International Journal of Cryptology Research 9(2): 1 - 25 (2019)

Factorization of Prime Power Moduli $N = p^r q^s$ Using Continued Fractions Method

Saidu Isah Abubakar *1 and **Sadiq Shehu**2

1,2*Department of Mathematics, Sokoto State University, Nigeria*

E-mail: siabubakar82@gmail.com, sadiqshehuzezi@gmail.com
**Corresponding author*

ABSTRACT

This paper proposes a new cryptanalysis attack of factoring prime power moduli $N = p^r q^s$ for $r, s \geq 2$ and $r > s$ by applying continued fractions method to find decryption exponent d from the convergents of the continued fractions expansion of $\frac{e}{N - N^{\frac{r+s-1}{2r}}\left(2^{-\frac{s-1}{2r}} + 2^{-\frac{s}{2r}}\right) + 2^{-\frac{s-1}{2r}} N^{\frac{r+s-2}{2r}}}$. The paper shows that if

$$d < \frac{1}{2}\left(N - N^{\frac{r+s-1}{2r}}\left(2^{-\frac{s-1}{2r}} + 2^{-\frac{s}{2r}}\right) + 2^{-\frac{s-1}{2r}} N^{\frac{r+s-2}{2r}}\right),$$

then prime factors p and q of the moduli $N = p^r q^s$ can be found in polynomial time. The paper also proposes two new attacks that lead to the simultaneous factorization of t prime power moduli $N_j = p_j^r q_j^s$ using generalized system of equation of the form $e_j d - k_j \phi(N_j) = 1$ and $e_j d_j - k\phi(N_j) = 1$ by applying simultaneous Diophantine approximations and LLL algorithm techniques.

Keywords: Continued Fractions, Factorization, Prime, Power, Moduli, LLL algorithm, Diophantine, Simultaneous, Approximations, etc

1 INTRODUCTION

The RSA cryptosystem invented by great mathematicians (Rivest, Shamir and Adleman) is considered to be one of the most practical public key cryptosystem in today's digital economy due to its numerous applications in web browsing, e-commerce, e-banking, digital signature and smart cards, Rivest and Adleman (1978).

The security of the cryptosystem is based on the integer factorization problem. Many researches are being conducted and reported to have break the security of the cryptosystem making it vulnerable to attacks using various techniques which include continued fractions method as reported by Wiener (1990), de Weger (2002), Maitra and Sarkar (2008), Chen C.Y. Hsueh and Lin (2009), Nitaj et al. (2014), Bunder and Tonien (2017), Abubakar et al. (2018), Ariffin et al. (2019), etc, Coppersimth's technique based on Lattice construction method as reported by Boneh and Durfee (1999), Blömer and May (2004), Hinek (2008),Sarkar (2016), among others.

Many variants of RSA cryptosystem have been proposed in order to achieve high efficiency in the decryption process. These variants include multi prime RSA of the form $N = p_1p_2, p_3, \dots, p_n$, as reported by Collins et al. (1998), Takagi scheme with moduli $N = p^rq$ as presented by Takagi (1998), also known as prime power RSA for $r \geq 2$, generalization of the Takagi cryptosystem with moduli $N = p^rq^s$ for $r, s \geq 2$ and $\gcd(r, s) = 1$ proposed by Lim et al. (2000). Many attacks related to the factoring problem of multi prime with modulus $N = p_1p_2, p_3, \dots, p_n$ were reported by Herrmann and May (2007), Hinek (2008), Santoso et al. (2008), Zhang and Takagi (2013), Zheng et al. (2017). Cryptanalysis attacks for factoring Takagi scheme with moduli $N = p^rq$ is being reported by Nitaj et al. (2014), Ariffin and Shehu (2016),Sarkar (2016), etc.

As for the RSA-like scheme with moduli $N = p^rq^s$ for $r, s \geq 2$ and $\gcd(r, s) = 1$, Lim et al. (2000) was the first to have reported the factoring of the moduli in polynomial time using Takagi's method except that the decryption process is faster than that of Takagi. In their research work, Lim et al. reported that the moduli $N = p^rq^s$ is faster than the Takagi's cryptosystem which is faster than the standard RSA scheme, Lim et al. (2000). In their experiment, Lim et al. proved that for a moduli $N = p^3q^2$, the decryption process is 15-times faster than the standard RSA modulus of the same bit size, Lim et al. (2000). Moreover, the security of the cryptosystem with the moduli $N = p^r q^s$ also relies on the hardness of factoring a very large composite integer into its two distinct prime factors.

Since then, very little research works have been reported on the security of the prime power moduli $N = p^r q^s$. Coron et al. (2016) showed that the polynomial time algorithm of $N = p^r q^s$ only requires the condition $r = \omega(\log_2^3 \max\{p, q\})$, under which a constant number of bits need to be given and thus can be obtained through exhaustive search, Coron et al. (2016). Also Lu et al. (2017) proposed that one can factor the moduli $N = p^r q^s$ in polynomial time if $\min\{\frac{r}{r+s}, \frac{2|r-s|}{r+s}\}$-fraction of the least significant bits (LSBs) of one of the prime factors p, q is known and have same bit size, for $r, s \geq 2$ and $\gcd(r, s) = 1$ Lu et al. (2017). Later, Coron et al. (2018) revisited their work and improve it by obtaining a weaker condition of $r = \omega(\log_2 q)$ as the required number of bits that need to be known for the attack to be mounted successfully, Coron and Zeitoun (2018). In order to improve the works of Lu et al. (2017), Coron et al. (2016), Coron and Zeitoun (2018), Wang et al. (2019), proposed a better lattice construction attack on the moduli $N = p^r q^s$ where they showed that the polynomial time factorization of the prime power moduli $N = p^r q^s$ requires a condition of $\varsigma > \alpha\beta(su - ru) \log_2 N$ by selecting u, v such that $su - rv = 1$ is satisfied which is sufficient to recover p and q. They further proved that, for the polynomial-time factorization of $N = p^r q^s$, one only need to know more than $\alpha\beta \log_2 N$ LSBs of p, Wang et al. (2019). All the above mentioned attacks on the prime power moduli $N = p^r q^s$ are based on the Coppersmith's method and their lattice construction look similar and use $\gcd(r, s) = 1$. The only difference among them depends on the choice of non-negative integers u, v.

In this paper, we propose a continued fractions method that can lead to the factorization of the prime power moduli $N = p^r q^s$ in polynomial time for $r, s \geq 2$ and $r > s$ by making good approximations of $\phi(N)$. In our approach, we show that if $q^s < p^r < 2q^r$ and $p \approx N^{\frac{1}{2r}}$ and $q \approx 2^{-\frac{1}{2r}} N^{\frac{1}{2r}}$, then our approach enables us to get approximation of $\phi(N) = N - N^{\frac{r+s-1}{2r}}(2^{-\frac{s-1}{2r}} + 2^{-\frac{s}{2r}}) + 2^{-\frac{s-1}{2r}} N^{\frac{r+s-2}{2r}}$ which can be used further in getting the right candidate

$\frac{k}{d}$ as decryption keys from the convergents of the continued fractions expansion of $\frac{e}{N-N^{\frac{r+s-1}{2r}}\left(2^{-\frac{s-1}{2r}}+2^{-\frac{s}{2r}}\right)+2^{-\frac{s-1}{2r}}N^{\frac{r+s-2}{2r}}}$ that leads to the factorization of the moduli N into prime factors p and q in polynomial time where p and q are considered to be balanced primes and $r, s \geq 2$, $r > s$. We further give numerical experiment in order to justify the efficiency of our work.

Lastly, the paper reports generalization of system of equations of the form $e_jd - k_j\phi(N_j) = 1$ and $e_jd_j - k\phi(N_j) = 1$ where $j = 1, 2 \ldots t$. Here, the paper proposes two instances that lead to the factorization of t prime power moduli $N_j = p_j^r q_j^s$ in polynomial time. The first instance shows that if $d, k_j < N^{\omega}$ where $\omega = \frac{1-\eta t}{3t+1}$,$0 < \eta < 1$ and satisfying $e_jd - k_j\phi(N_j) = 1$, then t prime factors p_j and q_j can be found simultaneously through utilization of simultaneous Diophantine approximations and LLL algorithm techniques. Likewise, the second instance proves that if $d_j, k < N^{\omega}$ where $\omega = \frac{(\sigma-\eta)t}{3t+1}$,$0 < \omega, \eta < \sigma < 1$ and the relation $e_jd_j - k\phi(N_j) = 1$ holds, then it is sufficient enough to factor t moduli $N_j = p_j^r q_j^s$ in polynomial time by utilizing similar technique as adopted in the first instance. The paper also gives numerical results to justify how the proposed attacks work.

The rest of the paper is organized as follows. In Section 2, we present definitions of some basic terms and theorems that could be used in this paper . In Section 3 , we present our major findings which contain proofs of lemma and theorems. We also give some numerical results/examples where necessary to illustrate how our theorems work and finally in Section 4, we conclude the paper.

2 PRELIMINARIES

In this section, we give basic definitions of some terms and state theorems that could be used in this paper.

Definition 2.1 (Continued fraction)**.** *The continued fraction of a real number*

x is an expression of the form

$$x = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}}$$

This expression is often used in the form $x = [a_0, a_1, a_2, \dots]$. Any rational number $\frac{a}{b}$ can be expressed as a finite continued fraction $x = [a_0, a_1, a_2, \dots, a_m]$. For $i \geq 0$, we define the i^{th} convergent of the continued fraction $[a_0, a_1, a_2, \dots]$ to be $[a_0, a_1, a_2, \dots, a_i]$. Each convergent is a rational number.

Theorem 2.1. *If $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \dots, \frac{p_k}{q_k}, \dots$ are convergents of the simple continued fraction $[a_1, a_2, \dots, a_k, \dots]$, then the numerators and denominators of these convergents satisfy the following recursive relations:*

$$p_1 = a_1,\ p_2 = a_2 a_1 + 1, p_k = a_k p_{k-1} + p_{k-2},$$

$$q_1 = 1,\ q_2 = a2,\ q_k = a_k q_{k-1} + q_{k-2},$$

for $k \geq 3$, Wang et al. (2016).

Theorem 2.2. *Let α be an arbitrary real number. If the rational number $\frac{p}{q}$ satisfies*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{2q^2},$$

then $\frac{p}{q}$ must be a convergent of α.

Definition 2.2. *Let $\vec{b_1}, \dots, \vec{b_m} \in \mathcal{R}^n$. The vectors $b_i's$ are said to be linearly dependent if there exist $x_1, \dots x_m \in R$, which are not all zero and such that*

$$\sum_{i}^{m} (x_i b_i = 0).$$

Otherwise, they are said to be linearly independent.

Definition 2.3. *(Lenstra et-al., 1982): Let n be a positive integer. A subset $\mathcal{L}$ of an n-dimensional real vector space $\mathcal{R}^n$ is called a lattice if there exists a basis $b_1 \cdots b_n$ on $\mathcal{R}^n$ such that $\mathcal{L} = \sum_{i=1}^{n} \mathcal{Z} b_i = \sum_{i=1}^{n} r_i b_i\ for\ r_i \in \mathcal{Z}, 1 \leq i \leq n$. In this situation, we say that $b_1, \dots b_n$ are basis for $\mathcal{L}$ or that they span $\mathcal{L}$, Lenstra and Lovsz (1982).*

Definition 2.4. *(LLL Reduction, Nitaj (2013)) Let $\mathcal{B} = \langle b_1 \cdots b_n \rangle$ be a basis for a lattice $\mathcal{L}$ and let $B^* = \langle b_1^*, \ldots, b_n^* \rangle$ be the associated Gram- Schmidt orthogonal basis. Let*

$$\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} for 1 \leq j < i.$$

The basis $\mathcal{B}$ is said to be LLL reduce if it satisfies the following two conditions:

1. $\mu_{i,j} \leq \frac{1}{2}, \quad for \quad 1 \leq j < i \leq n$
2. $\frac{3}{4}||b_{i-1}^*||^2 \leq ||b_i^* + \mu_{i,i-1} b_{i-1}^*||^2 \quad for \quad 1 \leq i \leq n$*. Equivalently, it can be written as*
$$||b_i^*||^2 \geq (\frac{3}{4} - \mu_{i,i-1}^2)||b_{i-1}^*||^2.$$

Theorem 2.3. *Let $\mathcal{L}$ be a lattice basis of dimension n having a basis $v_1 \cdots v_n$. The LLL algorithm produces a reduced basis $b_1, \ldots, b_n$ satisfying the following condition*

$$||b_1|| \leq ||b_2|| \leq \cdots \leq ||b_j|| \leq 2^{\frac{n(n-1)}{4(n+1-j)}} det(\mathcal{L})^{\frac{1}{n+1-j}}$$

for all $1 \leq j \leq n$, Lenstra and Lovsz (1982).

Theorem 2.4. *(Simultaneous Diophantine Approximations) Nitaj et al. (2014). Given any rational numbers of the form $\alpha_1, \ldots, \alpha_n$ and $0 < \varepsilon < 1$, there is a polynomial time algorithm to compute integers $p_1, \ldots, p_n$ and a positive integer q such that*

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

3 MAJOR FINDINGS AND RESULTS DISCUSSION

This section presents the major findings of the paper and discusses the modalities/methodologies adopted in achieving the desired results.

Lemma 3.1. *Let $N = p^r q^s$ be prime power moduli where p and q have the same bit size for $r, s \geq 2$, and $r > s$. If $q^s < p^r < 2q^s$, then*

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

and approximation of $\phi(N)$ is

$$\phi(N) = N - N^{\frac{r+s-1}{2r}}(2^{-\frac{s-1}{2r}} + 2^{-\frac{s}{2r}}) + 2^{-\frac{s-1}{2r}} N^{\frac{r+s-2}{2r}}.$$

Proof. Since $N = p^r q^s$ for $r, s \geq 2$, and $r > s$. Suppose $q^s < p^r < 2q^s$, then multiplying by p^r gives $p^r q^s < p^{2r} < 2p^r q^s$ which implies $N < p^{2r} < 2N$, that is $N^{\frac{1}{2r}} < p < 2^{\frac{1}{2r}} N^{\frac{1}{2r}}$. Also, since $N = p^r q^s$, then $q^s = \frac{N}{p^r}$ which in turn implies $2^{-\frac{1}{2s}} N^{\frac{1}{2s}} < q < N^{\frac{1}{2s}}$. Since p and q have same bit size, we can write $q \approx p \approx N^{\frac{1}{2r}}$, hence

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

Also, taking $N = p^r q^s$ and $\phi(N) = p^{r-1} q^{s-1}(p-1)(q-1)$ for $r, s \geq 2$, $r > s$. We compute the approximation of $\phi(N)$ as follows:

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

Taking $p \approx N^{\frac{1}{2r}}$ and $q \approx 2^{-\frac{1}{2r}} N^{\frac{1}{2r}}$ give the following result:

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

This completes the proof. □

Theorem 3.1. *Let $N = p^r q^s$ be prime power moduli, where p and q are prime numbers with same bit size and $q^s < p^r < 2q^s$ for $r, s \geq 2$, and $r > s$. Also, Let (e, N, M) and $(d, p, q, \phi(N))$ be public and private key* *tuples respectively satisfying* $ed \equiv 1 \pmod{\phi(N)}$ *where* $1 < e < \phi(N)$ *and* $M = p^{r-2}q^{s-2}(p-1)(q-1)$. *If* $p \approx N^{\frac{1}{2r}}$ *and* $q \approx 2^{-\frac{1}{2r}}N^{\frac{1}{2r}}$*, then* $d < \frac{1}{2}\left(N - N^{\frac{r+s-1}{2r}}(2^{-(\frac{s-1}{2r})} + 2^{-\frac{s}{2r}}) + 2^{-\frac{s-1}{2r}}N^{\frac{r+s-2}{2r}}\right)$ *can be found from the convergents of the continued fractions expansion of* $\frac{e}{N-N^{\frac{r+s-1}{2r}}\left(2^{-(\frac{s-1}{2r})}+2^{-\frac{s}{2r}}\right)+2^{-\frac{s-1}{2r}}N^{\frac{r+s-2}{2r}}}$ *which lead to the factorization of the moduli* N *into prime factors* p *and* q *in polynomial time.*

Proof. From Lemma 3.1, it was shown that $2^{-\frac{1}{2r}}N^{\frac{1}{2r}} < q < N^{\frac{1}{2r}} < p$ where $q \approx 2^{-\frac{1}{2r}}N^{\frac{1}{2r}}$ and $p \approx N^{\frac{1}{2r}}$. Equation $ed - k\phi(N) = 1$ for $k \in \mathcal{Z}$ can be rewritten as

$$\begin{aligned}
ed - k(p^{r-1}q^{s-1}(p-1)(q-1)) &= 1\\
ed - k(p^r q^s - (p^r q^{s-1} + p^{r-1}q^s) + p^{r-1}q^{s-1}) &= 1\\
ed - k(N - (p^r q^{s-1} + p^{r-1}q^s) + p^{r-1}q^{s-1}) &= 1\\
ed - k\left(N - (2^{-\frac{s-1}{2r}}N^{\frac{r+s-1}{2r}} + 2^{-\frac{s}{2r}}N^{\frac{r+s-1}{2r}}) + 2^{-\frac{s-1}{2r}}N^{\frac{r+s-2}{2r}}\right) &= 1\\
ed - k\left(N - N^{\frac{r+s-1}{2r}}(2^{-\frac{s-1}{2r}} + 2^{-\frac{s}{2r}}) + 2^{-\frac{s-1}{2r}}N^{\frac{r+s-2}{2r}}\right) &= 1.
\end{aligned}$$

Dividing both sides by $d\left(N - N^{\frac{r+s-1}{2r}}(2^{-\frac{s-1}{2r}} + 2^{-\frac{s}{2r}}) + 2^{-\frac{s-1}{2r}}N^{\frac{r+s-2}{2r}}\right)$ yields

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

Applying Theorem 2.2, we have

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

Hence,

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

Then $\frac{k}{d}$ is among the convergents of the continued fractions expansion of $\frac{e}{N-N^{\frac{r+s-1}{2r}}(2^{-(\frac{s-1}{2r})}+2^{-\frac{s}{2r}})+2^{-\frac{s-1}{2r}}N^{\frac{r+s-2}{2r}}}$. Also, from $ed - k\phi(N) = 1$, we have $\phi(N) = \frac{ed-1}{k}$. Next, we find the $\gcd(\phi(N), N) = W$ and compute $p^{r-2} = \gcd(M, W)$. From $N = p^r q^s$, q can be computed by taking the sth-root of $\frac{N}{p^r}$. This completes the proof. □

Algorithm 1 Theorem 3.1

```
Initialization: The public keys $(N, e, M)$ satisfying Theorem 3.1.
Choose $r$, $s$, to be suitable small positive integers where $r, s \geq 2$ and $r > s$.
for any $(r, s)$ do
    The convergents $\frac{k}{d}$ of the continued fractions expansion of $\frac{e}{N - N^{\frac{r+s-1}{2r}}\left(2^{-(\frac{s-1}{2r})} + 2^{-\frac{s}{2r}}\right) + 2^{-\frac{s-1}{2r}} N^{\frac{r+s-2}{2r}}}$.
end for
Compute $\phi(N) := \frac{ed-1}{k}$
Compute $W := \gcd(\phi(N), N)$
Compute $p^{r-2} := \gcd(M, W)$
Compute $q^s := \frac{N}{p^r}$
return prime factors $p$ and $q$.
```

Example 3.1. *In what follows, we give an illustration of how Theorem 3.1 works in factoring $N = p^3q^2$.*
Let

$$\begin{aligned} N &= 26491842129862567523966736379427945138090 63 \\ e &= 404987857411793368699537524195878794 79 \\ M &= 2860291665319113523129473 6 \end{aligned}$$

Taking $r = 3$, $s = 2$ and the continued fractions expansion of $\frac{e}{N - N^{\frac{r+s-1}{2r}}\left(2^{-(\frac{s-1}{2r})} + 2^{-\frac{s}{2r}}\right) + 2^{-\frac{s-1}{2r}} N^{\frac{r+s-2}{2r}}}$ gives the following:

$$[0, 65413, 1, 11, 16, 14, 2, 3, 1, 1, 1, 1, 16, 1, 2, 1, 1, 5, 1, 5, 1, 3,$$

$$1, 3, 3, 1, 2, 1, 5, 21, 1, 3, 2, 1, 121, 1, 3, 2, 2, 1, 1, 34, 1, 6, 1, 1, 4, 1,$$

$$2, 2, 16, 2, 1, 1, 1, 5, 2, 1, 3, 1, 5, 65, 2, 4, 14, 2, 1, 6, 15, 1, \cdots]$$

which produces the convergent $\frac{k}{d} = \frac{12}{784967}$. Next, using Algorithm 1, we compute the following:

$$\begin{aligned}
\phi(N) &= \frac{ed-1}{k} \\
&= 2649184195574693377066415597962219915916016 \\
W &= \gcd(\phi(N), N) \\
&= 28602916841181648257245273 \\
p &= \gcd(M, W) \\
&= 308822183 \\
q &= \sqrt{\frac{N}{p^3}} \\
&= 299911657.
\end{aligned}$$

Finally, prime factors p and q of the prime power moduli $N = p^3q^2$ are found in polynomial time.

3.1 System of Equation Using $N - N^{\frac{r+s-1}{2r}}\left(2^{-(\frac{s-1}{2r})} + 2^{-\frac{s}{2r}}\right) + 2^{-\frac{s-1}{2r}}N^{\frac{r+s-2}{2r}}$ as Approximation of $\phi(N)$

In this section, we present two instances of factoring t prime power moduli $N_j = p_j^r q_j^s$ using system of equation of the form $e_jd - k_j\phi(N_j) = 1$ and $e_jd_j - k\phi(N_j) = 1$ for $j = 1, \ldots, t$, $r, s \geq 2$ and $r > s$ which lead to the successful factorization of t prime power moduli $N_j = p_j^r q_j^s$ in polynomial time.

3.1.1 The Attack on t Prime Power Moduli $N_j = p_jq_j$ Satisfying System of Equation $e_jd - k_j\phi(N_j) = 1$

For $t, r, s \geq 2$, let $N_j = p_j^r q_j^s$, where $j = 1, \ldots, t$ and $r > s$. The attack works for t instances of (N_j, e_j) when there exists integers (d, k_j) satisfying equation of the form $e_jd - k_j\phi(N_j) = 1$. The paper shows that prime factors p_j and q_j of t prime power moduli N_j can be simultaneously found in polynomial time for $N = \max\{N_j\}$ and $d, k_j < N^{\omega}$, for all $\omega = \frac{1-\eta t}{3t+1)}$ and $0 < \omega, \eta < 1$. In this case, the prime power moduli instances (N_j, e_j) share common decryption exponent d.

Theorem 3.2. *Let $N_j = p_j^r q_j^s$ be prime power moduli and $M_j = p_j^{r-2} q_j^{s-2}(p_j - 1)(q_j - 1)$ be public key for $j = 1, \dots, t$, $r, s \geq 2$ and $r > s$. Let (e_j, N_j, M_j) and $(d, p_j, q_j, \phi(N_j))$ be public and private key tuples respectively such that $1 < e_j < \phi(N_j)$ is satisfied. Let $N = \max\{N_j\}$,if there exists positive integers $d, k_j < N^{\omega}$, for all $\omega = \frac{1-\eta t}{3t+1}$ such that key equation $e_j d - k_j \phi(N_s) = 1$ holds, then t prime power moduli N_j can be simultaneously factored in polynomial time for $0 < \omega, \eta < 1$.*

Proof. For $t, r, s \geq 2$, $j = 1, \dots, t$ and $r > s$, let $N_j = p_j^r q_j^s$ be t prime power moduli and $M_j = p_j^{r-2} q_j^{s-2}(p_j - 1)(q_j - 1)$ be t public keys. Suppose $N = \max\{N_j\}$ and $k_j < N^{\omega}$ for $j = 1, \cdots, t$. Then $e_j d - k_j \phi(N_j) = 1$ can be rewritten as

$$\begin{aligned}
e_j d - k_j (p_j^{r-1} q_j^{s-1} (p_j - 1)(q_j - 1)) &= 1 \\
e_j d - k_j (p_j^r q_j^s - (p_j^r q_j^{s-1} + p_j^{r-1} q_j^s) + p_j^{r-1} q_j^{s-1}) &= 1 \\
e_j d - k_j (N_j - (p_j^r q_j^{s-1} + p_j^{r-1} q_j^s) + p_j^{r-1} q_j^{s-1}) &= 1 \\
e_j d - k_j \left(N_j - (2^{-\frac{s-1}{2r}} N_j^{\frac{r+s-1}{2r}} + 2^{-\frac{s}{2r}} N_j^{\frac{r+s-1}{2r}}) + 2^{-\frac{s-1}{2r}} N_j^{\frac{r+s-2}{2r}} \right) &= 1 \\
e_j d - k_j \left(N_j - N_j^{\frac{r+s-1}{2r}} (2^{-\frac{s-1}{2r}} + 2^{-\frac{s}{2r}}) + 2^{-\frac{s-1}{2r}} N_j^{\frac{r+s-2}{2r}} \right) &= 1.
\end{aligned}$$

Let $\Lambda = N^{\frac{r+s-1}{2r}} (2^{-\frac{s-1}{2r}} + 2^{-\frac{s}{2r}})$, and from Lemma 3.1, it was shown that

$$N_j^{\frac{r+s-1}{2r}} (2^{-(\frac{s-1}{2r})} + 2^{-\frac{s}{2r}}) = N_j - \phi(N_j) + 2^{-\frac{s-1}{2r}} N_j^{\frac{r+s-2}{2r}}.$$

Then we have

$$e_j d - k_j \left(N_j - \Lambda + \Lambda - (N_j - \phi(N_j) + 2^{-\frac{s-1}{2r}} N_j^{\frac{r+s-2}{2r}}) + 2^{-\frac{s-1}{2r}} N_j^{\frac{r+s-2}{2r}} \right) = 1.$$

The above equation becomes

$$e_jd - k_j\left(N_j - \Lambda + 2^{-\frac{s-1}{2r}}N_j^{\frac{r+s-2}{2r}}\right) = \quad 1 + k_j\left(\Lambda - N_j + \phi(N_j) - 2^{-\frac{s-1}{2r}}N_j^{\frac{r+s-2}{2r}}\right)$$

$$\left|\frac{e_j}{N_j - \Lambda + 2^{-\frac{s-1}{2r}}N_j^{\frac{r+s-2}{2r}}}d - k_j\right| = \frac{\left|1 + k_j\left(\Lambda - N_j + \phi(N_j) - 2^{-\frac{s-1}{2r}}N_j^{\frac{r+s-2}{2r}}\right)\right|}{N_j - \Lambda + 2^{-\frac{s-1}{2r}}N_j^{\frac{r+s-2}{2r}}}$$

Suppose $N = \max\{N_j\}$, $k_j < N^\omega$, $N_j - \Lambda + 2^{-\frac{s-1}{2r}}N_j^{\frac{r+s-2}{2r}} > \frac{3}{4}N$ and $\left|\Lambda - N_j + \phi(N_j) - 2^{-\frac{s-1}{2r}}N_j^{\frac{r+s-2}{2r}}\right| < N^{2\omega+\eta}$, for $0 < \omega, \eta < 1, j = 1, \ldots, t$. Plugging the conditions into the above equation yields

$$\begin{aligned}\left|\frac{e_j}{N_j - \Lambda + 2^{-\frac{s-1}{2r}}N_j^{\frac{r+s-2}{2r}}}d - k_j\right| &< \frac{1 + N^\omega(N^{2\omega+\eta})}{\frac{3}{4}N} \\ &= \frac{4(1 + N^{3\omega+\eta})}{3N} \\ &< \frac{3}{2}N^{3\omega+\eta-1} \\ \left|\frac{e_j}{N_j - \Lambda + 2^{-\frac{s-1}{2r}}N_j^{\frac{r+s-2}{2r}}}d - k_j\right| &< \frac{3}{2}N^{3\omega+\eta-1}.\end{aligned}$$

In order to show the existence of the integers d, k_j, we let $\mu = \frac{3}{2}N^{3\omega+\eta-1}$ for $\omega = \frac{1-\eta t}{3t+1}$ and $0 < \eta < 1$. Then, we have

$$N^\omega\mu^t = N^\omega\left(\frac{3}{2}N^{3\omega+\eta-1}\right)^t = \left(\frac{3}{2}\right)^t N^{\omega+3\omega t+\eta t-t} = \left(\frac{3}{2}\right)^t.$$

Applying Theorem 2.4, we get $\left(\frac{3}{2}\right)^t < 2^{\frac{t(t-3)}{4}} \cdot 3^t$ for $t \geq 2$. This implies $N^\omega\mu^t < 2^{\frac{t(t-3)}{4}} \cdot 3^t$. It follows that if $d < N^\omega$ then $d < 2^{\frac{t(t-3)}{4}} \cdot 3^t \cdot \mu^{-t}$ for $j = 1, \ldots, t$. This gives

$$\left|\frac{e_j}{N_j - \Lambda + 2^{-\frac{s-1}{2r}}N_j^{\frac{r+s-2}{2r}}}d - k_j\right| < \mu.$$

The above inequality clearly satisfies the conditions of Theorem 2.4. Next, we apply LLL algorithm to get the decryption exponent d and t integers k_j for $j = 1, \ldots, t$ and make the following computations:

$$\begin{aligned} \phi(N_j) &= \frac{e_j d - 1}{k_j} \\ \gcd(\phi(N_j), N_j) &= W_j \\ p_j^{r-2} &= \gcd(M_j, W_j) \\ q_j^s &= \frac{N_j}{p_j^r}. \end{aligned}$$

Finally, the prime factors (p_j, q_j) of the prime power moduli N_j can be found simultaneously in polynomial time for N_j for $j = 1, \ldots, t$. This completes the proof. □

Let

$$\begin{aligned} V_1 &= \frac{e_1}{N_1 - N_1^{\frac{r+s-1}{2r}}\left(2^{-\frac{s-1}{2r}} + 2^{-\frac{s}{2r}}\right) + 2^{-\frac{s-1}{2r}} N_1^{\frac{r+s-2}{2r}}}, \\ V_2 &= \frac{e_2}{N_2 - N_2^{\frac{r+s-1}{2r}}\left(2^{-\frac{s-1}{2r}} + 2^{-\frac{s}{2r}}\right) + 2^{-\frac{s-1}{2r}} N_2^{\frac{r+s-2}{2r}}} \\ V_3 &= \frac{e_3}{N_3 - N_3^{\frac{r+s-1}{2r}}\left(2^{-\frac{s-1}{2r}} + 2^{-\frac{s}{2r}}\right) + 2^{-\frac{s-1}{2r}} N_3^{\frac{r+s-2}{2r}}}. \end{aligned}$$

Define

$$Y = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \mu^{-t-1}].$$

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

$$X = \begin{bmatrix} 1 & -[YV_1] & -[YV_2] & -[YV_3] \\ 0 & Y & 0 & 0 \\ 0 & 0 & Y & 0 \\ 0 & 0 & 0 & Y \end{bmatrix}$$

Taking $r = 3, s = 2$, the matrix X can be used in computing the reduced basis after applying the LLL algorithm.

Algorithm 2 Theorem 3.2

```
Initialization: The public key tuple $(N_j, e_j, M_j, \eta)$ satisfying Theorem 3.2.
Choose $r, s, t \geq 2$, $r > s$ and $N = \max\{N_j\}$ for $j = 1, \dots, t$.
for any $(N, \omega, \eta)$ do
    $\mu := \frac{3}{2} N^{3\omega+\eta-1}$ where $\omega = \frac{1-\eta t}{3t+1}$ and $0 < \omega, \eta < 1$
    $Y := [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \mu^{-t-1}]$ for $t \geq 2$.
end for
Consider the lattice $\mathcal{L}$ spanned by the matrix $X$ as stated above.
Applying the LLL algorithm to $\mathcal{L}$ yields the reduced basis matrix $Z$.
for any $(X, Z)$ do
    $R := X^{-1}$
    $U = RZ.$
end for
Produce $d$, $k_j$ from $U$
for each triplet $(d, k_j, e_j)$ do
    $\phi(N_j) := \frac{e_j d - 1}{k_j}$
    $W_j := \gcd(\phi(N_j), N_j)$
    $p_j^{r-2} := \gcd(M_j, W_j)$
    $q_j^s := \frac{N_j}{p_j^r}$
end for
return the prime factors $(p_j, q_j)$.
```

Example 3.2. *In what follows, we give a numerical example to illustrate how Theorem 3.2 works on three prime power moduli and their corresponding public keys:*

Let

$$\begin{aligned}
N_1 &= 3934513265246647663023562325419214225216712201875\!3\\
N_2 &= 45782584109378359634358469174446104262680719273079\!3\\
N_3 &= 70797222692943531256535175304400137373344309965085\!7\\
e_1 &= 1161315615849750656260732387408463316428962321182\!7\\
e_2 &= 36546274522704347683547519431797247601317608074241\!9\\
e_3 &= 35761516198937597815646161878310723311634414459757\!1\\
M_1 &= 101535203131951001877755154633\!6\\
M_2 &= 342584561536867458546481493609\!6\\
M_3 &= 374236914153303792396636953460\!8.
\end{aligned}$$

Observe that $\max\{N_1, N_2, N_3\}$=

$$N = 707972226929435312565351753044001373733443099650857.$$

By taking $r, t = 3$, $s = 2$, $\eta = 0.595$, and applying Algorithm 2 gives $\omega = \frac{1-\eta t}{3t+1} = 0.12150$ and $\mu = \frac{3}{2}N^{3\omega+\eta-1} = 0.01308174268$. Applying Theorem 2.4 and using Algorithm 2, for $t = 3$ we have

$$Y = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \mu^{-t-1}] = 1382905852.$$

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

$$X = \begin{pmatrix} 1 & -[YV_1] & -[YV_2] & -[YV_3] \\ 0 & Y & 0 & 0 \\ 0 & 0 & Y & 0 \\ 0 & 0 & 0 & Y \end{pmatrix}$$

Therefore, by applying LLL algorithm to $\mathcal{L}$, we obtain reduced basis as follows:

$$Z = \begin{pmatrix} 1620667 & -1080304 & -1016246 & -1755243 \\ 796043 & 1889924 & -8322194 & 4677223 \\ -5392047 & 7485796 & 239422 & -1653527 \\ -9114657 & 558716 & 712482 & 7012619 \end{pmatrix}$$

Next, from Algorithm 2, we compute $U = Z \cdot R$,

$$U = \begin{pmatrix} -1620667 & -478358 & -1293709 & -818641 \\ 796043 & 234961 & 635447 & 402102 \\ -5392047 & -1591523 & -4304240 & -2723663 \\ -9114657 & -2690293 & -7275840 & -4604050 \end{pmatrix} \qquad (1)$$

From the first row of matrix U, we obtain d, k_1, k_2, k_3 as follows:

$$d = 1620667,\ k_1 = 478358,\ k_2 = 1293709,\ k_3 = 818641.$$

Using Algorithm 2, we now compute $\phi(N_j) = \frac{e_j d - 1}{k_j}$ for $j = 1, 2, 3$.

$$\begin{aligned} \phi(N_1) &= 393451326243601621971434025584209319724343917777376 \\ \phi(N_2) &= 457825840988102324767408340476664766792876944698208 \\ \phi(N_3) &= 707972226819614456631048508843756970604900213637616. \end{aligned}$$

Next, from Algorithm 2, we compute $W_j = \gcd(\phi_j, N_j)$ and $p^{r-2} = \gcd(M_j, W_j)$for $j = 1, 2, 3$ and $r = 3$ as follows:

$$\begin{aligned} W_1 &= 1015352032044829811825501298133 \\ W_2 &= 3425845616159472501271490748491 \\ W_3 &= 3742369142113555304134728608591 \\ p_1 &= 26202472313\, P_2 = 25635115217,\ p_3 = 19782311033. \end{aligned}$$

Finally, q can be found by computing $q_j^s = \frac{N_j}{p_j^r}$ for $r = 3$ and $s = 2$ which lead to the simultaneous factorization of three prime power moduli N_1, N_2, N_3 in polynomial time. That is,

$$q_1 = 1478877157,\ q_2 = 5213114219,\ q_3 = 9562965119.$$

3.1.2 The Attack on t Prime Power Moduli $N_j = p_j^r q_j^s$ Satisfying System of Equation $e_j d_j - k\phi(N_j) = 1$

In this section, we present another attack for the simultaneous factorization of t prime power moduli $N_j = p_j^r q_j^s$ in polynomial time satisfying t equation of the form $e_j d_j - k\phi(N_j) = 1$ for unknown integers d_j, k, for $j = 1, \ldots, t$, $r, s \geq 2$ and $r > s$. In this case, every pair of the prime power moduli instances (N_j, e_j) has its own unique decryption exponent d_j.

Theorem 3.3. *Let $N_j = p_j^r q_s^s$ be t prime power moduli, $M_j = p_j^{r-2} q_j^{s-2}(p_j - 1)(q_j - 1)$ be t public keys for $j = 1, \cdots, t$, $r, s, t \geq 2$ and $r > s$. Let (e_j, N_j, M_j) and $(d_j, p_j, q_j, \phi(N_j))$ be public and private key tuples respectively such that $1 < e_j < \phi(N_j)$ is satisfied. Let $e = \min\{e_j\} = N^\sigma$ be public exponent. If there exists integers $d_j, k < N^\omega$, for all $\omega = \frac{t(\sigma-\eta)}{3t+1}$ such that $e_j d_j - k\phi(N_j) = 1$ holds, then prime factors p_j and q_j of t prime power moduli N_j can be simultaneously factored in polynomial time for $0 < \eta, \omega < \sigma < 1$.*

Proof. For $t, r, s \geq 2$, $j = 1, \ldots, t$ and $r > s$, let $N_j = p_j^r q_j^s$ be t prime power moduli and $M_j = p_j^{r-2} q_j^{s-2}(p_j - 1)(q_j - 1)$ be t public keys. Suppose $e = \min\{e_j\} = N^\sigma$ and $d_j < N^\omega$ for $j = 1, \cdots, t$. Then $e_j d_j - k\phi(N_j) = 1$ can be rewritten as

$$\begin{aligned}
e_j d_j - k(p_j^{r-1} q_j^{s-1}(p_j - 1)(q_j - 1)) &= 1\\
e_j d_j - k(p_j^r q_j^s - (p_j^r q_j^{s-1} + p_j^{r-1} q_j^s) + p_j^{r-1} q_j^{s-1}) &= 1\\
e_j d_j - k(N_j - (p_j^r q_j^{s-1} + p_j^{r-1} q_j^s) + p_j^{r-1} q_j^{s-1}) &= 1\\
e_j d_j - k\left(N_j - (2^{-\frac{s-1}{2r}} N_j^{\frac{r+s-1}{2r}} + 2^{-\frac{s}{2r}} N_j^{\frac{r+s-1}{2r}}) + 2^{-\frac{s-1}{2r}} N_j^{\frac{r+s-2}{2r}}\right) &= 1\\
e_j d_j - k\left(N_j - N_j^{\frac{r+s-1}{2r}}(2^{-\frac{s-1}{2r}} + 2^{-\frac{s}{2r}}) + 2^{-\frac{s-1}{2r}} N_j^{\frac{r+s-2}{2r}}\right) &= 1.
\end{aligned}$$

Let $\Lambda = N^{\frac{r+s-1}{2r}}(2^{-\frac{s-1}{2r}} + 2^{-\frac{s}{2r}})$, and from Lemma 3.1, it was shown that

$$N_j^{\frac{r+s-1}{2r}}(2^{-(\frac{s-1}{2r})} + 2^{-\frac{s}{2r}}) = N_j - \phi(N_j) + 2^{-\frac{s-1}{2r}} N_j^{\frac{r+s-2}{2r}}.$$

Then we have

$$e_j d_j - k\left(N_j - \Lambda + \Lambda - \left(N_j - \phi(N_j) + 2^{-\frac{s-1}{2r}} N_j^{\frac{r+s-2}{2r}}\right) + 2^{-\frac{s-1}{2r}} N_j^{\frac{r+s-2}{2r}}\right) = 1.$$

The above equation becomes

$$e_jd_j - k\left(N_j - \Lambda + 2^{-\frac{s-1}{2r}}N_j^{\frac{r+s-2}{2r}}\right) = 1 + k\left(\Lambda - N_j + \phi(N_j) - 2^{-\frac{s-1}{2r}}N_j^{\frac{r+s-2}{2r}}\right)$$

$$\left|\frac{N_j - \Lambda + 2^{-\frac{s-1}{2r}}N_j^{\frac{r+s-2}{2r}}}{e_j}k - d_j\right| = \frac{\left|1 + k\left(\Lambda - N_j + \phi(N_j) - 2^{-\frac{s-1}{2r}}N_j^{\frac{r+s-2}{2r}}\right)\right|}{e_j}.$$

Suppose $N = \max\{N_j\}$, $d_j, k < N^{\omega}$ are positive integers for $j = 1, \dots, t$, $e = \min\{e_j\} = N^{\sigma}$ and $\left|\Lambda - N_j + \phi(N_j) - 2^{-\frac{s-1}{2r}}N_j^{\frac{r+s-2}{2r}}\right| < N^{2\omega+\eta}$. This implies

$$\begin{aligned}\left|\frac{N_j - \Lambda + 2^{-\frac{s-1}{2r}}N_j^{\frac{r+s-2}{2r}}}{e_j}k - d_j\right| &< \frac{1 + N^{\omega}(N^{2\omega+\eta})}{N^{\sigma}} \\ &< \frac{2}{3}N^{3\omega+\eta-\sigma}.\end{aligned}$$

In order to show the existence of the integers d_j, k, we let $\mu = \frac{3}{2}N^{3\omega+\eta-\sigma}$ for $\omega = \frac{t(\sigma-\eta)}{3t+1}$ and $0 < \eta, \omega < \sigma < 1$. Then, we have

$$N^{\omega}\mu^t = N^{\omega}\left(\frac{2}{3}N^{3\omega+\eta-\sigma}\right)^t = \left(\frac{2}{3}\right)^t N^{\omega+3\omega t+\eta t-\sigma t} = \left(\frac{2}{3}\right)^t.$$

Applying Theorem 2.4, we get $\left(\frac{2}{3}\right)^t < 2^{\frac{t(t-3)}{4}} \cdot 3^t$ for $t \geq 2$. This implies $N^{\omega}\mu^t < 2^{\frac{t(t-3)}{4}} \cdot 3^t$. It follows that if $k < N^{\omega}$ then $k < 2^{\frac{t(t-3)}{4}} \cdot 3^t \cdot \mu^{-t}$ for $j = 1, \dots, t$. This gives

$$\left|\frac{N_j - \Lambda + 2^{-\frac{s-1}{2r}}N_j^{\frac{r+s-2}{2r}}}{e_j}k - d_j\right| < \mu.$$

The above inequality clearly satisfies the conditions of Theorem 2.4. Next, we apply LLL algorithm to get the decryption exponents d_j and integer k for

$j = 1, \dots, t$ which can be used to make the following computations:

$$\begin{aligned} \phi(N_j) &= \frac{e_j d_j - 1}{k} \\ \gcd(\phi(N_j), N_j) &= W_j \\ p_j^{r-2} &= \gcd(M_j, W_j) \\ q_j^s &= \frac{N_j}{p_j^r}. \end{aligned}$$

Finally, the prime factors (p_j, q_j) of the prime power moduli N_j can be found simultaneously in polynomial time for $j = 1, \dots, t$. This completes the proof. □

Let

$$\begin{aligned} V_{11} &= \frac{N_1 - N_1^{\frac{r+s-1}{2r}} \left(2^{-\frac{s-1}{2r}} + 2^{-\frac{s}{2r}}\right) + 2^{-\frac{s-1}{2r}} N_1^{\frac{r+s-2}{2r}}}{e_1}, \\ V_{12} &= \frac{N_2 - N_2^{\frac{r+s-1}{2r}} \left(2^{-\frac{s-1}{2r}} + 2^{-\frac{s}{2r}}\right) + 2^{-\frac{s-1}{2r}} N_2^{\frac{r+s-2}{2r}}}{e_2} \\ V_{13} &= \frac{N_3 - N_3^{\frac{r+s-1}{2r}} \left(2^{-\frac{s-1}{2r}} + 2^{-\frac{s}{2r}}\right) + 2^{-\frac{s-1}{2r}} N_3^{\frac{r+s-2}{2r}}}{e_3}. \end{aligned}$$

Define

$$Y_1 = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \mu^{-t-1}].$$

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

$$X_1 = \begin{bmatrix} 1 & -[Y_1 V_{11}] & -[Y_1 V_{12}] & -[Y_1 V_{13}] \\ 0 & Y_1 & 0 & 0 \\ 0 & 0 & Y_1 & 0 \\ 0 & 0 & 0 & Y_1 \end{bmatrix}$$

Taking $r = 3, s = 2$, the matrix X_1 can be used in computing the reduced basis after applying the LLL algorithm.

Algorithm 3 Theorem 3.3

```
Initialization: The public key tuple $(N_j, e_j, M_j, \eta)$ satisfying Theorem 3.3.
Choose $r, s \geq 2$, $r > s$, $e =: \min\{e_j\} := N^{\sigma}$ and $N = \max\{N_j\}$ for $j = 1, \dots, t$.
**for any** $(N, \omega, \eta, \sigma)$ **do**
    $\mu := \frac{2}{3}N^{3\omega+\eta-\sigma}$ for $\omega = \frac{t(\sigma-\eta)}{3t+1}$ and $0 < \omega, \eta < \sigma < 1$
    $Y_1 := [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \mu^{-t-1}]$ for $t \geq 2$.
**end for**
Consider the lattice $\mathcal{L}$ spanned by the matrix $X_1$ as stated above.
Applying the LLL algorithm to $\mathcal{L}$ yields the reduced basis matrix $Z_1$.
**for any** $(X_1, Z_1)$ **do**
    $R_1 := X_1^{-1}$
    $U_1 = R_1 Z_1$.
**end for**
Produce $d_j, k$ from $U_1$
**for each** triplet $(d_j, k, e_j)$ **do**
    $\phi(N_j) := \frac{e_j d_j - 1}{k}$
    $W_j := \gcd(\phi(N_j), N_j)$
    $p_j^{r-2} := \gcd(M_j, W_j)$
    $q_j^s := \frac{N_j}{p_j^r}$
**end for**
**return** the prime factors $(p_j, q_j)$.
```

Example 3.3. *In what follows, we give a numerical example to illustrate how Theorem 3.3 works on three prime power moduli and their corresponding public keys: Let*

$$
\begin{aligned}
N_1 &= 2790456916996092208017072372472705922274621623783630114674768018070410951\\
N_2 &= 8978892610864821038741248358704008658755390077322655166290213046402786537 9\\
N_3 &= 1469889806935193652496065998302040756392356744522935970878350078956729637\\
e_1 &= 1153990559282340762451170346586697592025886173858233752582223038487250964\\
e_2 &= 2042333605378114844219892005584191197008428539316263499112137918885535875 1\\
e_3 &= 348814513827450361866943977739701818744104747623482255293363469341504620\\
M_1 &= 519509956126915567470769197163486594445196 00\\
M_2 &= 247542056061849796104427546447062173228796596\\
M_3 &= 387436776977578140403787273875544991239026 32.
\end{aligned}
$$

Observe that $\max\{N_1, N_2, N_3\}$=

$N = 89788926108648210387412483587040086587553900773226551662902130464027865379$,

and $e_j = \min\{e_1, e_2, e_3\} =$

$348814513827450361866943977739701818744104747623482255293363469341504620$

with $e_j = \min\{e_1, e_2, e_3\} = N^{\sigma}$ for $\sigma = 0.9674033378$ and $\eta = 0.545$. Also, from Algorithm 3, $\omega = \frac{t(\sigma-\eta)}{3t+1} = 0.1267210013$ and $\mu := \frac{2}{3}N^{3\omega+\eta-\sigma} = 0.0005013025547$. Applying Theorem 2.4 and using Algorithm 3, for $t = 3$ we have

$$Y_1 = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \mu^{-t-1}] = 641291305500000.$$

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

$$X_1 = \begin{pmatrix} 1 & -[Y_1 V_{11}] & -[Y_1 V_{12}] & -[Y_1 V_{13}] \\ 0 & Y_1 & 0 & 0 \\ 0 & 0 & Y_1 & 0 \\ 0 & 0 & 0 & Y_1 \end{pmatrix}$$

Therefore, by applying LLL algorithm to $\mathcal{L}$, we obtain reduced basis as follows:

$$Z_1 = \begin{pmatrix} -10689 & 320730 & 103584 & 815229 \\ -826666802866 & 3326275265620 & -5607977569504 & -606915904374 \\ -718775031721 & 6928397172970 & 1265873221376 & -2896060020219 \\ -6203162212727 & -1716050241610 & 117602127712 & 578857273947 \end{pmatrix}$$

Next, from Algorithm 3 we compute $U_1 = Z_1 \cdot R_1$,

$$U_1 = \begin{pmatrix} -10689 & -25847 & -46993 & -45043 \\ -826666802866 & -1998957512740 & -3634348682485 & -3483539414491 \\ -718775031721 & -1738065136579 & -3160014507032 & -3028887992685 \\ -6203162212727 & -14999825401100 & -27271512944399 & -26139866736633 \end{pmatrix} \tag{2}$$

From the first row of matrix U_1 we obtain k, d_1, d_2, d_3 as follows:

$$k = 10689, \; d_1 = 25847, \; d_2 = 46993, \; k_3 = 45043.$$

Using Algorithm 3, we now compute $\phi(N_j) = \frac{e_j d_j - 1}{k}$ for $j = 1, 2, 3$.

$$\begin{aligned} \phi(N_1) &= 27904569169960390763472167600548575789216091248679734121987 76 \\ &\quad 206921131600 \\ \phi(N_2) &= 897889261086479098834553138913068546365582209262692212683849 7 \\ &\quad 2609400306276 \\ \phi(N_3) &= 146988980693515264754165568241457470499492096053929378100654 6 \\ &\quad 051973935128. \end{aligned}$$

Next, from Algorithm 3, we compute $W_j = \gcd(\phi_j, N_j)$ and $p_j^{r-2} = \gcd(M_j, W_j)$ for $j = 1, 2, 3$ and $r = 3$ as follows:

$$\begin{aligned} W_1 &= 519509956126925459195420998390327030634 67881 \\ W_2 &= 247542056061850624573712528172703509876452159 \\ W_3 &= 387436776977588948579544319721393185033 66403 \\ p_1 &= 967191404644711 \, P_2 = 682456870518539, \; p_3 = 1021214348494357. \end{aligned}$$

Finally, q can be found by computing $q_j^s = \frac{N_j}{p_j^r}$ for $r = 3, j = 1, 2, 3$ and $s = 2$ which leads to the simultaneous factorization of three prime power moduli N_1, N_2, N_3 in polynomial time. That is,

$$q_1 = 55535286711161, \; q_2 = 531494253385079, \; q_3 = 37150702190747.$$

4 CONCLUSION

In this paper, we presented the polynomial time factorization of the prime power moduli $N = p^r q^s$ using continued fractions method. Our approach proved that the decryption exponent d can be found from the convergents of the continued fractions expansion of $\frac{e}{N-N^{\frac{r+s-1}{2r}}\left(2^{-(\frac{s-1}{2r})}+2^{-\frac{s}{2r}}\right)+2^{-\frac{s-1}{2r}}N^{\frac{r+s-2}{2r}}}$ efficiently, where $N-N^{\frac{r+s-1}{2r}}\left(2^{-(\frac{s-1}{2r})}+2^{-\frac{s}{2r}}\right)+2^{-\frac{s-1}{2r}}N^{\frac{r+s-2}{2r}}$ is considered to be a good approximation of $\phi(N)$. The paper also utilizes the combination of LLL algorithm and simultaneous Diophantine approximations techniques for the successful factorization t prime power moduli $N_j = p_j^r q_j^s$ into its prime factors of p_j and q_j using generalized system of equation which has not been reported by previous research works based on the available literature within our reach.

REFERENCES

Abubakar, S. I., Ariffin, M. R. K., and Asbullah, M. A. (2018). A new simultaneous diophantine attack upon rsa moduli $n = pq$. In *Cryptology and Information Security Conference*, page 119.

Ariffin, K., Rezal, M., Abubakar, S. I., Yunos, F., and Asbullah, M. A. (2019). New cryptanalytic attack on rsa modulus $n = pq$ using small prime difference method. *Cryptography*, 3(1):2.

Ariffin, M. R. K. and Shehu, S. (2016). New attacks on prime power rsa modulus $n = p^r q$. *Asian Journal of Mathematics and Computer Research*, pages 77–90.

Blömer, J. and May, A. (2004). A generalized Wiener attack on RSA. In *International Workshop on Public Key Cryptography*, pages 1–13. Springer.

Boneh, D. and Durfee, G. (1999). Cryptanalysis of RSA with private key $d < N^{0.292}$. In *Advances in Cryptology-Eurocrypt99, Lecture Notes in Computer Science*, pages 1–11. Springer-Verlag.

Bunder, M. and Tonien, J. (2017). A new attack on the RSA cryptosystem based on continued fractions. *Malaysian Journal of Mathematical Sciences:Special Issue: The 5th International Cryptology and Information Security Conference (New Ideas in Cryptology*, 11(S):45–57.

Chen C.Y. Hsueh, C. and Lin, Y. (2009). A generalization of de Weger's method. *IEEE*, 1:344–347.

Collins, T., Hopkins, D., Langford, S., and Sabin, M. (1998). Public key cryptographic apparatus and method. US Patent 5,848,159.

Coron, J.-S., Faugère, J.-C., Renault, G., and Zeitoun, R. (2016). Factoring $n = p^r q^s$for large r and s. In *Cryptographers Track at the RSA Conference*, pages 448–464. Springer.

Coron, J.-S. and Zeitoun, R. (2018). Improved factorization of $n = p^r q^s$. In *Cryptographers Track at the RSA Conference*, pages 65–79. Springer.

de Weger, B. (2002). Cryptanalysis of RSA with small prime difference. *Applicable Algebra in Enginering, Commnication and Computing AAECC*, 13:17–28.

Herrmann, M. and May, A. (2007). On factoring arbitrary integers with known bits. *Informatik 2007–Informatik trifft Logistik–Band 2*.

Hinek, M. J. (2008). On the security of multi-prime rsa. *Journal of Mathematical Cryptology*, 2(2):117–147.

Lenstra, A.K. Lenstra, H. and Lovsz, L. (1982). Factoring polynomials with rational coefficients. *Mathematische Annalen*, pages 513–534.

Lim, S., Kim, S., Yie, I., and Lee, H. (2000). A generalized takagi-cryptosystem with a modulus of the form $p^r q^s$. In *International Conference on Cryptology in India*, pages 283–294. Springer.

Lu, Y., Peng, L., and Sarkar, S. (2017). Cryptanalysis of an rsa variant with moduli $n = p^r q^l$. *Journal of Mathematical Cryptology*, 11(2):117–130.

Maitra, S. and Sarkar, S. (2008). Revisiting wieners attack new weak keys in RSA. In *Lecture Notes in Computer ScienceInternational Conference on Information Security-ISC 2008*, pages 228–243. Springer.

Nitaj, A. (2013). Diophantine and lattice cryptanalysis of the rsa cryptosystem. In *Artificial Intelligence, Evolutionary Computing and Metaheuristics*, pages 139–168. Springer.

Nitaj, A., Ariffin, M., Nassr, D., and Bahig, H. (2014). New Attacks on the RSA cryptosystem. In *Progress in Cryptology AFRICACRYPT 2014. Lecture Notes in Computer Science*, volume 8469, pages 178–198. Springer.

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

Santoso, B., Kunihiro, N., Kanayama, N., and Ohta, K. (2008). Factorization of square-free integers with high bits known. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 91(1):306–315.

Sarkar, S. (2016). Revisiting prime power rsa. *Discrete Applied Mathematics*, 203:127–133.

Takagi, T. (1998). Fast rsa-type cryptosystem modulo $p^k q$. In *Annual International Cryptology Conference*, pages 318–326. Springer.

Wang, S., Qu, L., Li, C., and Wang, H. (2019). Further improvement of factoring $n = p^r q^s$ with partial known bits. *Adv. in Math. of Comm.*, 13(1):121–135.

Wang, X., G., X., Wang, M., and Meng, X. (2016). *Mathematical Foundations of Public Key Cryptography*. CRC Press, Boca Rating London New York.

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

Zhang, H. and Takagi, T. (2013). Attacks on multi-prime rsa with small prime difference. In *Australasian Conference on Information Security and Privacy*, pages 41–56. Springer.

Zheng, M., Kunihiro, N., and Hu, H. (2017). Improved factoring attacks on multi-prime rsa with small prime difference. In *Australasian Conference on Information Security and Privacy*, pages 324–342. Springer.