Proceedings of International Mathematical Sciences
ISSN:2717-6355, URL:https://dergipark.org.tr/tr/pub/pims
Volume II Issue 2 (2020), Pages 103-128. Doi: 10.47086/pims.827108

DIOPHANTINE ATTACK ON PRIME POWER WITH MODULUS $N = p^r q$

SAIDU ISAH ABUBAKAR*, ZAID IBRAHIM**, SADIQ SHEHU *** AND AHMAD RUFAI****
*DEPARTMENT OF MATHEMATICS, SOKOTO STATE UNIVERSITY , SOKOTO, NIGERIA. ORCID NUMBER:0000-0002-0201-0064:
**DEPARTMENT OF MATHEMATICS, SOKOTO STATE UNIVERSITY , SOKOTO, NIGERIA. ORCID NUMBER:0000-0002-0251-6495:
***DEPARTMENT OF MATHEMATICS, SOKOTO STATE UNIVERSITY , SOKOTO, NIGERIA. ORCID NUMBER: 0000-0001-5908-7452:
****DEPARTMENT OF MATHEMATICS, SOKOTO STATE UNIVERSITY , SOKOTO, NIGERIA. ORCID NUMBER:0000-0003-3223-9924:

Abstract. The importance of keeping information secret cannot be overemphasized especially in today,s digital world where eavesdroppers are rampant in our chanels of communication. This made the use of strong encryption schemes inevitable in order to safeguard the security of our system. RSA cryptosystem and its variants have been designed to provide confidentiality and integrity of data in our medium of communication. This paper reports new short decryption exponent attack on prime power with modulus $N = p^r q$ for $r \geq 2$ using continued fraction method which makes it vulnerable to Diophantine attack and breaks the security of the cryptosystem by factoring the modulus into its prime factors since the hardness relies on the integer factorization problem. The paper also shows that if the short decryption exponent $d < \frac{1}{\sqrt{2}}\sqrt{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}}$, then one of the convergents $\frac{k}{d}$ can be found from the continued fraction expansion of $\frac{e}{N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil}$ which leads to the successful factorization of prime power modulus $N = p^r q$ in polynomial time. The second part of the paper presents new findings on simultaneous factorization of t prime power with moduli $N_s = p_s^r q_s$ for $s = 1, \ldots, t$ using simultaneous Diophantine approximations and lattice basis reduction methods which produces the prime factors of the form (p_s, q_s) for $s = 1, \ldots, t$ in polynomial time where solutions of four system of equations of the form $e_s d - k_s \phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s \phi(N_s) = z_s$ and $e_s d_s - k\phi(N_s) = z_s$ are provided. Our results increases the short decryption exponent bounds of some reported works.

2020 *Mathematics Subject Classification.* 11A52 ; 11A54; 11A55.
Key words and phrases. Diophantine; Attacks; Prime Power; Modulus; Continued Fraction.

Submitted November 17th, 2020. Published on december 30th, 2020. Communicated by Sahin UYAVER.

1. INTRODUCTION

The RSA cryptosystem invented by Rivest, Shamir and Adleman is considered to be the most widely used public key cryptosystem in today's digital world, [1]. Since then it has being extensively used for many applications in government as well as commercial domains which include e-banking, secure telephone, smart cards and communications in different types of Networks [2].

The security of this cryptosystem relies on the integer factorization problem. This cryptosystem has also many variants for computational efficiency. In this paper, we will focus on one of the variants known as prime power RSA with modulus $N = p^r q$ for $r \geq 2$. Fujioka et al. was the first to use the modulus $N = p^2 q$ for digital signature whose computational speed is faster than the original RSA scheme, as reported in [3]. Also in 1998, Okamoto et al. proposed a public key cryptography scheme whose security is considered to be as difficult as factoring an RSA modulus of the form $N = p^2 q$, as reported [4].

This paper focuses on the first variant given as $ed \equiv 1 \pmod{p^{r-1}(p-1)(q-1)}$ Using the first prime power RSA variant, Takagi in 1999 proposed a fast CRT-RSA variant with modulus $N = p^r q$ which is considered to be less vulnerable to attacks than the original RSA scheme, [5]. Takagi (1999) showed that when $d < N^{\frac{1}{2(r+1)}}$ for $r \geq 2$, the modulus $N = p^r q$ can be factored efficiently using lattice based technique. May (2004), reported an improvement on the bound of Takagi, where he showed that the modulus $N = p^r q$ is insecure if the short secret exponent $d < N^{\max\{\frac{r}{(r+1)^2}, \frac{(r-1)^2}{(r+1)^2}\}}$ using generalized Coppersmith's method, as reported by [6]. Also, Sarkar (2014) reported the used of small secret exponent attack on prime power RSA with modulus $N = p^2 q$ where he proved that the cryptosystem is insecure if the decryption exponent bound $d < N^{0.395}$, [7]. Furthermore, Lu et. al (2015) improved May's bound to $d < N^{\frac{r(r-1)}{(r+1)^2}}$ by method of lattice construction, [8]. In another result, Sarkar (2016) reported an improved bound of Lu et al. for $2 \leq r \leq 4$, [9].

For the second variant of prime power modulus $N = p^r q$, Itoh et al. (2008) showed that the prime factors of the prime power RSA modulus $N = p^r q$ can be found in polyomial time if the bound $d < \frac{2-\sqrt{2}}{r+1}$, [10].

Also, Blomer and May (2004) reported generalized Wiener's attack using combination of continued fraction and lattice basis reduction techniques which showed that RSA modulus $N = pq$ is insecure when there exist some unknown integers x, y, z such that equation $ex - y\phi(N) = z$ is satisfied where $x < \frac{1}{3} N^{\frac{1}{4}}$ and $|z| < exN^{\frac{-3}{4}}$, [11]. In his work, Hinek (2007) proved that k instances of RSA moduli N_i can be factored if $d < N^{\gamma}$ for $\gamma = \frac{k}{2(k+1)} - \varepsilon$ where ε is a small constant determine based on the size of $\max\{N_i\}$, as reported in [12].

In another development, Nitaj et al. (2014) presented two scenarios which showed that k instances of RSA moduli $N_i = p_i q_i$ can be factored simultaneously in polynomial time using simultaneous Diophantine approximation and LLL algorithm , [13]. In the first scenario, they showed that if the equation $e_i x - y_i \phi(N_i)$ is satisfied where $x < N^{\delta}$, $y_i < N^{\delta}$, $|z_i| < \frac{p_i - q_i}{3(p_i+q_i)} y_i N^{\frac{1}{4}}$ for $\delta = \frac{k}{2(k+1)}$, $N = \min\{N_i\}$ then k RSA moduli can be factored simultaneously. For the second scenario, they proved that k instances of RSA public key pairs (N_i, e_i) satisfying $e_i d_i - y\phi(N_i) = z_i$ for unknown integers $x_i,\ y, z_i$ where $x < N^{\delta},\ y_i < N^{\delta},\ |z_i| < \frac{p_i - q_i}{3(p_i+q_i)} y_i N^{\frac{1}{4}}$ for

$\delta = \frac{k(2\alpha-1)}{2(k+1)}$, $N = \min\{N_i\}$ and $\min\{e_i\} = N^\alpha$. They used simultaneous Diophantine approximations and lattice basis reduction techniques and finally use the Coppersmith's method to compute prime factors p_i and q_i of RSA moduli N_i in polynomial time.

Furthermore, Shehu and Ariffin (2017) also presented a polynomial time attack on j instances of prime power RSA with modulus $N_i = p_i^r q_i$ using a good approximation of $\phi(N)$ in which they proved that for j, $r \geq 2$ and given public key pairs (N_i, e_i) and $N = \min\{N_i\}$, then equation $e_i d - k_i \phi(N_i) = 1$ can be satisfied only if the unknown integer $d < N^\delta$ and j integers $k_i < N^\delta$ where $\delta = \frac{j-\gamma j}{j+1}$ for $0 \leq \gamma < 1$, as reported in [14]. Also using equation $e_i d_i - k\phi(N_i) = 1$, Shehu and Ariffin (2014) showed that j prime power RSA modulus $N_i = p_i^r q_i$ can be simultaneously factored if the j integers $d_i < N^\delta$ and integer $k < N^\delta$, $N = \min\{N_i\}$, and $\min\{e_i\} = N^\beta$ where $\delta = \frac{j(\beta-\gamma)}{j+1}$ for $\gamma < \beta < 1$, [14].

The findings of this paper is reported in two parts. In the first part, we work on the first variant of prime power modulus with equation of the form $ed \equiv 1 \pmod{p^{r-1}(p-1)(q-1)}$ using continued fraction method. Firstly, we construct a lemma which gives approximation of $\phi(N)$ given by $\phi(N) > N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil$ and formulate a theorem which shows that if the secret exponent $d < \frac{1}{\sqrt{2}} \sqrt{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}}$, then one of the convergents $\frac{k}{d}$ can be found from the continued fraction expansion of $\frac{e}{N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil}$ which leads to the factorization of prime power modulus $N = p^r q$ in polynomial time for $r \geq 2$. The paper also gives numerical example to justify how Theorem 3.2 works.

The second part of this paper presents cryptanalysis attacks of factoring t instances of prime power moduli $N_s = p_s^r q_s$ in which we show that the moduli can be factored simultaneously using simultaneous Diophantine approximations and lattice basis reduction techniques. We present four new attacks using system of equations of the form $e_s d - k_s \phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s \phi(N_s) = z_s$ and $e_s d_s - k\phi(N_s) = z_s$ for $s = 1, \ldots, t$, for $r \geq 2$ where the parameters d, d_s, k, k_s, and z_s are unknown positive integers. In all the presented attacks, we have improved decryption exponent bound of some reported attacks.

The rest of the paper is organize as follows. In Section 2, we present review of some basic definitions of the terms used such as continued fraction, lattice basis reduction and some theorems that are related to our attacks. In Section 3 , we present the proofs of our main results with lemma and theorems and their respective numerical examples and finally in Section 4, we conclude the paper.

2. PRELIMINARIES

In this section, we present some basic definitions on continued fraction, lattice basis reduction and some theorems on continued fraction, LLL and simultaneous Diophantine approximations.

Definition 2.1. *(Continued fraction)The continued fraction of a real number x is an expression of the form*

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

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

Definition 2.2. *Let* $\vec{b_1}, \cdots \vec{b_m} \in \mathcal{R}^n$. *The vectors* $b_i's$ *are said to be linearly dependent if there exist* $x_1, \ldots, x_m \in R$, *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* $b_1 \ldots b_n$ *on* $\mathcal{R}^n$ *suchthat* $\mathcal{L} = \sum_{i=1}^{n} \mathcal{Z} b_i = \sum_{i=1}^{n} r_i b_i : r_i \in \mathcal{Z}, 1 \leq i \leq n$.
In this situation, we say that $b_1 \cdots b_n$ *are basis for* $\mathcal{L}$ *or that they span* $\mathcal{L}$, [15].

Definition 2.4. *(LLL Reduction)* [16] *Let* $\mathcal{B} = \langle b_1 \cdots b_n \rangle$ *be a basis for a lattice* $\mathcal{L}$ *and let* $B^* = \langle b_1^* \cdots b_n^* \rangle$ *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 2.1. *If* $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_k}{q_k}, \ldots$ *are convergents of the simple continued fraction* $[a_1, a_2, \ldots, a_k, \ldots]$, *then the numerators and denominators of these convergents satisfy the following recursive relations:*

$$p_1 = a_1, \; p_2 = a_2 a_1 + 1, p_k = a_k p_{k-1} + p_{k-2},$$
$$q_1 = 1, q_2 = a_2, \; q_k = a_k q_{k-1} + q_{k-2},$$

for $k \geq 3$, [17].

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.

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* $b_1 \cdots b_n$ *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 $1 \leq j \leq n$, [15].

Theorem 2.4. *(Simultaneous Diophantine Approximations, [13]) 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*

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

3. MAIN RESULTS

This section has two parts. The first part reports short decryption exponent attack on prime power modulus $N = p^r q$ using continued fraction method which leads to the successful factorization of the modulus in polynomial time. In the second part of the paper, we present cryptanalysis attacks using simultaneous Diophantine approximations and lattice basis reduction methods in factoring t prime power modulus $N_s = p_s^r q_s$ using system of equations of the form $e_s d - k_s\phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s\phi(N_s) = z_s$ and $e_s d_s - k\phi(N_s) = z_s$ for $s = 1, \ldots, t$, for $r \geq 2$ where parameters d, d_s, k, k_s and z_s are unknown positive integers.

3.1. Cryptanalytic Attack Through Analyzing Approximation of $\phi(N)$ given by $N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil$.

This section presents a lemma which shows that if $q < p < 2q$ and the prime power modulus $N = p^r q$, then $\phi(N) > N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil$ where p and q are distinct prime factors of the modulus $N = p^r q$, for $r \geq 2$. The section also proves a theorem which shows that the prime factors p and q can be recovered efficiently if $d < \frac{1}{\sqrt{2}}\sqrt{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}}$.

Lemma 3.1. *Let p and q be prime numbers where $p < q < 2p$ and $N = p^r q$ for $r \geq 2$. If $e < \phi(N)$ and $N^{\frac{1}{r+1}} < p < 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$, then $\phi(N) > N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil$.*

Proof. Let $N = p^r q$ and the condition $q < p < 2p$ holds, then multiplying by p^r yields $N^{\frac{1}{r+1}} < p < 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$.
Using $\phi(N) = p^{r-1}(p-1)(q-1)$, gives the following

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

Since $q < p$ and $p < 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$, then we have

$$\begin{aligned} N - \phi(N) &< 2p^r \\ &< 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}. \end{aligned}$$

Hence $\phi(N) > N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}$. □

Theorem 3.2. *Let p and q be prime numbers satisfying $p < q < 2p$ and let $N = p^r q$ be prime power modulus where (N, e) and (N, d) are public and private keys pairs respectively with $e < \phi(N)$. If the decryption exponent $d < \frac{1}{\sqrt{2}}\sqrt{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}}$, then one of the convergents $\frac{k}{d}$ can be found from the continued fraction expansion of*

$\frac{e}{N-\left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil}$ *which leads to the factorization of prime power modulus* $N = p^r q$ *for* $r \geq 2$ *in polynomial time.*

Proof. Observe

$$\begin{aligned} \frac{ed - k\phi(N)}{d\phi(N)} &= \frac{e}{\phi(N)} - \frac{k}{d} \\ &= \frac{1}{d\phi(N)} \\ &> 0 \end{aligned}$$

Taking $N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil$ from Lemma 3.1 as approximation of $\phi(N)$ yields::

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

Since $N - \phi(N) < \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil$, let $\frac{e\left(N-\phi(N)-\left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil\right)}{\phi(N)(N-\left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil)} = T < 0$, then

$$\begin{aligned} &= \frac{e}{\phi(N)} - \frac{k}{d} - T \\ &< \frac{e}{\phi(N)} - \frac{k}{d} \\ &= \frac{1}{d\phi(N)} \\ &< \frac{1}{\phi(N)}. \end{aligned}$$

It was shown from Lemma 3.1 that $\phi(N) > N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}$, this implies

$$\frac{1}{\phi(N)} < \frac{1}{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}}$$

Since $d < \frac{1}{\sqrt{2}} \sqrt{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}}$, then

$$\frac{1}{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}} < \frac{1}{2d^2}.$$

Hence,

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

This shows that Theorem 3.2 produces $\frac{k}{d}$ as one of the convergent of the continued fraction expansion of $\frac{e}{N-2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}}$. This terminates the proof. □

The section also outlines below the algorithm to be followed in factoring the prime power modulus $N = p^r q$ for $r \geq 2$.

Algorithm 1 Theorem 3.2

1: Initialization: Input the size n and (e, N) satisfying Theorem 3.2.
2: Compute the continued fraction of $\frac{e}{N-\left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil}$ for $r \geq 2$
3: **for each** convergent $\frac{k}{d}$ of $\frac{e}{N-\left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil}$ **do**
4: $\quad \phi(N) := \frac{ed-1}{k}$.
5: $\quad p^{r-1} := \gcd\left(N, \frac{ed-1}{k}\right)$
6: **end for**
7: **if** $1 < p^{r-1} < N$ **then**
8: $\quad q := \frac{N}{p^r}$.
9: **end if**
10: **return** the private keys (p, q) .

Example 3.1. *This example gives an illustration of how Theorem 3.2 works on prime power modulus $N = p^r q$ for $r = 3$.*

$$\begin{aligned}
\textit{Let } N = {} & 64678246809679914850939685949849066984528469181266198775447954764512899975949030092389431143550672950630682676159477346727505541\\
& 77691953695737158023409301972062940648475622585500471848562296576246425671326682796985765039149169432233422230426191901156305513911690643137255586285890252274214143777796475233050043697253070\\
e = {} & 55281000751499877009107259165123700376809649466944460805706223523089195654398883367721127616833362407742058300902057826829515125034066183663278580767186726153429453492047380587411856008249.
\end{aligned}$$

Taking the continued fraction expansion of $\frac{e}{N-\left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil}$ for $r = 3$, gives the following: $[0, 87, 1, 1, 32, 1, 95, 1, 13, 1, 13, 1, 7, 2, 6, 2, 6, 2, 1, 2, 2, 4, 7, 580, 1, 22, 5, 3, 30, 1, 1, 3, 3, 1, 14, 12, 5, 2, 26, 2, 3, 2, 1, 1, 1, 1, 9, 1, 16, 4, 1, 2, 1, 1, 4, 5, 1, 1, 1, 32, 1, 76, 13, 1, 2, 1, 14, 1, 1, 22, 1, 5, 1, 40, 1, 5, 2, 2, 3, 1, 1, 4, 273, 3, 1, 40, 3, 15, 1, 3, 1, 10, 36, 1, 43, 1, 3, 2, 1, 1, 1, 4, 2, 2, 3, 3, 2, 3, 1, 2, 1, 10, 1, 10, 1, 1, 1, 1, 9, 1, 1, 5, 1, 4, 2, 1, 9, 10, 1, 6, 8, 2, 4, 4, 6, 1, \ldots,]$. Then the convergent $\frac{k}{d}$ is found from the continued fraction expansion of $\frac{e}{N-\left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil}$ as

$$\frac{k}{d} = \frac{528369155574929758734471178633 5}{462362453808524086451896135480609}.$$

From Algorithm 1, we compute $\phi(N) = \frac{ed-1}{k}$ as follows:

$$\begin{aligned}
\phi(N) = {} & 64678246809679914850939685949849066984528469181266198775447954734769\\
& 19313372348183843208998399569436036670863930678884295028399128045789\\
& 53081294203558977769396768768923146094038024821936125526310321010437018161613390372921479673079645463655977965218274984.
\end{aligned}$$

Finally, from Algorithm 1 the following computations reveal the prime factors p and q of the prime power modulus $N = p^r q$:

$p^{r-1} = \gcd(N, \phi(N))$

$p = 568411957220695483099546712094710810857461543921464398521916102 7$

$q = \frac{N}{p^3}$

$q = 352183190503750596342466341162994165841738914383679121520787819 7.$

From our result, one can observe that, this work yields $d \approx N^{0.1281}$ which is greater than Shehu-Ariffin's bound $d \approx N^{0.102}$, as reported in [14].

3.2. Cryptanalysis Attacks on t Prime Power With Moduli $N_s = p_s^r q_s$ Using $N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}$ as Approximation of $\phi(N)$.

This section presents four successful cryptanalysis attacks of factoring t prime power with moduli $N_s = p_s^r q_s$ using systems of equations $e_s d - k_s\phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s\phi(N_s) = z_s$ and $e_s d_s - k\phi(N_s) = z_s$ where the parameter $\phi(N) = N - (p^r + p^{r-1}q - p^{r-1})$ for $r \geq 2$ and $s = 1, \ldots, t$.

3.2.1. *The Attack on t Prime Power Moduli $N_s = p_s^r q_s$ Satisfying System of Equation $e_s d - k_s\phi(N_s) = 1$.*

Taking $t \geq 2$, let $N_s = p_s^r q_s$, for $s = 1, \ldots, t$ and $r \geq 2$. The attack works for t instances of the public key tuple (N_s, e_s) when there exists an integer d and t integers k_s satisfying equation $e_s d - k_s\phi(N_s) = 1$. It shows that t prime factors p_s and q_s of t prime power with moduli $N_s = p_s^r q_s$ for $s = 1, \ldots, t,, r \geq 2$ can be found efficiently for $N = \max\{N_s\}$ and $d < N^{\varrho}$, $k_s < N^{\varrho}$, for all $\varrho = \frac{t(1-\beta)}{t+1}$ for $0 < \beta < 1$. In this case, the instances (N_s, e_s) shared common decryption exponent d.

Theorem 3.3. *Let $N_s = p_s^r q_s$ be prime power moduli for $r \geq 2$, $s = 1, \cdots, t$ and $t \geq 2$. Let (N_s, e_s) be public key pair and (d, N_s) be private key pair with condition $e_s < \phi(N_s)$ and the relation $e_s d \equiv 1 \mod \phi(N_s)$ is satisfied. Let $N = \max\{N_s\}$. If there exists positive integers $d < N^{\varrho}$, $k_s < N^{\varrho}$, for all $\varrho = \frac{t(1-\beta)}{t+1}$ such that equation $e_s d - k_s\phi(N_s) = 1$ holds, for $0 < \beta < 1$, then t prime power moduli N_s can successfully be factored in polynomial time for $\frac{1}{4} \leq \varrho \leq \frac{1}{2}$ and $0 < \beta < 1$.*

Proof. For $r, t \geq 2$ where $N_s = p_s^r q_s$ is prime power moduli. Suppose that $N = \max\{N_s\}$ and $k_s < N^{\varrho}$ for $s = 1, \ldots, t$. Then equation $e_s d - k_s\phi(N_s) = 1$ can be rewritten as follows:

$$e_s d - k_s(N_s - (N_s - \phi(N)_s)) = 1.$$

Let $\triangle = 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}$

$$e_s d - k_s\left(N_s - \triangle + \triangle - (N_s - \phi(N_s))\right) = 1$$

$$\left|\frac{e_s}{N - \triangle} d - k_s\right| = \frac{|1 - k_s(N_s - \phi(N_s) - \triangle)|}{N_s - \triangle}. \tag{3.1}$$

Since $N = \max\{N_s\}$ and $k_s < N_s^{\varrho}$, $d < N^{\varrho}$ be positive integers. Observe

$$|N_s - \phi(N_s) - \triangle| < N_s^{\beta} < N^{\beta}$$

for $\beta \in (0,1)$ and

$$N_s - \triangle > \frac{1}{r+2}N,$$

then plugging into equation (3.1) gives

$$\begin{aligned}\left|\frac{1 - k_s(N_s - \phi(N_s) - \triangle)}{N_s - \triangle}\right| &< \frac{|1 + k_s(N_s - \phi(N_s) - \triangle)|}{N_s - \triangle} \\ &< \frac{1 + N^{\varrho}(N^{\beta})}{\frac{1}{r+2}N} \\ &= \frac{r + 2(1 + N^{\varrho+\beta})}{N} \\ &< \sqrt{2r}N^{\varrho+\beta-1}.\end{aligned}$$

Then, it follows that

$$\left|\frac{e_s}{N_s - \triangle}d - k_s\right| \quad < \quad \sqrt{2r}N^{\varrho+\beta-1}.$$

We proceed to show the existence of integer d and t integers k_s. Let $\varepsilon = \sqrt{2r}N^{\varrho+\beta-1}$, with $\varrho = \frac{t(1-\beta)}{t+1}$. Then it gives

$$N^{\varrho}\varepsilon^t = N^{\varrho}\left(\sqrt{2r}N^{\varrho+\beta-1}\right)^t = (2r)^{\frac{t}{2}}\, N^{\varrho+\varrho t+\beta t-t} = (2r)^{\frac{t}{2}}\,.$$

Following Theorem 2.4, $(2r)^{\frac{t}{2}} < 2^{\frac{t(t-3)}{4}} \cdot 3^t$ for $t, r \geq 3$, then $N^{\varrho}\varepsilon^t < 2^{\frac{t(t-3)}{4}} \cdot 3^t$. It follows that since $d < N^{\varrho}$ then $d < 2^{\frac{t(t-3)}{4}} \cdot 3^t \cdot \varepsilon^{-t}$ for $s = 1, \cdots, t$, yields

$$\left|\frac{e_s}{N_s - \triangle}d - k_s\right| < \varepsilon.$$

This clearly satisfies the conditions of Theorem 2.4, and proceeds to reveal the private key d and t integers k_s for $s = 1, \ldots, t$. Next, from $e_s d - k_s\phi(N_s) = 1$ we perform the following computations:

$$\begin{aligned}\phi(N_s) &= \frac{e_s d - 1}{k_s} \\ p_s^{r-1} &= \gcd(\phi(N_s), N_s) \\ q_s &= \frac{N_s}{p_s^r}.\end{aligned}$$

Finally, the prime factors p_s and q_s can be revealed which leads to the factorization of t prime power moduli N_s for $s = 1, \cdots, t$ in polynomial time. □

Let

$$\begin{aligned}X_1 &= \frac{e_1}{N_1 - 2^{\frac{2r+1}{r+1}}N_1^{\frac{r}{r+1}}}, \\ X_2 &= \frac{e_2}{N_2 - 2^{\frac{2r+1}{r+1}}N_2^{\frac{r}{r+1}}}, \\ X_3 &= \frac{e_3}{N_3 - 2^{\frac{2r+1}{r+1}}N_3^{\frac{r}{r+1}}}.\end{aligned}$$

Define,

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

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

$$M = \begin{bmatrix} 1 & -[T(X_1)] & -[T(X_2)] & -[T \times X_3] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{bmatrix}$$

Taking $r \geq 2$, the matrix M can be used in computing the reduced basis after applying the LLL algorithm.

Algorithm 2 Theorem 3.3

Initialization: The public key tuple $(N_s, e_s, \varrho, \beta)$ satisfying Theorem 3.3.
Choose $r \geq 2$ and $N = \max\{N_s\}$ for $s = 1, \ldots, t$.
for any (r, N, ϱ, β) **do**
    $\varepsilon := \sqrt{2r} N^{\varrho+\beta-1}$
    $T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}]$ for $t \geq 2$.
end for
Consider the lattice $\mathcal{L}$ spanned by the matrix M as stated above.
Applying the LLL algorithm to $\mathcal{L}$ yields the reduced basis matrix K.
for any (M, K) **do**
    $J := M^{-1}$
    $Q = JK$.
end for
Produce d, k_s from Q
for each triplet (d, k_s, e_s) **do**
    $\phi(N_s) := \frac{e_s d - 1}{k_s}$
    $p_s^{r-1} := \gcd(\phi(N_s), N_s)$.
    $q_s := \frac{N_s}{p_s^r}$
end for
return the prime factors (p_s, q_s).

Example 3.2. *This example gives an illustration of how Theorem 3.3 works on 3 prime power moduli also their corresponding public exponents:*
Let $N_1 = 563382281374803858489382903716443474446580306437566005728878179$
$267676092551665191432331661132041057581935108036853538725342976031062566$
$064493977301796320064579931954653$

$N_2 = 110780160868938860790802031427539545689163771392478000053424961 7$
$140001335413025467235568243203922733387749142234285602245999359726144181$
$863789668190983522850626483669023$

$N_3 = 965401330168501605540050609837559483013713042769305626483689967 4$
$069160933238013628743471068194753666107834756424555627523960922969439392$
$110512678610069913809409216181 39$

$e_1 = 167644581477517488105562931315300218840429906809208126622351842 22$
$412584386285442254876550471043222816261798853928202440252160827176635480$

737937406061140259278673467716 1

$e_2 = 463152461180608542345912471172475221050879200856094014904488212481504858333502122923328285666380831883415086844453517642192115335016879503086688812611607958721881159677$

$e_3 = 417679330050262549730967902773056706769204590907920549790905313164765883718798498778729399201716067528829505703591869558941065895004395627923078418337259174212129372 61$

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

$N = 110780160868938860790802031427539545689163771392478000053424961714000133541302546723556824320392273338774914223428560224599935972614418186378966819098352285062648366902 3.$

Using Algorithm 2 for $t = 3$ $r = 3$ and $\beta = 0.75$ gives $\varrho = \frac{t(1-\beta)}{t+1} = 0.1875$ and $\varepsilon = \sqrt{2r}N^{\varrho+\beta-1} = 9.111089161 \times 10^{-39}$.
Applying Theorem 2.4 and using Algorithm 2 for $n = t = 3$, we compute

$$T = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}$$

$T = 1154165320000000000000000000000000000000000$
Consider the lattice $\mathcal{L}$ spanned by the matrix,

$$M = \begin{bmatrix} 1 & -[T(X_1)] & -[T(X_2)] & -[T \times X_3] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{bmatrix}$$

Therefore, by applying the LLL algorithm to $\mathcal{L}$, it yields the reduced basis with the following matrix

$$K = \begin{bmatrix} A_{11} & A_{12} & A_{13} & A_{14} \\ B_{11} & B_{12} & B_{13} & B_{14} \\ C_{11} & C_{12} & C_{13} & C_{14} \\ D_{11} & D_{12} & D_{13} & D_{14} \end{bmatrix}$$

where
$A_{11} = 77702944695646214262857290487 13,\ A_{12} = -11866076834029234002241236377582$
$A_{13} = -32633775130445983893911306068132,\ A_{14} = -33280824901442008630692923529 13$
$B_{11} = 18663562246576439716517789824933,\ B_{12} = 15048857017191042713184735691338$
$B_{13} = 10286010869239647472878709783788,\ B_{14} = 18549844424135999309545228522867$
$C_{11} = -17095263517456624755229311937397,\ C_{12} = -17505448553655077987743164400 42$
$C_{13} = -34574596282163621534726127220 92,\ C_{14} = 25713796499666717792079771007197$
$D_{11} = -11796372669551527880579978498483,\ D_{12} = 49475532903151632120923767998362$
$D_{13} = -35068780855417302192076780015 88,\ D_{14} = 25794295789469667887502782206 83.$

Next, from Algorithm 2, we compute $Q = KJ$,

$$Q = \begin{bmatrix} E_{11} & E_{12} & E_{13} & E_{14} \\ F_{21} & F_{22} & F_{23} & F_{24} \\ G_{31} & G_{32} & G_{33} & G_{34} \\ H_{41} & H_{24} & H_{43} & H_{44} \end{bmatrix}$$

where
$E_{11} = 77702944695646214262857290487 13,\ E_{12} = 23121915746594298457024824360 55$
$E_{13} = 32486241033126945250515990107 54,\ E_{14} = 33618053828189170577559203770 1$
$F_{21} = 18663562246576439716517789824933,\ F_{22} = 55536803075731848864083277393 49$
$F_{23} = 78029086806670615508451743719 10,\ F_{24} = 80747601353944792193225355638 4$
$G_{31} = -17095263517456624755229311937397,\ G_{32} = -50870046722773312723339638803 73$
$G_{33} = -71472304341644208929859488736 97,\ G_{34} = -73962382170715466592557117283 7$
$H_{41} = -11796372669551527880579978498483,\ H_{42} = -35102239181429742670400054092 44$
$H_{43} = -49318569246078306806002308361 38,\ H_{44} = 51036816292572652503909634871 5.$

From the second row of the matrix Q, it yields the values for d, k_1, k_2 and k_3 as follows:

$d = 18663562246576439716517789824933,\ k_1 = 55536803075731848864083277393 49$
$k_2 = 78029086806670615508451743719 10,\ k_3 = 80747601353944792193225355638 4.$

Using Algorithm 2, $\phi(N_s) = \frac{e_s d-1}{k_s}$ for $s = 1, 2, 3$ can be computed as follows,

$\phi(N_1) = 56338228137480385848938290371644347444657821557016451499919943564437595515683558642235304837245791250135951344035856352576613910331257682743324996840534419133508898 2588$

$\phi(N_2) = 11078016086893886079080203142753954568916350420128548912405458621486173567251534621700628102364318928358025354874774274406689185786711145616433025239686363424063920829 04$

$\phi(N_3) = 96540133016850160554005060983755948301371063111771234924523131194182141715371111214562914838512984578211413625756392936014365359380504038220596586504243032123344765916 8.$

Next, from Algorithm 2, p_s^{r-1} for $s = 1, 2, 3$ and $r = 3$ can be computed as follows,

$$\begin{aligned} p_1 &= 11720876728196985761402956937987 9515111959 \\ p_2 &= 12058019819639900134363121551161 50241125443 \\ p_3 &= 11655394061187804887158616519073008 62321907. \end{aligned}$$

Finally, from Algorithm 2, q_s for $s = 1, 2, 3$ can be computed as follows,

$$\begin{aligned} q_1 &= 34988303815617434955503783366716292472 6907 \\ q_2 &= 63187912974577270249788026409319467912 2189 \\ q_3 &= 60971518167998350136625385645645532757 9473. \end{aligned}$$

This shows the factorization of 3 prime power moduli $N_s = p_s^r q_s$ for $s = 1, 2, 3$ and $r = 3$ in polynomial time. One can also observe that , our work yield $d \approx N^{0.18608}$ which is greater than $d \approx N^{0.1857}$, as reported in [14]. This shows that Shehu and Ariffin's attack can not yield the factorization of t prime power moduli in our case.

3.2.2. *The Attack on t Prime Power Moduli $N_s = p_s^r q_s$ Satisfying System of Equation $e_s d_s - k\phi(N_s) = 1$.*

This section considers second case in which t prime power moduli satisfies equations of the form $e_s d_s - k\phi(N_s) = 1$ for unknown positive integers d_s and k for $s = 1, \ldots, t$. In this case, every pair of the instances (N_s, e_s) has its own unique decryption exponent d_s.

Theorem 3.4. *Let $N_s = p_s^r q_s$ be prime power moduli where p_s and q_s are prime numbers for $s = 1, \ldots, t$, $r, t \geq 2$. Let (e_s, N_s) be public key pair and (d_s, N_s) be private key pair with $e_s < \phi(N_s)$ and the relation $e_s d_s \equiv 1 \mod \phi(N_s)$ is satisfied. Let $e = \min\{e_s\} = N^{\alpha}$ be public exponent. If there exists t integers $d_s < N^{\varrho}$ and integer $k < N^{\varrho}$, for all $\varrho = \frac{t(\alpha-\beta)}{t+1}$ such that $e_s d_s - k\phi(N_s) = 1$ holds, then prime factors p_s and q_s of t prime power moduli N_s can be successfully recovered in polynomial time for $0 < \varrho \leq \frac{1}{2}$, $0 < \beta < 1$ and $\beta < \alpha < 1$.*

Proof. For $r, t \geq 2$ and $N_s = p_s^r q_s$, be t prime power moduli $e = \min\{e_s\} = N^{\alpha}$ be public exponent for $s = 1, \ldots t$ and suppose that $d_s < N^{\varrho}$. Then equation $e_s d_s - k\phi(N_s) = 1$ can be transformed into

$$e_s d_s - k(N_s - (N_s - \phi(N_s))) = 1$$

Let $\triangle = 2^{\frac{2r+1}{r+1}} N_s^{\frac{r}{r+1}}$

$$\begin{aligned} e_s d_s - k(N_s - \triangle + \triangle - (N_s - \phi(N_s))) &= 1 \\ e_s d_s - k(N_s - \triangle) &= 1 - k(N_s - \phi(N_s) - \triangle) \\ \left| k\frac{(N_s - \triangle)}{e_s} - d_s \right| &= \frac{|1 - k\,(N_s - \phi(N_s) - \triangle)|}{e_s}. \end{aligned}$$

Since $N = \max\{N_s\}$ and $d_s < N^{\varrho}$, $k < N^{\varrho}$ are positive integers. Observe

$$N_s - \phi(N_s) - \triangle < N_s^{\beta} < N^{\beta}$$

for $\beta \in (0, 1)$. Since also $e = \min\{e_s\} = N^{\alpha}$, for $s = 1, \cdots, t$ then it gives

$$\begin{aligned} \frac{|1 - k\,(N_s - \phi(N_s) - \triangle)|}{e_s} &\leq \frac{|1 + k\,(N_s - \phi(N_s) - \triangle)|}{e_s} \\ &< \frac{1 + N^{\varrho}(N^{\beta})}{N^{\alpha}} \\ &= \frac{1 + N^{\varrho+\beta}}{N^{\alpha}} \\ &< \sqrt{r} N^{\varrho+\beta-\alpha}. \end{aligned}$$

Hence,

$$\left| k\frac{(N_s - \triangle)}{e_s} - d_s \right| < \sqrt{r} N^{\varrho+\beta-\alpha}.$$

We proceed to show the existence of integer k and t integers d_s. Taking $\varepsilon = \sqrt{r}N^{\varrho+\beta-\alpha}$ and $\varrho = \frac{t(\alpha-\beta)}{t+1}$. Then it gives

$$N^{\varrho}\varepsilon^t = N^{\varrho}\left(\sqrt{r}N^{\varrho+\beta-\alpha}\right)^t = (\sqrt{r})^t N^{\varrho+\varrho t+\beta t-\alpha t} = r^{\frac{t}{2}}.$$

Following Theorem 2.4, $r^{\frac{t}{2}} < 2^{\frac{t(t-3)}{4}} \cdot 3^t$ for $r, t \geq 2$, then it gives $N^{\varrho}\varepsilon^t < 2^{\frac{t(t-3)}{4}} \cdot 3^t$. It follows that if $k < N^{\varrho}$ then $k < 2^{\frac{t(t-3)}{4}} \cdot 3^t \cdot \varepsilon^{-t}$ for $s = 1, \ldots, t$, yields

$$\left| k\frac{(N_s - \triangle)}{e_s} - d_s \right| < \varepsilon.$$

This clearly satisfies the conditions of Theorem 2.4, and proceeds to reveal the private keys k and t integers d_s for $s = 1, \ldots, t$. Next from $e_s d_s - k\phi(N_s) = 1$ we make the following computations :

$$\begin{aligned} \phi(N_s) &= \frac{e_s d_s - 1}{k} \\ p_s^{r-1} &= \gcd(\phi(N_s), N_s) \\ q_s &= \frac{N_s}{p_s^r}. \end{aligned}$$

Finally, the prime factors p_s and q_s can be revealed which lead to the factorization of t prime power moduli N_s for $s = 1, \ldots, t$ and $r \geq 2$. □

Let

$$\begin{aligned} X_1 &= \frac{N_1 - 2^{\frac{2r+1}{r+1}} N_1^{\frac{r}{r+1}}}{e_1} \\ X_2 &= \frac{N_2 - 2^{\frac{2r+1}{r+1}} N_2^{\frac{r}{r+1}}}{e_2} \\ X_3 &= \frac{N_3 - 2^{\frac{2r+1}{r+1}} N_3^{\frac{r}{r+1}}}{e_3}. \end{aligned}$$

Define,

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

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

$$M = \begin{bmatrix} \mathbf{1} & -[T(X_1)] & -[T(X_2)] & -[T(X_3)] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{bmatrix}$$

Taking $r \geq 2$, the matrix M can be used in computing the reduced basis after applying the LLL algorithm

Algorithm 3 Theorem 3.4

Initialization: The public key tuple $(N_s, e_s, \alpha, \beta, \varrho)$ satisfying Theorem 3.4.
Choose $r \geq 2$ and $N = \max\{N_s\}$ for $s = 1, \ldots, t$.
for any $(r, N, \alpha, \beta, \varrho)$ **do**
    $\varepsilon = \sqrt{r} N^{\varrho+\beta-\alpha}$
    $e =: \min\{e_s\} := N^{\alpha}$
    $T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}]$ for $t \geq 2$.
end for
Consider the lattice $\mathcal{L}$ spanned by the matrix M as stated above.
Applying the LLL algorithm to $\mathcal{L}$ yields the reduced basis matrix K.
for any (M, K) **do**
    $J := M^{-1}$
    $Q = JK$.
end for
Produce d_s, k from Q
for each triplet (d_s, k, e_s) **do**
    $\phi(N_s) := \frac{e_s d_s - 1}{k}$
    $p_s^{r-1} := \gcd(\phi(N_s), N_s)$.
    $q_s := \frac{N_s}{p_s^r}$
end for
return the prime factors (p_s, q_s).

Example 3.3. *This example gives an illustration of how Theorem 3.4 works on 3 prime power moduli and their corresponding public exponents:*

$N_1 = 230752430767013072249887684293910718837040040071399248283866636915143445411611467379$

$N_2 = 434991743050236060915996189147523264755865914949477613614468188806740952003913552583$

$N_3 = 980914643623371382312729458097187264388503427621447777571718784533143406738292636683$

$e_1 = 629049148810559949841785049761568215700026226807264231457363256802126488638937888039$

$e_2 = 265035571511591897022174737291070924314658140619585199620247165205557379598308572799$

$e_3 = 424302253973827276427319770823031080967261427337097513012296323366084850555293675453.$

Observe

$N = \max\{N_1, N_2, N_3\} = 980914643623371382312729458097187264388503427621447777571718784533143406738292636683$

$e = \min\{e_1, e_2, e_3\} = 629049148810559949841785049761568215700026226807264231457363256802126488638937888039$

with $e = \min\{e_1, e_2, e_3\} = N^{\alpha}$ for $\alpha = 0.9857968390$. Taking $t = 3$, $\beta = 0.75$ it gives $\varrho = \frac{t(\alpha-\beta)}{t+1} = 0.1768476292$ and $\varepsilon = 0.00001937850804$.
Applying Theorem 2.4 and using Algorithm 3, we compute

$$T = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}] = 287192882900000000000.$$

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

$$M = \begin{bmatrix} \mathbf{1} & -[T(X_1)] & -[T(X_2)] & -[T(X_3)] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{bmatrix}$$

Therefore, by applying the LLL algorithm to $\mathcal{L}$, it yields the reduced basis with the following matrix

$$K = \begin{bmatrix} -64528041013590 & 22316660983540 & -14660675253070 & -23287047712390 \\ -833898253680997 & -1831141920267418 & -628510813959081 & 1059071291894963 \\ 509570466489060 & -4655727886202360 & -481050100124620 & -5658983802111740 \\ 5843566312885470 & 3758022552321180 & -17342920355447690 & -1610120341214130 \end{bmatrix}$$

Next, from Algorithm 3, we compute $Q = KJ$,

$$Q = \begin{bmatrix} -64528041013590 & -236706501307159 & -105907161352079 & -149177855554037 \\ -833898253680997 & -3058966845644782 & -1368642151792744 & -1927830928699482 \\ 509570466489060 & 1869243826365026 & 836336587427863 & 1178040248091503 \\ 5843566312885470 & 21435799310693196 & 9590799761610551 & 13509331410827634 \end{bmatrix}$$

From the first row of matrix Q, it yields the values for $k,\ d_1,\ d_2$ and d_3 as follows:

$$k = 64528041013590,\ d_1 = 236706501307159,$$
$$d_2 = 105907161352079,\ d_3 = 149177855554037.$$

Using Algorithm 3, $\phi(N_s) = \frac{e_s d_s - 1}{k}$ for $s = 1, 2, 3$ can be computed as follows,

$$\begin{aligned} \phi(N_1) = {} & 230752430767013072248776543267470057677453472488988696401562070407244760015236527680 \\ \phi(N_2) = {} & 434991743050236060914973940031031094365510983789392873571099791027040771533822542568 \\ \phi(N_3) = {} & 980914643623371382310759325156502208018839297372581980030651478359865012354849827664. \end{aligned}$$

Next, from Algorithm 3, p_s^{r-1} for $s = 1, 2, 3$ and $r = 3$ can be computed as follows,

$$p_1 = 954408180105791988011,\ p_2 = 770755872323270534549,$$
$$p_3 = 994602670246108900363.$$

Finally, from Algorithm 3, q_s for $s = 1, 2, 3$ can be computed as follows,

$$q_1 = 265426222155632917409,\ q_2 = 950015052524020374467,$$
$$q_3 = 996970609016663314889.$$

This shows the factorization of 3 prime power moduli $N_s = p_s^r q_s$ for $s = 1, 2, 3$ and $r = 3$ in polynomial time. Also, one can observe that our work yield $\min(d_1, d_2, d_3) \approx N^{0.1669}$ which is greater than $d \approx N^{0.1319}$, as reported in [14]. This shows that Shehu and Ariffin's attack can not yield the factorization of t prime power moduli in this case.

3.2.3. *The Attack on t Prime Power Moduli $N_s = p_s^r q_s$ Satisfying System of Equation $e_s d - k_s \phi(N_s) = z_s$.*

This section considers another case in which t prime power moduli satisfies equations of the form $e_s d - k_s \phi(N_s) = z_s$ for unknown positive integers $d,\ k_s,$ and z_s for $s = 1, \ldots, t$.
Taking $r \geq 2$, let $N_s = p_s^r q_s,\ s = 1, \ldots, t$. The attack works for t instances (N_s, e_s) when there exists integer d and t integers k_s such that $e_s d - k_s \phi(N_s) = z_s$ is satisfied. The attack shows that t prime factors p_s and q_s of t prime power moduli $N_s = p_s^r q_s$ for $s = 1, ..., t$ can be found efficiently for $N = \max\{N_s\}$ and $d < N^{\varrho},\ k_s < N^{\varrho},\ z_s < N^{\varrho},$ for all $\varrho = \frac{t(1-\beta)}{t+1}$ for $0 < \varrho \leq \frac{1}{2}$ and $o < \beta < 1$. In this case, the instances (N_s, e_s) shared common decryption exponent d.

Theorem 3.5. *Let $N_s = p_s^r q_s$ be t prime power moduli for $r \geq 2$ where p_s and q_s are prime numbers for $s = 1 \ldots, t$. Let (e_s, N_s) be public key pair and (d, N_s) be private key pair with condition $e_s < \phi(N_s)$ and relation $e_s d \equiv z_s \mod \phi(N_s)$ is satisfied. Let $N = \max\{N_s\}$. If there exists positive integer $d < N^{\varrho}$, t integers $k_s < N^{\varrho}$ and $z_s < N^{\varrho}$, for all $\varrho = \frac{t(1-\beta)}{t+1}$ such that equation $e_s d - k_s \phi(N_s) = z_s$ holds, then prime factors p_s and q_s of t prime power moduli N_s can be successfully recovered in polynomial time for $0 < \varrho \leq \frac{1}{2}$ and $o < \beta < 1$.*

Proof. Suppose $N_s = p_s^r q_s$ be t prime power moduli, $N = \max\{N_s\}$ and $k_s < N^{\varrho}$ for $r \geq 2$ and $s = 1, \ldots, t$. Then equation $e_s d - k_s \phi(N_s) = z_s$ can be rewritten as:

$$e_s d - k_s (N_s - (N_s - \phi(N_s)) = z_s.$$

Let $\triangle = 2^{\frac{2r+1}{r+1}} N_s^{\frac{r}{r+1}}$

$$e_s d - k_s \left(N_s - \triangle + \triangle - (N_s - \phi(N_s))\right) = z_s$$
$$e_s d - k_s (N_s - \triangle) = z_s - k_s (N_s - \phi(N_S) - \triangle)$$

$$\left| \frac{e_s}{N_s - \triangle} d - k_s \right| = \frac{|z_s - k_s (N_s - \phi(N_S) - \triangle)|}{N_s - \triangle}. \tag{3.2}$$

Since $N = \max\{N_S\}$ and $k_s < N^{\varrho}$, $z_s < N^{\varrho}$ are positive integers. Observe

$$|N_s - \phi(N_S) - \triangle| < N_s^{\beta} < N^{\beta}$$
$$N_s - \triangle > \frac{\sqrt{r+1}}{r} N$$

for $\beta \in (0,1)$. Then plugging the conditions into equation (3.2) yields

$$\begin{aligned}\frac{|z_s - k_s(N_s - \phi(N_S) - \triangle)|}{N_s - \triangle} &\leq \frac{|z_s + k_s(N_s - \phi(N_S) - \triangle)|}{N_s - \triangle} \\ &< \frac{N^{\varrho} + N^{\varrho}(N^{\beta})}{\frac{\sqrt{r+1}}{r}N} \\ &= \frac{r(N^{\varrho} + N^{\varrho+\beta})}{\sqrt{r+1}N} \\ &< \sqrt{2r+1}N^{\varrho+\beta-1}.\end{aligned}$$

Hence,

$$\left|\frac{e_s}{N_s - \triangle}d - k_s\right| < \sqrt{2r+1}N^{\varrho+\beta-1}.$$

We proceed to show the existence of an integer d, let $\varepsilon = \sqrt{2r+1}N^{\varrho+\beta-1}$, for $\varrho = \frac{t(1-\beta)}{t+1}$. Then it gives

$$N^{\varrho}\varepsilon^t = N^{\varrho}\left(\sqrt{2r+1}N^{\varrho+\beta-1}\right)^t = \left(\sqrt{2r+1}\right)^t N^{\varrho+\varrho t+\beta t-t} = (2r+1)^{\frac{t}{2}}.$$

Following Theorem 2.4, $(2r+1)^{\frac{t}{2}} < 2^{\frac{t(t-3)}{4}} \cdot 3^t$ for $r, t \geq 2$, then it gives $N^{\varrho}\varepsilon^t < 2^{\frac{t(t-3)}{4}} \cdot 3^t$. It follows that if $d < N^{\varrho}$, then $d < 2^{\frac{t(t-3)}{4}} \cdot 3^t \cdot \varepsilon^{-t}$ for $s = 1, \ldots, t$, yields

$$\left|\frac{e_s}{N_s - \triangle}d - k_s\right| < \varepsilon.$$

This clearly satisfies the conditions of Theorem 2.4, and proceeds to reveal the private key d and t integers k_s for $s = 1, \ldots, t$. Next, from $e_s d - k_s\phi(N_s) = z_s$, we make the following computations:

$$\begin{aligned}\phi(N_s) &= \frac{e_s d - z_s}{k_s} \\ p_s^{r-1} &= \gcd(\phi(N_s), N_s) \\ q_s &= \frac{N_s}{p_s^r}.\end{aligned}$$

Finally, the prime factors p_s and q_s can be revealed which lead to the factorization of t prime power moduli $N_s = p_s^r q_s$ for $r \geq 2$ and $s = 1, \ldots, t$ in polynomial time. □

Let

$$\begin{aligned}X_1 &= \frac{e_1}{N_1 - 2^{\frac{2r+1}{r+1}}N_1^{\frac{r}{r+1}}}, \; X_2 = \frac{e_2}{N_2 - 2^{\frac{2r+1}{r+1}}N_2^{\frac{r}{r+1}}}, \\ X_3 &= \frac{e_3}{N_3 - 2^{\frac{2r+1}{r+1}}N_3^{\frac{r}{r+1}}}.\end{aligned}$$

Define,

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

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

$$M = \begin{bmatrix} 1 & -[T(X_1)] & -[T(X_2)] & -[T \times X_3] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{bmatrix}$$

Taking $r \geq 2$, the matrix M can be used in computing the reduced basis after applying the LLL algorithm.

Algorithm 4 Theorem 3.5

Initialization: The public key tuple $(N_s, e_s, \varrho, \beta)$ satisfying Theorem 3.5.
Choose $r \geq 2$ and $N = \max\{N_s\}$ for $s = 1, \ldots, t$.
for any (r, N, ϱ, β) **do**
    $\varepsilon := \sqrt{2r+1} N^{\varrho+\beta-1}$
    $T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}]$ for $t \geq 2$.
end for
Consider the lattice $\mathcal{L}$ spanned by the matrix M as stated above.
Applying the LLL algorithm to $\mathcal{L}$ yields the reduced basis matrix K.
for any (M, K) **do**
    $J := M^{-1}$
    $Q = JK$.
end for
Produce d, k_s from Q
for each tuple (d, k_s, e_s, z_s) **do**
    $\phi(N_s) := \frac{e_s d - z_s}{k_s}$
    $p_s^{r-1} := \gcd(\phi(N_s), N_s)$.
    $q_s := \frac{N_s}{p_s^r}$
end for
return the prime factors (p_s, q_s).

Example 3.4. *This example gives an illustration of how Theorem 3.5 works on 3 prime power moduli and their corresponding public exponents:*

$$\begin{aligned}
\textit{Let } N_1 &= 552589083079296395582963537637258987710502984397243532808096725056837793945542263311852509300451 \\
N_2 &= 409009336956200004848526206159753677602922864786417839660443537581155477440303212646889912922681 \\
N_3 &= 185659991588494772190286490085248886795864584720306578938229732631116403569017708089856336697379 \\
e_1 &= 535660672991610223946156685795497788662147614731651359062338800947852331357924924200110870181597 \\
e_2 &= 398146646185722474414615357316831702372730383621128736712077969303212977619132096891312620129374 \\
e_3 &= 209451368450111882047031899410363595522073297167725702489117049064722361040283841327245761880 13.
\end{aligned}$$

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

$$N = 552589083079296395582963537637258987710502984397243532808096725056837793945542263311852509300451.$$

Using Algorithm 4 for $t = 3$ $r = 3$ and $\beta = 0.75$ gives $\varrho = \frac{t(1-\beta)}{t+1} = 0.1875$ and $\varepsilon = \sqrt{7}N^{\gamma+\beta-1} = 0.000002745673398$.
Applying Theorem 2.4 and using Algorithm 4 for $n = t = 3$, we compute

$$T = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}] = 712622481500000000000000.$$

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

$$M = \begin{bmatrix} 1 & -[T(X_1)] & -[T(X_2)] & -[T \times X_3] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{bmatrix}$$

Therefore, by applying the LLL algorithm to $\mathcal{L}$, it yields the reduced basis with the following matrix

$$K = \begin{bmatrix} 240575049922396781 & 45168467894653961 & -38707598398094518 & 195092642719432714 \\ -151248559543325924 & -488046878955018644 & 707575095426884472 & 620320224274381944 \\ -574956937086078187 & 491431650385399953 & -786566357699210214 & 209783791280367322 \\ -89655203762229785 & -1063060408191942085 & -430492105618860770 & 168843844246479710 \end{bmatrix}$$

Next, from Algorithm 4, we compute $Q = KJ$,

$$Q = \begin{bmatrix} 240575049922396781 & 233205101389831407 & 234185727874526165 & 27140351020204693 \\ -151248559543325924 & -146615102749620456 & -147231618648953995 & -17063028766409243 \\ -574956937086078187 & -557343294124629361 & -559686920366201207 & -64863472330366436 \\ -89655203762229785 & -86908641981956074 & -87274092461248535 & -10114405885730059 \end{bmatrix}$$

From the first row of matrix Q, it yields the values for k, d_1, d_2 and d_3 as follows:

$$d = 240575049922396781,\ k_1 = 233205101389831407,$$
$$k_2 = 234185727874526165,\ k_3 = 27140351020204693.$$

Using Algorithm 4, $\phi(N_s) = \frac{e_s d - z_s}{k_s}$ for $s = 1, 2, 3$ can be computed as follows, where z_1, z_2, z_3 are :

$$z_1 = 12594844191468409,\ z_2 = 7690976311642434,\ z_3 = 18446004731332273$$
$$\phi(N_1) = 552589083079296395582961635823819347184701123613286126361334990579765661347407538020846597914464$$
$$\phi(N_2) = 409009336956200004848524825976621275030379645558289047131769573374160014405441556077741716001204$$
$$\phi(N_3) = 185659991588494772190285551403327968148144196253737749368311956715037950804743239281977597971160.$$

Next, from Algorithm 4, p_s^{r-1} for $s = 1, 2, 3$ and $r = 3$ can be computed as follows,

$$p_1 = 112105281561818170503691307,\ p_2 = 988706976202053289655339,$$
$$p_3 = 901538558587875149528599.$$

Finally, from Algorithm 4, q_s for $s = 1, 2, 3$ can be computed as follows,

$$q_1 = 392214892049653107897457,\ q_2 = 423185157151460671796099,$$
$$q_3 = 253375960517480945644421.$$

This shows the factorization of 3 prime power moduli $N_s = p_s^r q_s$ simultaneously for $r \geq 2$ and $s = 1, \ldots, t$. From our result, one can also observe that our work yields $d \approx N^{0.18154}$. The equation $e_s d - k_s \phi(N_s) = z_s$ is a generalization of equation $e_i d - k_i \phi(N_i) = 1$, as reported in [14].

3.2.4. *The Attack on t Prime Power Moduli $N_s = p_s^r q_s$ Satisfying System of Equation $e_s d_s - k\phi(N_s) = z_s$.*

This section presents another cryptanalysis attack in which t prime power moduli $N_s = p_s^r q_s$ satisfies equations of the form $e_s d_s - k\phi(N_s) = z_s$ for unknown positive integers $d_s,\ k,$ and z_s for $s = 1, \ldots, t$ and $r \geq 2$ which can be simultaneously factored in polynomial time. In this case, every pair of the instances (N_s, e_s) has its own unique decryption exponent d_s.

Theorem 3.6. *Let $N_s = p_s^r q_s$ be t prime power moduli where p_s and q_s are prime numbers for $s = 1, \ldots, t$ and $t \geq 3$. Let (e_s, N_s) be public key pair and (d_s, N_s) be private key pair with $e_s < \phi(N_s)$ and relation $e_s d_s \equiv z_s \mod \phi(N_s)$ is satisfied. Let $e = \min\{e_s\} = N^\alpha$ be public exponent. If there exists positive t integers $d_s < N^\varrho$, integer $k < N^\varrho$ and t integers $z_s < N^\varrho$, for all $\varrho = \frac{t(\alpha-\beta)}{t+1}$ such that equation $e_s d_s - k\phi(N_s) = z_s$ holds, then prime factors p_s and q_s of t prime power moduli $N_s = p_s^r q_s$ for N_s and $r \geq 2$ can be successfully recovered in polynomial time for $0 < \varrho \leq \frac{1}{2}$, $0 < \beta < 1$ and $\beta < \alpha < 1$.*

Proof. Suppose $N_s = p_s^r q_s$ be t prime power moduli and $e = \min\{e_s\} = N^\alpha$ be public exponent for $s = 1, \ldots t$ and suppose that $d_s < N^\varrho$, for $r \geq 2$ and $t \geq 3$. Then equation $e_s d_s - k\phi(N_s) = z_s$ can be rewritten as

$$e_s d_s - k(N_s - (N_s - \phi(N_s))) = z_s.$$

Let $\triangle = 2^{\frac{2r+1}{r+1}} N_s^{\frac{r}{r+1}}$

$$e_s d_s - k(N_s - \triangle + \triangle - (N_s - \phi(N_s))) = z_s$$
$$e_s d_s - k\left(N_s - \triangle\right) = z_s - k(N_s - \phi(N_s) - \triangle)$$
$$\left| k\frac{(N_s - \triangle)}{e_s} - d_s \right| = \frac{|z_s - k(N_s - \phi(N_s) - \triangle)|}{e_s}.$$

Since $N = \max\{N_s\}$ and $d_s < N^\varrho$, $k < N^\varrho$, $z_s < N^\varrho$. Observe

$$|N_s - \phi(N_s) - \triangle| < N_s^\beta < N^\beta$$

for $\beta \in (0, 1)$. Also since $e = \min\{e_s\} = N^\alpha$, for $s = 1, \ldots t$ then it gives

$$\begin{aligned}\frac{|z_s - k(N_s - \phi(N_s) - \triangle)|}{e_s} \leq & \frac{|z_s + k(N_s - \phi(N_s) - \triangle)|}{e_s} \\ & < \frac{N^{\varrho} + N^{\varrho}(N^{\beta})}{N^{\alpha}} \\ & = \frac{N^{\varrho} + N^{\varrho+\beta}}{N^{\alpha}} \\ & < \sqrt{r+2}N^{\varrho+\beta-\alpha}.\end{aligned}$$

Hence,

$$\left| k\frac{(N_s - \triangle)}{e_s} - d_s \right| < \sqrt{r+2}N^{\varrho+\beta-\alpha}.$$

We proceed to show the existence of integer k and t integers d_s. Let $\varepsilon = \sqrt{r+2}N^{\varrho+\beta-\alpha}$ and $\varrho = \frac{t(\alpha-\beta)}{t+1}$. Then it gives

$$N^{\varrho}\varepsilon^t = N^{\varrho}\left(\sqrt{r+2}N^{\varrho+\beta-\alpha}\right)^t = (\sqrt{r+2})^t N^{\varrho+\beta t-\alpha t} = (r+2)^{\frac{t}{2}}.$$

Following Theorem 2.4, $(r+2)^{\frac{t}{2}} < 2^{\frac{t(t-3)}{4}} \cdot 3^t$ for $r, t \geq 2$, then $N^{\varrho}\varepsilon^t < 2^{\frac{t(t-3)}{4}} \cdot 3^t$. It follows that if $k < N^{\varrho}$ then $k < 2^{\frac{t(t-3)}{4}} \cdot 3^t \cdot \varepsilon^{-t}$ for $s = 1, \ldots, t$, yields

$$\left| k\frac{(N_s - \triangle)}{e_s} - d_s \right| < \varepsilon.$$

This clearly satisfies the conditions of Theorem 2.4, and proceeds to reveal the private keys t integers d_s and k for $s = 1, \ldots, t$. Next, from $e_s d_s - k\phi(N_s) = z_s$ we make the following computations:

$$\begin{aligned}\phi(N_s) &= \frac{e_s d_s - z_s}{k} \\ p_s^{r-1} &= \gcd(\phi(N_s), N_s) \\ q_s &= \frac{N_s}{p_s^r}.\end{aligned}$$

Finally, the prime factors p_s and q_s can be revealed which lead to the factorization of t prime power moduli N_s for $s = 1, \cdots, t$ in polynomial time. □

Let

$$X_1 = \frac{(N_1 - 2^{\frac{2r+1}{r+1}} N_1^{\frac{r}{r+1}}) + 1}{e_1},\ X_2 = \frac{(N_2 - 2^{\frac{2r+1}{r+1}} N_2^{\frac{r}{r+1}}) + 1}{e_2},\ X_3 = \frac{(N_3 - 2^{\frac{2r+1}{r+1}} N_3^{\frac{r}{r+1}}) + 1}{e_3}.$$

Define,

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

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

$$M = \begin{bmatrix} \mathbf{1} & -[T(X_1)] & -[T(X_2)] & -[T(X_3)] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{bmatrix}$$

Taking $r \geq 2$, the matrix M can be used in computing the reduced basis after applying the LLL algorithm

Algorithm 5 Theorem 3.6

Initialization: The public key tuple $(N_s, e_s, \alpha, \beta, \varrho)$ satisfying Theorem 3.6.
Choose $r \geq 2$ and $N = \max\{N_s\}$ for $s = 1, \ldots, t$.
for any $(r, N, \alpha, \beta, \varrho)$ **do**
    $\varepsilon = \sqrt{r+2} N^{\varrho+\beta-\alpha}$
    $e =: \min\{e_s\} := N^{\alpha}$
    $T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}]$ for $t \geq 2$.
end for
Consider the lattice $\mathcal{L}$ spanned by the matrix M as stated above.
Applying the LLL algorithm to $\mathcal{L}$ yields the reduced basis matrix K.
for any (M, K) **do**
    $J := M^{-1}$
    $Q = JK$.
end for
Produce d_s, k from Q
for each triplet (d_s, k, e_s, z_s) **do**
    $\phi(N_s) := \frac{e_s d_s - z_s}{k}$
    $p_s^{r-1} := \gcd(\phi(N_s), N_s)$.
    $q_s := \frac{N_s}{p_s^r}$
end for
return the prime factors (p_s, q_s).

Example 3.5. *This example gives an illustration of how Theorem 3.6 works on 3 prime power moduli and their corresponding public exponents:*

$$N_1 = 118206700499027973555226065271614027133355822416165333781707131772561895107920252379$$

$$N_2 = 153187267586393370493787125781781250360337971520690436340144738974644921936384902153$$

$$N_3 = 924899290347826697102573577323286044355305745566432529788292084959590562885708269169$$

$$e_1 = 944721701896524093348103370244093137009660979547777813024924191503242413565332231 23$$

$$e_2 = 925995466598943224506439532320239713941284965387703819238402532258026161689224667 97$$

$$e_3 = 629828696197243558343755829089787763417070253274519076605922408153811221100854704887.$$

Observe

$$N = \max\{N_1, N_2, N_3\} = 924899290347826697102573577323286044355305745566432529782928420849595905628857082691 69$$

$$e = \min\{e_1, e_2, e_3\} = 925995466598943224506439532320239713941284965387703819238402532258026161689224667 97$$

with $e = \min\{e_1, e_2, e_3\} = N^{\alpha}$ for $\alpha = 0.9880965575$. Taking $t = 3$, $\beta = 0.75$ it gives $\varrho = \frac{t(\alpha-\beta)}{t+1} = 0.1785724181$,$\varepsilon = 0.00002246340004$.
Applying Theorem 2.4 and using Algorithm 5, we compute

$$C = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}] = 159057099200000000000.$$

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

$$M = \begin{bmatrix} \mathbf{1} & -[T(X_1)] & -[T(X_2)] & -[T(X_3)] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{bmatrix}$$

Therefore, by applying the LLL algorithm to $\mathcal{L}$, it yields the reduced basis with the following matrix

$$K = \begin{bmatrix} -192479622515690 & -477895645520 & -115255751942450 & 123625906116600 \\ 300578256728925 & 1229934560231400 & -602650460625375 & 38597963550500 \\ -1282731106006613 & 354397216043096 & -475121843615865 & -2396325179490180 \\ 1337229767906843 & -1481780789001256 & -3446686105094985 & -1015254431182020 \end{bmatrix}$$

Next, from Algorithm 5, we compute $Q = KJ$,

$$Q = \begin{bmatrix} -192479622515690 & -240836862805235 & -318418701848887 & -282655057392665 \\ 300578256728925 & 376093445279694 & 497246082783771 & 441397189459762 \\ -1282731106006613 & -1604995538518056 & -2122019818292808 & -1883682177099557 \\ 1337229767906843 & 1673186064806441 & 2212176859064010 & 1963713103001738 \end{bmatrix}$$

From the first row of matrix Q, it yields the values for k, d_1, d_2 and d_3 as follows:

$$k = 192479622515690, d_1 = 240836862805235,$$
$$d_2 = 318418701848887,\ d_3 = 282655057392665.$$

Using Algorithm 5, $\phi(N_s) = \frac{e_s d_s - z_s}{k}$ for $s = 1, 2, 3$ can be computed as follows, where z_1, z_2, z_3 are :

$$z_1 = 125587188015385, z_2 = 213104320451339, z_3 = 223377252772855$$

$$\begin{aligned} \phi(N_1) &= 11820670049902797355481221322408897920442751821218512043829912018031086126906939320 8 \\ \phi(N_2) &= 15318726758639337049331746232391674144929515448559432423497865399547577916624799544 0 \\ \phi(N_3) &= 92489929034782669710021054527475913748082630652189351887545856298944763886324402490 0. \end{aligned}$$

Next, from Algorithm 5, p_s^{r-1} for $s = 1, 2, 3$ and $r = 3$ can be computed as follows,

$$p_1 = 601114833736581054997,\ p_2 = 601114833736581054997,$$
$$p_3 = 1161433282369002470551.$$

Finally, from Algorithm 5, q_s for $s = 1, 2, 3$ can be computed as follows,

$$q_1 = 544214062088679626023,\ q_2 = 718297824560170977461,$$
$$q_3 = 590352823628934085319.$$

This shows the factorization of 3 prime power moduli $N_s = p_s^r q_s$ simultaneously for $r \geq 2$ and $s = 1, \ldots, t$. From our result, one can also observe that our work yields $\min(d_1, d_2, d_3) \approx N^{0.1712}$. The equation $e_s d_s - k\phi(N_s) = z_s$ is a generalization of equation $e_i d_i - k\phi(N_i) = 1$, as reported in [14].

4. Conclusion

In this paper, we developed new technique that led to the successful factorization of prime power modulus $N = p^r q$ for $r \geq 2$ via good approximation of $\phi(N)$. The paper also showed that using $N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil$ as good approximation of $\phi(N)$ led to the extension of the bound to susceptible decryption exponent. The paper also presented four cryptanalysis attacks that successfully factored t prime power moduli $N_s = p_s^r q_s$ for $s = 1, \ldots, t$ using generalized key equations of the form $e_s d - k_s\phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s\phi(N_s) = z_s$ and $e_s d_s - k\phi(N_s) = z_s$. It has improved susceptible decryption exponent bounds of [14] from $d \approx N^{0.1857}$ to $d \approx N^{0.1863}$ and from $\min\{d_i\} \approx N^{0.1319}$ to $\min\{d_s\} \approx N^{0.1669}$. From these results, the paper generalized key equations of [14] from $e_i d - k_\phi(N_i) = 1$ to $e_s d - k_s\phi(N_s) = z_s$ and also from $e_i d_i - k\phi(N_i) = 1$ to $e_s d_s - k\phi(N_s) = z_s$.

References

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

[2] M. K. Dubey, N. Ratan, R. Verma, N. Saxena, *Cryptanalytic attacks and countermeasures on RSA*, in: P. K. (2014), In Proceedings of the Third International Conference on Soft Computing for Problem Solving, Springer, (2014), 10–18. .

[3] T. Fujioka, A. Okamoto, S. Miyaguchi, ESIGN, *An effient digital signature implementation for smart cards*, Advances in Cryptology EUROCRYPT 91, Lecture Notes in Computer Science, Springer, (1991), 446–457.

[4] T. Okamoto, S. Uchiyama, *A new public-key cryptosystem as secure as factoring*, in: Advances in Cryptology EUROCRYPT'98, Lecture Notes in Computer Science, Springer, (1998), 308–318.

[5] T. Takagi, *Fast RSA-type cryptosystem modulo $p^k q$*, in: Advances in Cryptology CRYPTO '98. CRYPTO 1998, Lecture Notes in Computer Science, Springer, (1998), 318–326.

[6] A. May, *Secret exponent attacks on RSA-type schemes with moduli $N = p^r q$*, in: Public Key Cryptography-PKC 2004, Springer, (2004), 218–230.

[7] S. Sarkar, *Small secret exponent attack on RSA variant with modulus $N = p^2 q$*, in: Proceedings International Workshop on Coding and Cryptography-WCC2013 Norway and INRIA, (2013), 215–222.

[8] R. Lu, Y. Zhang, D. Lin, *New results on solving linear equations modulo unknown divisors and its applications*, IACR Cryptology eprint **1** (2014) 343–354.

[9] S. Sarkar, *Revisiting prime power RSA*, Discrete Applied Mathematics **203**(C) (2016) 127–133.

[10] K. Itoh, K. Kunihiro, K. Kurosawa, *Small secret key attack on a variant of RSA (due to takagi)*, in: CT-RSA 2008, in:LNCS, (2008), 387–406.

[11] J. Blomer, A. May, *A generalized Wiener attack on RSA*, in: International Workshop on Public Key Cryptography, Springer, (2004), 1-13.

[12] J. Hinek, *On the security of some variants of RSA*, Phd thesis, Universiti Waterloo, Ontario, Canada (2007).

[13] A. Nitaj, M. Ariffin, D. Nassr, H. Bahig, *New Attacks on the RSA cryptosystem*, in: Progress in Cryptology AFRICACRYPT 2014. Lecture Notes in Computer Science, **8469**, Springer, (2014), 178-198.

[14] S. Shehu, M.R.K Ariffin, *New attacks on prime power RSA $N = p^r q$ using good approximation of $\phi(N)$*, Malaysian Journal of Mathematical Sciences special issues:The 5th International Cryptology and Information Security Conference(New Ideas in) **11**(S) (2017) 121–138.

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

[16] A. Nitaj, *Diophantine and lattice cryptanalysis of the RSA cryptosystem*, in: Artificial Intelligence, Evolutionary Computing and Metaheuristics, Springer, (2013), 139-168.

[17] X. Wang, X. G., M. Wang, X. Meng, Mathematical Foundations of Public Key Cryptography, CRC Press, Boca Rating London New York, 2016.

Saidu Isah Abubakar,
Department of Mathematics, Sokoto State University , Sokoto, :+2348069191131, Orcid number:0000-0002-0201-0064
Email address: siabubakar82@gmail.com

Zaid Ibrahi,
Department of Mathematics, Sokoto State University, Sokoto ,+2348035780166: Orcid number:0000-0002-0251-6495
Email address: malamzaid2@gmail.com

Sadiq Shehu,
Department of Mathematics, Sokoto State University , Sokoto, +2348066284440: Orcid number:0000-0001-5908-7452
Email address: sadiqshehuzezi@gmail.com

Ahmad Rufai,
Department of Mathematics, Sokoto State University , Sokoto, +2347068272590: Orcid number:0000-0003-3223-9924
Email address: rufaiahmad35@yahoo.com