dots, N_n$. This completes the proof.

**Algorithm 3**

```
Initialization: The public key $(e_i, N_i)$ satisfying Theorem 3.5.
Choose $\beta, \delta, \gamma, n,\ N = \max\{N_i\}$.
For **any** $(\beta, \delta, \gamma, n)$**do**
    $\epsilon = \frac{1}{2} N^{\delta+\gamma-\beta}$
    $C = 2^{\frac{(n+1)(n-4)}{4}} \times 3^{n+1} \times \epsilon^{-n-1}$ and $\min\{e_i\} = N^{\beta}$
**end for**
Consider the lattice $L$ spanned by the matrix $M$ as stated above
Applying the $LLL$ algorithm to $L$ yields a reduced basis matrix $K$,
For **any** $(M, K)$ **do**
    $U := M^{-1}$ and $W = U\,K$
**end for**
Produce $d, k_i$ from $W$
For **each** $(d_i, k\ e_i)$**do**
    $J_i = \frac{e_i d_i - 1}{k}$ for $i = 1, \dots, n$
    Compute $h_{1i} = \gcd(N_i, J_i)$
    Compute $h_{3i} = h_{1i} - h_{2i} + 1$
**end for**
Solve quadratic equation $x^2 + h_{3i}x + h_{1i} = 0$
Return prime factors $(p_i, q_i)$.
```

**Example 3.3.** As an illustration to our attack on n moduli we consider the following three prime power and their three public exponents respectively.

$$N_1 = 26048169474897051240907555909545384413836907662308449985361$$

$$N_2 = 79134611595042159627505966238399749635918131231343088985281$$

$$N_3 = 7141803987706703616947890057608651680148301956679551197641$$

$$e_1 = 237557590973185839355214053213437043755615353155002384956012$$

$$e_2 = 114400220158080621575534857129798178495256349984154945123021$$

$$e_3 = 13825507983913742154055901045058762001562763547392904159251.$$

Given the following positive integers

$$h_{21} = 161394453048723946268170122900$$

$$h_{22} = 281308747811086607628494352384$$

$$h_{23} = 84509194693279231352042173084$$

$N = 79134611595042159627505966238399749635918131231343088985281$ and $\min\{e_1, e_2, e_3\} = N^{\beta}$ where $\beta = 0.9988.$ For $n = 3, \gamma = 0.77588$ we get $\delta = \frac{n(\beta-\gamma)}{n+1} = 0.16719000000$ and $\epsilon = \frac{1}{2} N^{\delta+\gamma-\beta} = 0.0002609540495.$

Using Theorem 2.5, for $n = 3$ we compute $C = 2^{\frac{(n+1)(n-4)}{4}} \times 3^{n+1} \times \epsilon^{-n-1} = 8733711880000000.$

Consider the lattice $L$ spanned by the matrix

$$H = \begin{bmatrix} 1 & -[C(N_1 - \xi)\backslash e_1] & -[C(N_2 - \xi)\backslash e_2] & -[C(N_3 - \xi)\backslash e_3] \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}$$

Therefore, applying the LLL algorithm to $L$, we obtain reduced basis as displayed in the following matrix

$$K = \begin{bmatrix} -9141389923 & 9987187262 & 13563035431 & 93841112069 \\ 804271850683 & -188319638702 & 918335722849 & -29092570349 \\ -741807964732 & 641685617192 & 1106864222604 & -117511832604 \\ 559622713724 & -3609265876056 & -1466732116428 & 627075886428 \end{bmatrix}$$

Next, we compute and obtain

$$W = \begin{bmatrix} -9141389923 & -1002352621 & -6323417385 & -4722142223 \\ 804271850683 & 88188339445 & 556342815011 & 415460460266 \\ 741807964732 & -81339179708 & -513134372347 & -383193665419 \\ 559622713724 & 61362582561 & 387110497070 & 289082739899 \end{bmatrix}$$

Then, from the first row of $W$, we obtain $k = 9141389923,\ d_1 = 1002352621$

$d_2 = 6323417385, d_3 = 4722142223$ . Hence, using the values for $(k, d_i)$ for $i = 1,2,3$, we compute $J_i = \frac{e_i d_i - 1}{k} = \phi(N_i) = p_i^2 q_i^2 (p_i - 1)(q_i - 1) = J_i, h_{1i}, h_{3i}$ as follows:

$$J_1 = 26048169474896904777593497720720964505665659121754242210100$$
$$J_2 = 79134611595041841943136113421431285273732562509515201490944$$
$$J_3 = 71418039877066391072926056418895200827424017685356636658 36$$

$$h_{11} = 16139445304872485375483581 3769$$

$$h_{12} = 28130874781108773693702927 9841$$

$$h_{13} = 84509194693279994696853569629$$

$$h_{31} = 907486665690870,\ h_{32} = 1169725858177436, h_{33} = 1240241130363366$$

Finally, we solve quadratic equation $x^2 + h_{3i}x + h_{1i} = 0$, for $i = 1, 2, 3$ which produces prime factors of the moduli as follows:

$p_1 = 664666444554319, p_2 = 758369764917889, p_3 = 628987246697003$

$q_1 = 242820221136551, q_2 = 370938770009569, q_3 = 134357564699543.$

This leads to the factorization of the three moduli $N_1, N_2, N_3$ efficiently.

## 4. Conclusion

This paper proposed three new approaches for the factorization of the multi prime power modulus $N = p^2 q^2$. In the first approach, we applied continued fraction to prove that private exponents $\frac{k}{d}$ can be recovered among the convergent of the continued fraction expansion of $\frac{e}{N - 2N^{\frac{3}{4}} + N^{\frac{1}{2}}}$ which led to the factorization of prime power modulus N $N = p^2 q^2$ efficiently. The second and third approaches used public key pairs $(e_i, N_i)$ in the construction of two generalized key equations $e_i d - k_i \phi(N_i) = 1$ and $e_i d_i - k\phi(N_i) = 1$ such that unknown parameters $d, d_i, k, k_i$ and $\phi(N_i)$can be recovered simultaneously through simultaneous Diophantine approximation and LLL algorithm which led to factorization of $n$ prime power moduli $N_i$ for $i = 1, 2, 3$ in polynomial time.

## Conflict of Interest

The author declares that there is no conflict of interest.

## Acknowledgements

The authors wish to acknowledge the reviewers for their constructive and insightful criticisms which improved the quality of the article. Also, the authors appreciate the efforts of the Editors for their timely correspondence and useful suggestions.

## References

[1] Asbullah, M. A., and Ariffin, M. R. K (2015). New Attacks on RSA with Modulus $N = p^2 q$ Using Continued Fractions. Journal of Physics, Conference Series, 622(1), ***DOI***:10.1088/1742-6596/***622***/***1***/ 012019.

[2] Bonne de Weger (2002). Cryptanalysis of RSA with Small Prime Difference. *Applicable Algebra in Engineering Communication and Computing* 13(1), DOI:10.1007/s00200010088.

[3] C. Chen, C. Hsueh and Y. Lin (2009). A Generalization of de Weger's Method. 2*009 Fifth International Conference on Information Assurance and Security*, 344-347, doi: 10.1109/IAS.2009.153.

[4] Lenstra, A.K. , Lenstra, H.W., L. Lovasz, L (1982). Factoring polynomials with rational coefficients. *Mathematische Annalles*, 261, 513-534. http://eudml.org/doc/182903.

[5] Lim, S., Kim, S., Yie, I and Lee, H (2000). A Generalized Takagi-Cryptosystem with a Modulus of the Form $p^r q^s$ , International Conference on Cryptology , 283-294. https://doi.org/10.1007/3-540-44495-5_25.

[6] Lu, Y., Liqiang P., and Sarkar S (2017). Cryptanalysis of an RSA variant with moduli $N = p^r q^s$. *Journal of Mathematical Cryptology*,

11(2), 117-130, DOI: 10.1515/jmc-2016-0025.

[7] Maitra, S. and Sarkar, S (2008). Revisiting Wiener's attack- New Weak keys in RSA. In International Conference on Information Security, https://doi.org/10.1007/978-3-540-85886-7_16 .

[8] May, A (2004). New RSA Vulnerabilities Using Lattice Reduction Method. PhD. thesis, University of Paderborn.

[9] Nitaj, Abderrahmane (2009). Cryptanalysis of RSA Using the Ratio of the Primes. *Progress in Cryptology-AFRICACRYPT 2009*, 98-115, *https://doi.org/10.1007/978-3-642-02384-2_7.*

[10] Nitaj, Abderrahmane (2011). A New Vulnerable Class of Exponents in RSA. *JP Journal of Algebra, Number Theory and Applications* 21(2), 203-220, Online ISSN: 0972-5555.

[11] Nitaj, Abderrahmane (2013). Diophantine and Lattice Cryptanalysis of the RSA Cryptosystem. *Artificial Intelligence, Evolutionary Computing and Metaheuristics*, 427, 139-168, https://doi.org/10.1007/978-3-642-29694-9_7.

[12] Nitaj, A., Ariffin, M. R. K., Nassr, D. I., and Bahig, H. M (2014). New Attacks on the RSA Cryptosystem. Progress in Cryptology-AFRICACRYPT 2014, 178-198, https://doi.org/10.1007/978-3-319-06734-6_12

[13] Nitaj, Abderrahmane and Tajjeeddine Rachidi (2015). New Attacks on RSA with Moduli $N = p^r q$. *Codes, Cryptology, and Information Security*, 9084, 352-360, https://doi.org/10.1007/978-3-319-18681-8_28.

[14] Rivest, R., Shamir, A., Adleman, L, A (1978). Method for obtaining digital signatures and public-key cryptosystem. *Communications of the ACM*, 21(2), 120-126, https://doi.org/10.1145/359340.359342.

[15] Sarkar, S (2015). Small secret exponent attack on RSA variant with modulus $N = p^r q$. *Designs, Codes and Cryptography*, 73(2), 383-392, https://doi.org/10.1007/s10623-014-9928-6.

[16] Takagi, T (1998). Fast RSA-type cryptosystem modulo $p^k q$. In Advances in Cryptology-Crypto'98, 318-326, https://doi.org/10.1007/BFb0055738.

[17] Wiener, M (1990). Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, 36(3), 553-558, doi: 10.1109/18.54902.