New Trends in Mathematical Sciences

http://dx.doi.org/10.20852/ntmsci.2022.464

Cryptanalysis Attacks for Factoring Generalized Takagi's Scheme $N = p^r q^s$

Sadiq Shehu and Saidu Isah Abubakar

Department of Mathematics, Faculty of Science, Sokoto State University PMB 2134, Sokoto, Nigeria

Received: 25 December 2021 , Accepted: 31 January 2022
Published online: 13 March 2022

Abstract: This paper develops new strategies of factoring prime power moduli $N = p^r q^s$ also as known Generalized Takagi's scheme using method of continued fraction for $2 \leq s < r$. The paper proves that using an approximation of $\phi(N) = N + N^{\frac{r+s-2}{2r}} - 2N^{\frac{r+s-1}{2r}}$, private keys $\frac{k}{d}$ can be found from the convergents of the continued fractions expansion of $\frac{e}{N+N^{\frac{r+s-2}{2r}}-2N^{\frac{r+s-1}{2r}}}$ which leads to the factorization of the moduli $N = p^r q^s$ in polynomial time . The paper further reports two cryptanalysis attacks which exploit the security of the cryptosystem $N_i = p_i^r q_i^s$ by solving generalized key equations of the type $e_i d - k_i \phi(N_i) = 1$ and $e_i d_i - k\phi(N_i) = 1$ using simultaneous Diophantine approximation method and LLL algorithm to find the values of the unknown integers $d, k_i, \phi(N_i)$ and $d_i, k, \phi(N_i)$ respectively for $i = 1, 2, \cdots j$.

Keywords: Prime Power, Factorization, LLL algorithm, Diophantine approximations, Continued fraction.

1 Introduction

Public key cryptography is being considered and regarded as one of the major breakthrough in the field of information security. Transmission of information electronically is sometimes exposed to the threat of being attacked by eavesdroppers; this can be tackled through construction of strong encryption schemes. Among the public key cryptosystems, RSA cryptosystem invented by Rivest, Shamir and Adleman is regarded as fast growing, reliable and applicable cryptosystem due to its efficiency in providing confidentiality, integrity of the data being transmitted in an insecure communication channels and verification of the entities involved in communication [1].

The security of the RSA modulus $N = pq$ relied on the integer factorization problem where p and q are positive large prime numbers of equal bit length. The equation $ed - k\phi(N) = 1$ is called key equation where (e, N) and $(d, k, \phi(N), p, q)$ are public and private keys respectively. RSA cryptosystem involves three processes of key generation, encryption and decryption, details can be found in [2]. Many attacks of factoring modulus $N = pq$ can be found in [3], [5], [6], [7], [8] among others.

Cryptanalysis Attack on multi prime power modulus $N = p^r q$ for $r \geq 2$ was first reported by Takagi (1998) as one of the RSA variants. He showed that his scheme performed decryption process faster than standard RSA modulus $N = pq$, [9]. Since then, many attacks on the moduli $N = p^r q$ for $r \geq 2$ have been presented using various techniques which can be found in [10], [11], [12] and [13]. Prime moduli $N = p^r q^s$ is one of the variants of RSA cryptosystem reported to have high efficiency in the decryption process over standard RSA modulus $N = pq$, [14]. The cryptosystem provides privacy and authentication in the digital communication channels using complex mathematics and logic. The security of the cryptosystem is embedded in the integer factorization problem. The prime power moduli also undergoes similar processes of key generation, encryption and decryption as in standard RSA cryptosystem except that the decryption process is faster than standard RSA and its variants.

* Corresponding author e-mail: [1]sadiqshehuzezi@gmail.com [2]siabubakar82@gmail.com

Cryptanalysis attack prime power moduli $N = p^r q^s$ has been reported by Lim et al. (2000) where they utilized Takagi's technique to reveal prime factors (p,q) where $\gcd(r,s) = 1$. They proved that their technique performed decryption process 15-times faster than the standard RSA cryptosystem, [14]. Another partial key exposure attack on the moduli $N = p^r q^s$ where $\gcd(r,s) = 1$ was reported by Lu et al. (2015) where they showed that $\min\left(\frac{l}{r+l}, \frac{2(r-l)}{r+l}\right)$ fraction of least significant bit(s) $(LSBs)$ or most significant bit(s)$(MSBs)$ of p is required in order to factor N in polynomial time, [15].

Subsequently, Coron et al. (2016) reported a lattice construction based attack where a constant number of bits $r = \omega \log_2^3 \max\{p,q\}$ is required for $N = p^r q^s$ to be factored efficiently, [16]. Furthermore, Coron et al. (2018) improved their work by reducing the number of bits needed for the successful factorization of $N = p^r q^s$ to $r = \omega \log_2 q$ [17].

Similarly, Wang et al. (2019) presented another cryptanalysis attack that led to the successful factorization of prime power moduli $N = p^r q^s$ based on lattice construction method which required a small amount of bits to be known as compared to [15], [16] and [17]. They proved that one needed only $\alpha\beta(\log_2 N)$ LSBs of p to factor N where the parameters α, β were related based on the condition $\varsigma > \alpha\beta(su - ru)\log_2 N$ satisfying $su - rv = 1$ for $s,u,r,v \in \mathbb{Z}$ and $\gcd(r,s) = 1$, [18].

This paper reports a continued fraction approach of factoring the generalized Takagi's scheme with moduli $N = p^r q^s$ for $2 \leq s < r$. The paper shows that if $q^s < p^r < 2q^s$ where p and q have equal bit-size, then $\frac{k}{d}$ can be found from the convergents of the continued fraction expansion of $\frac{e}{N+N^{\frac{r+s-2}{2r}} - 2N^{\frac{r+s-1}{2r}}}$. The paper computes for the values of $\phi(N) = \frac{ed-1}{k}$, the $\gcd(\phi(N), N)$ and finally reveals p and q in polynomial time. Subsequently, the research work presents successful attacks on the moduli $N_i = p_i^r q_i^s$ using two system of equation of the form $e_i d - k_i \phi(N_i) = 1$ and $e_i d_i - k\phi(N_i) = 1$ for $i = 1, \cdots, j$ by fixing d and k respectively. In the first equation $e_i d - k_i \phi(N_i) = 1$, the paper proves that if $N = \max\{N_i\}$ and $d, k_i < N^{\delta}$ where $\delta = \frac{j}{2(1+2j)}$, then the moduli N_i can be factored simultaneously using LLL and simultaneous Diophantine approximation methods. Similarly, in $e_i d_i - k\phi(N_i) = 1$, also this research work shows that if $d_i, k < N^{\delta}$, where $\delta = \frac{4\vartheta j - j}{4(1+3j)}$, then one can exploits the security of the moduli and successfully reveal the prime factors (p_i, q_i) in polynomial time. In all the attacks, the paper presents numerical examples to justify how such attacks work.
The rest of the research is organized as follows. In section 2, we give definitions on continued fraction, lattice, and state theorems related to lattice basis reduction and simultaneous Diophantine approximations. In section 3, we present the proposed attacks. We conclude the paper in section 4.

2 Preliminaries

In this section, the paper defines concepts and state theorems as follows:

Definition 1. *(Continued Fraction Expansion). The continued fraction representation of a real number x will be denoted by* $x = [a_0, a_1, ..., a_m, ...]$ *where*

$$[a_0, a_1, ..., a_m, ...] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_m}}}$$

and m may be infinite. All a_i*, called partial quotients, are positive integers, except for* a_0 *which may be any integer [2].*

Definition 2. *(Convergent) Let* $x \in \mathbb{R}$ *with* $x = [a_0, a_1, ..., a_m]$*. For* $0 \leq n \leq m$*, the* n^{th} *convergent of the continued fraction expansion of x is* $[a_0, a_1, ..., a_n]$*, [2].*

Theorem 1. *(Legendre) Let* $x \in \mathbb{R}$ *and* $\frac{p}{q}$ *be a rational fraction such that* $gcd(p,q) = 1$ *and* $q < b$ *if* $x = \frac{a}{b}$ *with* $gcd(a,b) = 1$ *and*

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

then $\frac{p}{q}$ is a convergent of the continued fraction expansion of x, [2].

Definition 3. *(Lattice) A Lattice $\mathscr{L}$ is a discrete additive subgroup of $\mathbb{R}^m$. Let $b_1,\cdots,b_n \in \mathbb{R}^m$ be $n \leq m$ linearly independent vectors. The lattice generated by $\{b_1,\cdots,b_n\}$ is the set*

$$\mathscr{L} = \sum_{i=1}^{n} \mathbb{Z}b_i = \left\{ \sum_{i=1}^{n} x_i b_i | x_i \in \mathbb{Z} \right\}.$$

The set $B = \langle b_1,\cdots,b_n \rangle$ is called a lattice basis for $\mathscr{L}$. The lattice dimension is $dim(\mathscr{L}) = n$. If $n = m$ then $\mathscr{L}$ is said to be a full rank lattice.
A lattice $\mathscr{L}$ can be represented by a basis matrix. Given a basis B, a basis matrix M for the lattice generated by B is the $n \times m$ matrix defined by the rows of the set $b_1 ..., b_n$

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

It is often useful to represent the matrix M by B. A very important notion for the lattice $\mathscr{L}$ is the determinant [2].

Definition 4. *(Determinant) Let $\mathscr{L}$ be a lattice generated by the basis $B = \langle b_1,...,b_n \rangle$. The determinant of $\mathscr{L}$ is defined as*

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

If $n = m$, we have

$$det(\mathscr{L}) = \sqrt{det(BB^T)} = |det(B)| \, [2].$$

Theorem 2. *Let L be a lattice of dimension ω with a basis $v_1,...,v_\omega$. The LLL algorithm produces a reduced basis $b_1,...b_\omega$ satisfying*

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

for all $1 \leq i \leq \omega$ [2].

Theorem 3. *(Simultaneous Diophantine Approximations) There is a polynomial time algorithm, for given rational numbers of the form $\alpha_1,...,\alpha_n$ and $0 < \varepsilon < 1$, to compute integers $p_1,...,p_n$ and a positive integer q such that*

$$\max_i |q\alpha_i - p_i| < \varepsilon \quad and \quad q \leq 2^{\frac{n(n-3)}{4}} \, [11].$$

3 Results

This section presents the findings of this research work as discussed below:

3.1 Attack on Factoring $N = p^r q^s$ Based on Continued Fraction Method

In this section, we present results using continued fractions to factor multi prime power modulus $N = p^r q^s$ with $2 \leq s < r$ for some unknown parameters $(\phi(N), d, k, p, q)$ using good approximation of $\phi(N)$ given as $\phi(N) \approx N + N^{\frac{r+s-2}{2r}} - 2N^{\frac{r+s-1}{2r}}$ where (N, e) are public keys satisfying key equation $ed - k\phi(N) = 1$.

Lemma 1. *Let $N = p^r q^s$ be prime power moduli where p and q have the same bit size for $2 \leq s < r$. If $q < p < 2q$ and $q^s < p^r < 2q^s$, 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

$$\phi(N) \approx N + N^{\frac{r+s-2}{2r}} - \omega$$

where $\omega = 2N^{\frac{r+s-1}{2r}}$.

Proof. Suppose $N = p^r q^s$, $q < p < 2q$ and $q^s < p^r < 2q^s$ for $2 \leq s < r$, 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, defining $\phi(N) = p^{r-1} q^{s-1}(p-1)(q-1)$, 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 $p \approx q \approx N^{\frac{1}{2r}}$ gives the following result:

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

This completes the proof.

Theorem 4. *Let $N = p^r q^s$ be a generalized Takagi's moduli with condition $q < p < 2q$ and $q^s < p^r < 2q^s$ where p and q are distinct prime numbers and $2 \leq s < r$. Also, Let (e,N) and $(d,p,q,\phi(N))$ be public and private key tuples respectively satisfying $ed - k\phi(N) = 1$ where $1 < e < \phi(N)$. Let $Z = p^{r-2} q^{s-2}(p-1)(q-1)$ be known. If $p \approx q \approx N^{\frac{1}{2r}}$, then $d < \sqrt{\frac{N + N^{\frac{r+s-2}{2r}} - \omega}{8N^{\frac{r+s-1}{2r}}}}$, where $\left| \frac{e}{N + N^{\frac{r+s-2}{2r}} - \omega} - \frac{k}{d} \right| < \frac{1}{2d^2}$, which leads to the factorization of N into prime factors p and q in polynomial time.*

Proof. Key equation $ed - k\phi(N) = 1$ can be rewritten as follows:

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

Dividing by $d\left(N+N^{\frac{r+s-2}{2r}}-\omega\right)$ gives

$$\begin{aligned}\left|\frac{e}{\left(N+N^{\frac{r+s-2}{2r}}-\omega\right)}-\frac{k}{d}\right| &= \left|\frac{1+k\left(\omega-2N^{\frac{r+s-1}{2r}}\right)}{d\left(N+N^{\frac{r+s-2}{2r}}-\omega\right)}\right| \\ &< \left|\frac{\omega+2N^{\frac{r+s-1}{2r}}}{N+N^{\frac{r+s-2}{2r}}-\omega}\right| \\ &< \frac{4N^{\frac{r+s-1}{2r}}}{N+N^{\frac{r+s-2}{2r}}-\omega}.\end{aligned}$$

Therefore, from Theorem 2.3 we can write

$$\frac{4N^{\frac{r+s-1}{2r}}}{N+N^{\frac{r+s-2}{2r}}-\omega} < \frac{1}{2d^2}$$

then

$$d < \sqrt{\frac{N+N^{\frac{r+s-2}{2r}}-\omega}{8N^{\frac{r+s-1}{2r}}}}.$$

Hence $\frac{k}{d}$ can be found from the convergents of the continued fractions expansion of $\frac{e}{N+N^{\frac{r+s-2}{2r}}-\omega}$.

1: Initialization: The public key pair (N,e) and Z satisfying Theorem 4.
2: Choose r, s, to be suitable small positive integers where $2 \leq s < r$. **for *any*** (r,s) **do**
3:
end
The convergents $\frac{k}{d}$ of the continued fractions expansion of $\frac{e}{N+N^{\frac{r+s-2}{2r}}-\omega}$.
4: Compute $\phi(N) := \frac{ed-1}{k}$
5: Compute $H := \gcd(\phi(N),N)$
6: Compute $p^{r-2} := \gcd(Z,H)$
7: Compute $q^s := \frac{N}{p^r}$
8: **return** *prime factors p and q.*

Algorithm 1: : An outline on how Theorem 4 works

Example 1. To illustrate our attack for $N = p^r q^s$, for $r = 3$ and $s = 2$, let the public keys (e,N) be given as follows:

$$N = 807395611571163482838311336675686040347782521667346720955 3$$
$$e = 323427609321803974897591294248290179055667952937945433 55$$

and let the known integer Z be

$$Z = 800525443197071249380122932575686 72$$

Suppose that N and e satisfy all the conditions stated in Theorem 4, then taking the continued fraction expansion of $\frac{e}{N+N^{\frac{r+s-2}{2r}}-\omega}$ we get,
$[0,249,1,1,1,3,9,1,2,50,1,1,1,2,3,3,18,1,100,1,1,3,2,2,1,1,1,9,1,2,2,1,1,2,1,1,7,1,4,1,]$
$[8,1,6,1,3,2,3,2,5,2,2,2,1,2,3,1,1,1,1,3,2,1,76,1,1,2,6,1,1,1,1,95,3,1,4,80,1,23,1,]$
$[1,2,1,10,2,2,3,1,1,2,19,3,1,1,1,1,1,1,2,2,1,3,1,1,1,1,1,1,62,3,3,2,2,2,5,7,1,1,1,]$
$[2,3,2,1,4,1,1,2,5,9,2]$

We also obtain the convergent $\frac{k}{d} = \frac{16513}{4122259}$ from the above continued fractions expansion. Using algorithm 1 gives the following results

$$\frac{ed-1}{k} = \frac{(32342760932180397489759129424829017905566795293794543355)(4122259)-1}{16513}$$
$$= 807395611563792364656555314622819854189934427426889120668 8$$

$H = 800525443204379646360234595736473 57$
which leads to the factorization of N and return the prime factors
$p = 793713733433$, $q = 127071264013$.

3.2 Attacks on Generalized System of Equations Using $N+N^{\frac{r+s-2}{2r}} - \omega$ as Approximation of $\phi(N)$

In this section, we show that if $e_i < \phi(N_i) < N_i + N_i^{\frac{r+s-2}{2r}} - \omega$, where $\omega = 2N_i^{\frac{r+s-1}{2r}}$, then $N_i = p_i^r q_i^s$, can be factored simultaneously using simultaneous Diophantine Approximation and lattice basis reduction methods for $i = 1,...,j$ and $2 \le s < r$.

Theorem 5. *Let $N_i = p_i^r q_i^s$ be prime power moduli where $q < p < 2q$, $q^s < p^r < 2q^s$ $2 \le s < r$ and $Z_i = p_i^{r-2} q_i^{s-2}(p_i - 1)(q_i - 1)$ be known. Let (e_i, N_i) and $(d, p_i, q_i, \phi(N_i))$ be public and private key tuples respectively such that $1 < e_i < \phi(N_i) < N_i + N_i^{\frac{r+s-2}{2r}} - \omega_i$, where $\omega_i = 2N_i^{\frac{r+s-1}{2r}}$ is satisfied. Let $N = \max\{N_i\}$, define $\delta = \frac{j}{2(1+2j)}$. If there exists integers $d, k_i < N^{\delta}$ such that $e_i d - k_i \phi(N_i) = 1$ holds, then one can simultaneously factor j moduli $N_1,...,N_j$ in polynomial time for $i = 1,...,j$,.*

Proof. Suppose $N_i = p_i^r q_i^s$ be j moduli and $N = \max\{N_i\}$, if $k_i < N^{\delta}$, then $e_i d - k_i \phi(N_i) = 1$ can be rewritten as

$$\begin{aligned}
e_i d - k_i(p_i^{r-1} q_i^{s-1}(p_i-1)(q_i-1)) &= 1 \\
e_i d - k_i(p_i^r q_i^s - (p_i^r q_i^{s-1} + p_i^{r-1} q_i^s) + p_i^{r-1} q_i^{s-1}) &= 1 \\
e_i d - k_i(N_i - (p_i^r q_i^{s-1} + p_i^{r-1} q_i^s) + p_i^{r-1} q_i^{s-1}) &= 1 \\
e_i d - k_i\left(N_i + N_i^{\frac{r+s-2}{2r}} - \left(2N_i^{\frac{r+s-1}{2r}}\right)\right) &= 1 \\
e_i d - k_i\left(N_i + N_i^{\frac{r+s-2}{2r}} - \omega_i + \omega_i - \left(2N_i^{\frac{r+s-1}{2r}}\right)\right) &= 1 \\
e_i d - k_i\left(N_i + N_i^{\frac{r+s-2}{2r}} - \omega_i\right) &= 1 + k_i\left(\omega_i - 2N_i^{\frac{r+s-1}{2r}}\right)
\end{aligned}$$

$$\left| \frac{e_i}{N_i + N_i^{\frac{r+s-2}{2r}} - \omega_i} d - k_i \right| = \frac{\left| 1 + k_i\left(\omega_i - 2N_i^{\frac{r+s-1}{2r}}\right)\right|}{N_i + N_i^{\frac{r+s-2}{2r}} - \omega_i}. \tag{1}$$

Suppose $N = \max\{N_m\}$ and $k_i < N^{\delta}$, $N_i + N_i^{\frac{r+s-2}{2r}} - \omega_i > \frac{2}{3}N$, $4N_i^{\frac{r+s-1}{2r}} < N^{\delta+\frac{1}{2}}$ for $i = 1,...,j$ with $0.19\& \le \delta < 1$

$$\left| \frac{1 + k_i\left(\omega_i - 2N_i^{\frac{r+s-1}{2r}}\right)}{N_i + N_i^{\frac{r+s-2}{2r}} - \omega_i} \right| \le \left| \frac{1 + k_i + 2\omega_i}{N_i + N_i^{\frac{r+s-2}{2r}} - \omega_i} \right| < \frac{1 + N^{\delta} + 4N^{\frac{r+s-1}{2r}}}{N_i + N_i^{\frac{r+s-2}{2r}} - \omega_i} < \frac{1 + N^{\delta} + N^{\delta+\frac{1}{2}}}{\frac{2}{3}N} < \frac{4}{3}N^{2\delta-\frac{1}{2}}.$$

This implies

$$\left| \frac{e_i}{N_i + N_i^{\frac{r+s-2}{2r}} - \omega_i} d - k_i \right| < \frac{4}{3}N^{2\delta-\frac{1}{2}}.$$

For the unknown integer d, we let $\varepsilon = \frac{4}{3}N^{2\delta-\frac{1}{2}}$, with $\delta = \frac{j}{2(1+2j)}$, then

$$N^{\delta}\varepsilon^{j} = \left(\frac{4}{3}\right)^{j} N^{\delta+2\delta j-\frac{j}{2}} = \left(\frac{4}{3}\right)^{j}.$$

For $2^{j} < 2^{\frac{j(j-3)}{4}} \cdot 3^{j}$ with $j \geq 2$, we get $N^{\delta}\varepsilon^{j} < 2^{\frac{j(j-3)}{4}} \cdot 3^{j}$. It follows that if $d < N^{\delta}$ then $d < 2^{\frac{j(j-3)}{4}} \cdot 3^{j} \cdot \varepsilon^{-j}$. Hence

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

Using Theorem 3, we can obtain parameters d and k_i. One can observe that from $e_i d - k_i \phi(N_i) = 1$ we get

$$\begin{aligned} \phi(N_i) &= \frac{e_i d - 1}{k_i} \\ \gcd(\phi(N_i), N_i) &= H_i \\ p_i^{r-2} &= \gcd(Z_i, H_i) \\ q_j^{s} &= \frac{N_i}{p_i^{r}}. \end{aligned}$$

Finally, the prime factors (p_i, q_i) of the prime power moduli N_i can be found simultaneously in polynomial time for N_i for $i = 1, \ldots, j$.

Let

$$\eta_1 = \frac{e_1}{N_1 + N_1^{\frac{r+s-2}{2r}} - \omega_1}, \quad \eta_2 = \frac{e_2}{N_2 + N_2^{\frac{r+s-2}{2r}} - \omega_2}$$
$$\eta_3 = \frac{e_3}{N_3 + N_3^{\frac{r+s-2}{2r}} - \omega_3}$$

1: Initialization: The public key pair (N_i, e_i) and Z_{2i} satisfying Theorem 5.
2: Choose $r, s, t \geq 2$, $r > s$ and $N = \max\{N_i\}$ for $i = 1, \ldots, j$. **for *any*** (N, j, δ) **do**
3:
end
$\varepsilon := \frac{4}{3}N^{2\delta-\frac{1}{2}}$ where $\delta = \frac{j}{2(1+2j)}$
4: $Y := [3^{j+1} \times 2^{\frac{(j+1)(j-4)}{4}} \times \varepsilon^{-j-1}]$ for $j \geq 2$.
5: Consider the lattice $\mathscr{L}$ spanned by the matrix D as stated below.
6: Applying the LLL algorithm to $\mathscr{L}$ yields the reduced basis matrix F. **for *any*** (D, F) **do**
7:
end
$R := D^{-1}$
8: $U = RF$.
9: Produce d, k_i from U **for *each*** *triplet* (d, k_i, e_i) **do**
10:
end
$\phi(N_i) := \frac{e_i d - 1}{k_i}$
11: $H_i := \gcd(\phi(N_i), N_i)$
12: $p_i^{r-2} := \gcd(Z_{2i}, H_i)$
13: $q_i^{s} := \frac{N_i}{p_i^{r}}$
14: **return** *the prime factors* (p_i, q_i).

Algorithm 2: :An outline on how Theorem 5 works

Example 2. We consider the following three prime power moduli and their three public exponents respectively.

$$N_1 = 13873827124306049405017949703493 1524261190081$$
$$N_2 = 88523664622460396417800514546480692359295 07$$
$$N_3 = 28226616528702863229255664398023669153767201$$
$$e_1 = 11318701522644462250308522248728273762260 1387$$
$$e_2 = 69846353300025288824637793603126367841695 5$$
$$e_3 = 13528816480342124811487941361080338269800475$$

Let the following integers be known

$$Z_{21} = 377981394868844988732983600$$
$$Z_{22} = 74584932995851315518846144$$
$$Z_{23} = 15931666676463828916990 7952$$

Then $N = \min(N_1,N_2,N_3) = 88523664622460396417800514546480692359295 07$, $j = 3$ with $\delta = \frac{j}{2(1+2j)} = 0.2142857143$ and $\varepsilon := \frac{4}{3}N^{2\delta-\frac{1}{2}} = 0.001141015749$. Using Theorem 3, we obtain

$$\mu = [3^{j+1} \cdot 2^{\frac{(j+1)(j-4)}{4}} \cdot \varepsilon^{-j-1}] = 23893978460000$$

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

$$D = \begin{bmatrix} 1 & -[\mu\eta_1] & -[\mu\eta_2] & -[\mu\eta_3] \\ 0 & \mu & 0 & 0 \\ 0 & 0 & \mu & 0 \\ 0 & 0 & 0 & \mu \end{bmatrix}$$

Therefore, applying the LLL algorithm to $\mathscr{L}$, we obtain the reduced basis as indicated below

$$F = \begin{bmatrix} -86323 & -6355142339 & -1120692219 & -6116850563 \\ 3615170865 & 2825366945 & 8384746345 & -680167935 \\ 4634014334 & -8967937538 & -3375128498 & 3635168254 \\ 11779079649 & 9087358257 & -4236111303 & -8169829231 \end{bmatrix}$$

Next, we compute

$$U = \begin{bmatrix} -86323 & -70425 & -6811 & -41374 \\ 3615170865 & 2949369313 & 285241808 & 1732725675 \\ 4634014334 & 3780573639 & 365629918 & 2221050101 \\ 11779079649 & 9609741102 & 929385111 & 5645629072 \end{bmatrix}$$

Then, from the first row of matrix U we get $d = 86323$, $k_1 = 70425$, $k_2 = 6811$, $k_3 = 41374$. Hence using d and k_i for $i = 1,2,3$, we compute $B_i = \frac{e_i d-1}{k_i} = \phi(N_i) = p_i^{r-1}q_i^{s-1}(p_i-1)(q_i-1)$

$$B_1 = 13873827071909661552479695648945271934392 3600$$

$$B_2 = 88523664012892130483177334564714101471130 24$$

$$B_3 = 28226616354052623389135050082480254277178576$$

Applying algorithm 2 gives $H_i = \gcd(\phi(N_i), N_i)$ and $p_i^{r-2} = \gcd(Z_i, H_i)$, for $i = 1,2,3$

$$\begin{aligned} H_1 &= 377981396296342943258473931 \\ H_2 &= 74584933509438374731735417 \\ H_3 &= 159316667750399165073750827 \\ p_1 &= 1029780281 \\ p_2 &= 628409627 \\ p_3 &= 899215129 \end{aligned}$$

Finally, we compute $q_i^s := \frac{N_i}{p_i^r}$ for $i = 1,2,3$, that is

$$q_1 = 356435771, q_2 = 188871073, q_3 = 197030747.$$

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

Theorem 6. *Let $N_j = p_j^r q_s^s$ be j multi prime power moduli $2 \le s < r$ and $Z_i = p_i^{r-2} q_i^{s-2}(p_i-1)(q_i-1)$ be known integer where (e_i, N_i) are j public exponents and $(d_i, p_i, q_i, \phi(N_i))$ are private keys for $e_i < \phi(N_i) < N_i + N_i^{\frac{r+s-2}{2r}} - \omega$, where $\omega_i = 2N_i^{\frac{r+s-1}{2r}}$ with $e = \min\{e_i\} = N^{\vartheta}$ and $N = \max\{N_i\}$ is satisfied. If $d_i, k < N^{\delta}$ for $\delta = \frac{4\vartheta j - j}{4(1+3j)}$ such that $e_i d_i - k\phi(N_i) = 1$ holds, then prime factors p_i and q_i of j prime power moduli N_i can be simultaneously factored in polynomial time for $i = 1, \cdots, j$ and $0 < \vartheta < 1$.*

Proof. Suppose $N_i = p_i^r q_i^s$, for $1 \le i \le j$ be j multi prime power moduli. Equation $e_i d_i - k\phi(N_i) = 1$ can be rewritten as

$$\left| \frac{N_i + N_i^{\frac{r+s-2}{2r}} - \omega_i}{e_i} k - d_i \right| = \frac{\left| 1 + k(\omega_i - 2N_i^{\frac{r+s-1}{2r}}) \right|}{e_i} \tag{2}$$

Suppose that $2N_i^{\frac{r+s-1}{2r}} < N^{2\delta+\frac{1}{4}}$ for $0.22\& \le \delta < 1$, $N = \max\{N_i\}$, $k < N^{\delta}$ and $\max\{e_i\} = N^{\vartheta}$, then

$$\begin{aligned} \frac{\left| 1 + k(\omega_i - 2N^{\frac{r+s-1}{2r}}) \right|}{e_i} &\le \frac{\left| 1 + N^{\delta}(2\omega_i) \right|}{N^{\vartheta}} \\ &< \frac{1 + N^{3\delta+\frac{1}{4}}}{N^{\vartheta}} \\ &< \frac{3}{2} N^{3\delta+\frac{1}{4}-\vartheta} \end{aligned}$$

Hence

$$\left| \frac{N_i + N_i^{\frac{r+s-2}{2r}} - \omega}{e_i} k - d_i \right| < \frac{3}{2} N^{3\delta+\frac{1}{4}-\vartheta}.$$

To recover unknown integer k, d_i, we define $\varepsilon = \frac{3}{2} N^{3\delta+\frac{1}{4}-\vartheta}$, where $\delta = \frac{4\vartheta j - j}{4(1+3j)}$, this gives

$$N^{\delta} \varepsilon^j = \left(\frac{3}{2}\right)^j N^{\delta + 3\delta j + \frac{j}{4} - \vartheta j} = \left(\frac{3}{2}\right)^j.$$

For $\left(\frac{3}{2}\right)^j < 2^{\frac{j(j-3)}{4}} \cdot 3^j$ we get $N^\delta \varepsilon^j < 2^{\frac{j(j-3)}{4}} \cdot 3^j$. This shows that if $k < N^\delta$, then $k < 2^{\frac{j(j-3)}{4}} \cdot 3^j \cdot \varepsilon^{-j}$. Thus

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

Applying Theorem 3 gives the values of the unknown integers k, d_i. Finally, from equation $e_i d_i - k\phi(N_i) = 1$, we get

$$\begin{aligned} \phi(N_i) &= \frac{e_i d_i - 1}{k} \\ \gcd(\phi(N_i), N_i) &= W_i \\ p_i^{r-2} &= \gcd(Z_i, W_i) \\ q_i^s &= \frac{N_i}{p_i^r}. \end{aligned}$$

This produces the prime factors (p_i, q_i) of the prime power moduli N_i in polynomial time for $i = 1, \ldots, j$.

$$\eta_1 = \frac{N_1 + N_1^{\frac{r+s-2}{2r}} - \left(2N_1^{\frac{r+s-1}{2r}}\right)}{e_1}$$

$$\eta_2 = \frac{N_2 + N_2^{\frac{r+s-2}{2r}} - \left(2N_2^{\frac{r+s-1}{2r}}\right)}{e_2}$$

$$\eta_3 = \frac{N_3 + N_3^{\frac{r+s-2}{2r}} - \left(2N_3^{\frac{r+s-1}{2r}}\right)}{e_3}$$

Initialization: The public key tuple (N_i, e_i) and Z_i satisfying Theorem 6.
Choose $r, s, t \geq 2$, $r > s$ and $N = \max\{N_i\}$ for $i = 1, \ldots, j$. **for *any*** (N, j, δ) **do**
    end
    $\varepsilon := \frac{3}{2} N^{3\delta + \frac{1}{4} - \vartheta}$ where $\delta = \frac{4\vartheta j - j}{4(1+3j)}$
$X := [3^{j+1} \times 2^{\frac{(j+1)(j-4)}{4}} \times \varepsilon^{-j-1}]$ for $j \geq 2$.
Consider the lattice $\mathscr{L}$ spanned by the matrix N as stated below.
Applying the LLL algorithm to $\mathscr{L}$ yields the reduced basis matrix M. **for *any*** (N, M) **do**
    end
    $Q := N^{-1}$
$L = QM$.
Produce d_i, k from L **for *each*** *triplet* (d_i, k, e_i) **do**
    end
    $\phi(N_i) := \frac{e_i d_i - 1}{k}$
$W_i := \gcd(\phi(N_i), N_i)$
$p_i^{r-2} := \gcd(Z_i, W_i)$
$q_i^s := \frac{N_i}{p_i^r}$
return *the prime factors* (p_i, q_i).

Algorithm 3: Theorem 6

Example 3. We consider the following three prime power and their three public exponents respectively

$$N_1 = 950621999049136935924895883094612513975772 81$$
$$N_2 = 137693559757217588444578212995468215278958 99$$
$$N_3 = 287138496523993263132047398101089476151143799$$
$$e_1 = 336340578048319995519268037862851012176283 66$$
$$e_2 = 107716120168812702051648669949758927358153 06$$
$$e_3 = 126714743380844315452962509689636013886045916$$

Also, let

$$Z_{21} = 298939934396197318633406304$$
$$Z_{22} = 111194140870991807939370060$$
$$Z_{23} = 535782131539689139327165160$$

Then, one can observe that

$$N = \max\{N_1, N_2, N_3\} = 287138496523993263132047398101089476151143799$$

and $\min\{e_1, e_2, e_3\} = N^{\vartheta}$ with $\vartheta = 0.73311$ and $j = 3$ we get $\varepsilon = \frac{3}{2}N^{3\delta+\frac{1}{4}-\vartheta} = 0.01067275167$ and $\delta = \frac{4\vartheta j - j}{4(1+3j)} = 0.1449330000$. Using algorithm 3, we compute

$$X = [3^{j+1} \cdot 2^{\frac{(j+1)(j-4)}{4}} \cdot \varepsilon^{-j-1}] = 3121399850.$$

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

$$N = \begin{bmatrix} 1 & -[X\eta_1] & -[X\eta_2] & -[X\eta_3] \\ 0 & X & 0 & 0 \\ 0 & 0 & X & 0 \\ 0 & 0 & 0 & X \end{bmatrix}$$

Therefore, applying the LLL algorithm to $\mathscr{L}$, we obtain reduced basis as follows

$$M = \begin{bmatrix} 167215 & -6081330 & -5694925 & -3459380 \\ -7102929 & -608092 & 1551915 & 4928508 \\ 7258660 & -314170 & -1554300 & 9527330 \\ 11049869 & -19920088 & 26147935 & 3391212 \end{bmatrix}$$

Next, we compute

$$L = \begin{bmatrix} 167215 & 472611 & 213751 & 378913 \\ -7102929 & -20075486 & -9079677 & -16095399 \\ 7258660 & 20515639 & 9278748 & 16448289 \\ 11049869 & 31230988 & 14125052 & 25039255 \end{bmatrix}$$

From the first row of matrix L we obtain $k = 167215$, $d_1 = 472611$, $d_2 = 213751$, $d_3 = 378913$. Hence using d_i, k and algorithm 3, we compute $A_i = \frac{e_i d_i - 1}{k} = \phi(N_i) = p_i^{r-1} q_i^{s-1}(p_i - 1)(q_i - 1)$, $W_i = \gcd(\phi(N_i), N_i)$ and $p_i^{r-2} = \gcd(Z_i, W_i)$,

for $i = 1,2,3$.

$$A_1 = 950621995227668339576932611562359116799602 88$$
$$A_2 = 13769355860541149942434563197339305972390380$$
$$A_3 = 28713849570113842718194171237047544137549 4520$$
$$W_1 = 29893993559792584713835937 3$$
$$W_2 = 11119414180113036936332056 3$$
$$W_3 = 53578213307508381664677931 7$$
$$p_1 = 940069609$$
$$p_2 = 897945931$$
$$p_3 = 999735311$$

Finally, we compute $q_i^s := \frac{N_i}{p_i^r}$ for $i = 1,2,3$ which gives

$$q_1 = 338270333, q_2 = 137905483, q_3 = 536065877.$$

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

4 Conclusion

In this research work, we presented three cryptanalysis attacks that led to the successful factorization of prime power modulus $N = p^r q^s$ and its generalized form $N_i = p_i^r q_i^s$ for $2 \leq s < r$ using continued fraction and simultaneous Diophantine approximation and lattice basis reduction methods respectively. The paper also gave numerical examples to illustrate how our attacks work. This has not been reported by other researches based on the available literature within our reach.

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

All authors have contributed to all parts of the article. All authors read and approved the final manuscript.

References

[1] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM* **21(2)**, (1978) 120–126.
[2] Nitaj, Abderrahmane, *The Mathematical Cryptography of the RSA Cryptosystem*, 2012.
[3] M. Wiener, Cryptanalysis of short RSA secret exponents, *IEEE Transactions on Information Theory*, **36**, (1990) 553–558.
[4] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, *22(6)*, (1976) 644–654.
[5] B. de Weger B, Cryptanalysis of RSA with Small Prime Difference, *Applicable Algebra in Engineering Communication and Computing* **13(1)**, (2002).
[6] S. Maitra, and S. Sarkar, Revisiting Wieners attack new weak keys in RSA, *in International Conference on Information Security*, (2008).
[7] A. May, *New RSA Vulnerabilities Using Lattice Reduction Methods*, PhD. thesis, University of Paderborn (2003).
[8] Nitaj, Abderrahmane, Diophantine and Lattice Cryptanalysis of the RSA Cryptosystem, *Artificial Intelligence, Evolutionary Computing and Metaheuristics*, (2013) 139-168.

[9] T. Takagi, Fast RSA-type cryptosystem modulo $p^k q$, *Advances in Cryptology-CRYPTO 1998*, Springer Berlin Heidelberg, (1998), 318–326.

[10] S. Sarkar, Small Secret Exponent Attack on RSA Variant with Modulus $N = p^2 q$, *in Proc. Int. Workshop on Coding and Cryptography -WCC*, (2013), pp. 215–222.

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

[12] Sarkar, S, Revisiting Prime Power RSA, *Discrete Applied Mathematics*, **203** (2016) 127–133.

[13] Sadiq Shehu and Muhammad Rezal Kamel Ariffin, New Attacks on Prime Power $N = p^r q$ Using Good Approximation of $\phi(N)$, *Malaysian Journal of Mathematical Science*, **11(S)**, (2016) 121–136.

[14] S. Lim, S. Kim, I. Yie and H. Lee, A generalized Takagi-cryptosystem with a modulus of the form $p^r q^s$, *Progress in Cryptology-INDOCRYPT 2000*, Springer Berlin Heidelberg, **1977**, (2000) 283–294.

[15] Y. Lu, L. Peng and S. Sarkar, Cryptanalysis of an RSA variant with moduli $N = p^r q^l$, *The 9th International Workshop on Coding and Cryptography*, WCC 2015.

[16] J. S. Coron, J. C. Faug'ere, G. Renault and R. Zeitoun, Factoring $N = p^r q^s$ for large r and s, *Cryptographers' Track at the RSA Conference*, Springer, Cham, **9610** ,(2016) 448–464.

[17] J. S. Coron and R. Zeitoun, Improved factorization of $N = p^r q^s$, *Cryptographers' Track at the RSA Conference*, Springer, Cham, (2018) 65–79.

[18] S. Wang, L. Qu, C. Li, and H. Wang, Further Improvement to Factoring $N = p^r q^s$ with Partial Known Bits, *Adv. in Math. of Comm.*, **13(1)** (2019) 21–135.

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