International Journal of Cryptology Research 10(1): 37 - 72 (2020)

A New Short Decryption Exponent Cryptanalysis Attacks of Factoring RSA Modulus $N = pq$

Saidu Isah Abubakar[*1], **Muhammad Rezal Kamil Ariffin**[2,3], and **Muhammad Asyraf Asbullah**[2]

[1]*Department of Mathematics, Sokoto State University, Nigeria*
[2]*Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia*
[3]*Department of Mathematics,Faculty of Science, Universiti Putra Malaysia*

E-mail: siabubakar82@gmail.com
[*]*Corresponding author*

ABSTRACT

This paper proposes new cryptanalysis attacks on RSA modulus $N = pq$ with generalized method of small prime difference using continued fraction technique which result to a new short decryption exponent bound $d < \sqrt{\frac{a^j+b^i(b^i-2)}{2b^i}}N^{\frac{3}{4}-\gamma}$. The paper also shows that if $|b^ip - a^jq| < N^\gamma$, then RSA modulus $N = pq$ can be factored in polynomial time from the convergents of continued fraction expansions of $\frac{e}{N-\left\lceil \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N}\right\rceil+1}$ where a, b, i and j are small positive integers. The paper also reports t instances of factoring RSA moduli $N_s = p_sq_s$ with public key pair (N_s, e_s) where three new attacks using key equations of the form $e_sd - k_s\phi(N_s) = 1$, $e_sd_s - k\phi(N_s) = 1$, $e_sd - k\phi(N_s) = z_s$ and $e_sd_s - k\phi(N_s) = z_s$ which lead to successful factorization of t RSA moduli $N_s = p_sq_s$ in polynomial time using simultaneous Diophantine approximation and lattice basis reduction techniques for unknown positive integers d, d_s, k, k_s and z_s are being reported . The paper improves short decryption exponent bounds of some reported researches.

Keywords: Short Decryption, Exponent, Cryptanalysis, Attacks , RSA Modulus

1 INTRODUCTION

The most widely reported and widely used public key cryptosystem in today's digital world is RSA cryptosystem. It was invented by three gentlemen Rivest, Shamir and Adleman in the year 1977, as reported in Rivest and Adleman (1978). The RSA cryptosystem can be used for message encryption which helps us safeguard our information from being tempered by unauthorized parties (eavesdroppers) and also provides authentication between entities involved in communication through digital signature.

The RSA key generation involves random selection of two distinct random large prime numbers such that their product is represented by $N = pq$ and called the RSA modulus. The Euler totient function $\phi(N)$ is computed as $\phi(N) = (p-1)(q-1)$ where an integer $e < \phi(N)$ such that $\gcd(e, \phi(N)) = 1$. Also, a short decryption exponent d such that the relation $ed \equiv 1 \mod \phi(N)$ is satisfied is to be considered. The pairs (e, N) and (d, p, q) are called the public and private keys respectively.

The encryption function is to be computed by choosing a message $M \in (1, N-1)$ and computing ciphertext $C = M^e \pmod N$. Plaintext can be recovered by computing the decryption exponent from the equation $M = C^d \pmod N$. The primes p and q in most cases are consider to have same bit size.

The security of RSA depends on the failure of an adversary to compute the secret key d from the public keys(e, N).The problem of computing d from (e, N) is equivalent to the problem of factoring RSA modulus N into its primes factors of p and q as it was reported by Bach and Shallit (1986). It is therefore recommended for RSA users to generate primes p and q in such a way that the problem of factoring $N = pq$ is computationally infeasible for an adversary. Choosing p and q as strong primes has been recommended as a way of maximizing the difficulty of factoring RSA modulus N. The security of RSA can also be associated with the problem of solving RSA key equation

$ed \equiv 1 \pmod{\phi(N)}$ where the parameters $d, \phi(N)$ are unknown and (e, N) are public key pair.

The wisdom behind using short decryption is to speed up decryption and signature verification processes. But this suffered a setback in 1990 when Wiener showed that RSA modulus $N = pq$ can be broken if the short decryption exponent is $d < \frac{1}{3}N^{0.25}$. He found d from the convergents of the continued fraction expansion of $\frac{e}{N}$ where N was considered as a good approximation of $\phi(N)$ which led to the factorization of RSA modulus N into its two prime factors in polynomial time, as reported by Wiener (1990). Since then, there have been improvement on the bound d. Boneh and Durfee (1999) used a heuristic approach and applied Coppersmith method which enabled them to found an improved bound of $d < N^{0.292}$ and they conjectured that the better bound for a short decryption exponent attack for total break of RSA modulus $N = pq$ is $d < N^{0.5}$, as reported by Boneh and Durfee (1999). Furthermore, using small prime difference of $|p - q|$ and taking $N - 2N^{\frac{1}{2}} + 1 < N^{\delta}$ as an approximation of $\phi(N)$, de Weger (2002) proved that, the short decryption d can be found from the convergents of the continued fraction expansion of $\frac{e}{N-2N^{\frac{1}{2}}+1}$. He showed that RSA modulus $N = pq$ is insecure if the short secret exponent $d < N^{\delta}$ where $\delta < \frac{3}{4} - \beta$ for $\beta = [\frac{1}{4}, \frac{1}{2}]$ and p and q are balanced primes satisfying $q < p < 2p$, as reported by de Weger (2002).

In another development, Maitra and Sarkar (2008), reported an improved bound of de Weger where they proved that if the prime difference $|2q - p| < N^{\delta}$ for $\beta = [\frac{1}{4}, \frac{1}{2}]$ where p and q are balanced primes, then the short secret exponent d can be found from the convergents of continued fraction expansion of $\frac{e}{N-\frac{3}{\sqrt{2}}N^{\frac{1}{2}}+1}$ where $N - \frac{3}{\sqrt{2}}N^{\frac{1}{2}} + 1$ was taken as a good approximation of $\phi(N)$ which led to the factorization of N into prime factors p and q in polynomial time, as reported by Maitra and Sarkar (2008). Chen et al. (2009) also reported a generalized de Weger method of factoring RSA modulus $N = pq$. They used prime difference approach by choosing some small integers a, b and showed that if $|aq - bp| < N^{\gamma}$ where $\gamma = \frac{1}{5}$, then d can be found from the convergents of continued fraction expansion of $\frac{e}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}+1}$. They proved that if $d < N^{\frac{3}{4}-\gamma}$, then RSA modulus $N = pq$ can be factored efficiently provided $p < q < 2q$ and $a > b$, as reported by Chen C.Y. Hsueh and Lin (2009). Blömer and May (2004) also reported an attack on RSA modulus $N = pq$ us-

ing generalized key equation of the form $ex - y\phi(N) = z$ where they showed that RSA modulus is insecure if $x < \frac{1}{3}N^{\frac{1}{4}}$ and $|z| < exN^{\frac{-3}{4}}$. They employed continued fraction and lattice basis reduction methods to carryout their attack which yielded the prime factors p and q efficiently, as reported by Blömer and May (2004). Also, Nitaj et al. (2014) reported some cryptanalysis attacks on factoring j RSA modulus $N_i = p_i q_i$ where $i = 1, 2 \ldots, j$ for $j \geq 2$. In the first case, they proved 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 $\delta = \frac{k}{2(k+1)}$, $N = \min\{N_i\}$ for unknown parameters $x,\ y,\ z$, then k RSA moduli N_i can be factored simultaneously. In their second attack, they also proved that k instances of RSA public key pair (N_i, e_i) satisfying $e_i x_i - y\phi(N_i) = z_i$ for unknown parameters x_i, y, and z_i where $x < N^{\delta}$, $y_i < N^{\delta}$, and $|z_i| < \frac{p_i - q_i}{3(p_i+q_i)} y_i N^{\frac{1}{4}}$ for all $\delta = \frac{k(2\alpha-1)}{2(k+1)}$, $N = \min\{N_i\}$ and $\min\{e_i\} = N^{\alpha}$ can be factored efficiently. They applied simultaneous Diophantine approximations and lattice basis reduction techniques and finally used Coppersmith's method to compute prime factors p_i and q_i of RSA moduli N_i in polynomial time, as reported by Nitaj et al. (2014).

The contributions of this paper is reported into two parts. The first part reports the use of generalized prime difference technique to mount an attack on RSA modulus $N = pq$ which make it insecure if the decryption exponent $d < \sqrt{\frac{a^j + b^i(b^i - 2)}{2b^i}} N^{\frac{3}{4} - \gamma}$. The decryption exponent d can be recovered from the convergent of continued fraction expansion of $\frac{e}{N - \left\lceil \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} \right\rceil + 1}$. The second part of the paper reports four new cryptanalysis attacks on t instances of factoring RSA moduli $N_s = p_s q_s$ for a given public key pair (N_s, e_s). We construct system of equations of the form $e_s d - k_s \phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k\phi(N_s) = z_s$ and $e_s d_s - k\phi(N_s) = z_s$ by using $N - \left\lceil \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} \right\rceil + 1$ as good approximation of $\phi(N)$ to simultaneously factor t instances of RSA moduli $N_s = p_s q_s$ in polynomial time.The paper shows new bounds that are considered to be larger (bounds) over some results as reported by researchers.

The rest of the paper is organized as follows. In Section 2, we present definitions of some basic terms and theorems that form the basis of this paper . In Section 3 , we present our main findings which contains proofs of

our main results with lemmas and theorems. We also give some numerical results/examples to illustrate how our theorems work and finally in Section 4, we conclude the paper.

2 PRELIMINARIES

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

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

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

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 $x = [a_0, a_1, a_2, \ldots, a_m]$. 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 $\vec{b_1}, \ldots, \vec{b_m} \in \mathcal{R}^n$. 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*

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

Otherwise, they are said to be linearly independent.

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

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

orthogonal basis. Let

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

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

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

Theorem 2.1. *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:*

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

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

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

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

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

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

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

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

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

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

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

3 FINDINGS AND DISCUSSIONS

In this section, we present the major findings of the paper and discuss the techniques employed in achieving the results. This paper is divided into two parts. In the first part, we propose a new short decryption exponent cryptanalytic attack on factoring RSA modulus $N = pq$ using continued fraction method which yields an improved bound and in the second part of the paper, we present four cryptanalysis attacks of factoring t RSA moduli $N_s = p_s q_s$ for $s = 1, \ldots, t$ efficiently and report some improvements on the decryption exponent over reported attacks .

3.1 Cryptanalytic Attacks Through Analyzing Small Prime Difference Satisfying $|b^i p - a^j q| < N^\gamma$

In this section, we show that if the decryption exponent $d < \sqrt{\frac{a^j + b^i(b^i-2)}{2b^i}} N^{\frac{3}{4}-\gamma}$, then RSA modulus $N = pq$ can be factored efficiently from the convergent of the continued fraction expansion of $\frac{e}{N - \left\lceil \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} \right\rceil + 1}$. The section also presents numerical example to illustrates how the attack works for $i > j$.

Lemma 3.1. *Let p and q be balanced prime numbers where $q < p < 2q$ and $N = pq$. If a, b, i and j are small positive integers less than $\log N$ and $(b^i p - a^j q)(a^j p - b^i q) < 0$ such that $\frac{b^i}{a^j} < \frac{q}{p}$ for $a > b$, $2 < j < i$ and $b^i p - a^j q \neq 0$, $e < \phi(N)$, then $\phi(N) > N - \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} + 1$.*

Proof. Suppose $(b^i p - a^j q)(a^j p - b^i q) < 0$, then we have

$$a^j b^j p^2 - a^{2j} pq - b^{2j} pq + a^j b^j q^2 < 0$$
$$a^j b^i (p^2 + q^2) < (a^{2j} + b^{2i}) pq.$$

Adding $2a^j b^i pq$ to both sides gives

$$a^j b^i (p+q)^2 < (a^j + b^i)^2 pq$$
$$p+q < \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N}.$$

Then

$$\phi(N) > N - \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} + 1.$$

□

Lemma 3.2. *Let p and q be balanced prime numbers where $q < p < 2q$ and $N = pq$. If*

$$\left(\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} - (p+q) \right) \left(\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} + (p+q) \right) - (b^i p - a^j q)^2 < 0$$

then

$$\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} - (p+q) < \frac{(b^i p - a^j q)^2}{\left(\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} + 2 \right) \sqrt{N}}$$

for suitably small positive integers $a > b$, $2 < j < i$.

Proof. Observe

$$\left(\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} - (p+q) \right) \left(\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} + (p+q) \right) - (b^i p - a^j q)^2 < 0$$

Then

$$\left(\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} - (p+q) \right) \left(\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} + (p+q) \right) < (b^i p - a^j q)^2$$
$$\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} - (p+q) < \frac{(b^i p - a^j q)^2}{\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} + (p+q)}$$
$$\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} - (p+q) < \frac{(b^i p - a^j q)^2}{\left(\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} + 2 \right) \sqrt{N}}.$$

□

Theorem 3.1. *Let p and q be balanced prime numbers where $q < p < 2q$ and $N = pq$. Let (e, N) be public key pair and (d, p, q) be private key tuple. If $|b^i p - a^j q| < N^\gamma$, and $\frac{b^i}{a^j} < \frac{q}{p}$, then the decryption exponent $d < \sqrt{\frac{a^j+b^i(b^i-2)}{2b^i}} N^{\frac{3}{4}-\gamma}$ can be found from the convergent of the continued fraction expansion of $\frac{e}{N-\lceil \frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} \rceil + 1}$ which leads to the factorization of N in polynomial time where $a > b$, $i > j$ are suitably small positive integers and $\frac{1}{4} \leq \gamma \leq \frac{1}{2}$.*

Proof. From Lemma 3.2, it was shown that:

$$\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} - (p + q) < \frac{(b^i p - a^j q)^2}{\left(\frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} + 2 \right) \sqrt{N}}.$$

Also, suppose $|b^i p - a^j q| < N^\gamma$, then we have:

$$\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} - (N - \phi(N) + 1) < \frac{N^{2\gamma}}{\left(\frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} + 2 \right) \sqrt{N}}. \tag{1}$$

Using RSA key equation $ed - k\phi(N) = 1$, for some $k \in \mathcal{Z}$, we get

$$\left| \frac{e}{\phi(N)} - \frac{k}{d} \right| = \frac{1}{d\phi(N)}.$$

Also, taking $N - \frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} + 1$ from Lemma 3.1 as approximation of $\phi(N)$, this becomes:

$$\begin{aligned}
\left| \frac{e}{\phi(N)} - \frac{k}{d} \right| &= \left| \frac{e}{N - \frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} + 1} - \frac{k}{d} \right| \\
&= \left| \frac{e}{N - \frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} + 1} - \frac{e}{\phi(N)} + \frac{e}{\phi(N)} - \frac{k}{d} \right| \\
&\leq \left| \frac{e}{N - \frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} + 1} - \frac{e}{\phi(N)} \right| + \left| \frac{e}{\phi(N)} - \frac{k}{d} \right|.
\end{aligned}$$

But $e < \phi(N)$ and $\frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N} - (N - \phi(N) + 1) < \frac{N^{2\gamma}}{\left(\frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}+2\right)\sqrt{N}}$. This implies:

$$\left|\frac{e}{N - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N}+1} - \frac{k}{d}\right| < \frac{N^{2\gamma}}{(N - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N}+1)(\frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}+2)\sqrt{N}} + \frac{1}{d\phi(N)}. \tag{2}$$

Now, assuming that $N - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N}+1 > \frac{a^j+b^i}{2a^j}N$, $\phi(N) > \frac{b^i}{a^j}N$, $N > a^j b^i d$ and a, b are small positive integers. Plugging the conditions into inequality (2), yields:

$$\begin{aligned}\left|\frac{e}{N - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N}+1} - \frac{k}{d}\right| &< \frac{N^{2\gamma}}{(\frac{a^j+b^i}{2a^j}N)(\frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}+2)\sqrt{N}} + \frac{1}{b^i d^2} \\ &< \frac{1}{a^j+b^i}N^{2\gamma-\frac{3}{2}} + \frac{1}{b^i d^2}.\end{aligned}$$

Suppose $d < \sqrt{\frac{a^j+b^i(b^i-2)}{2b^i}}N^{\frac{3}{4}-\gamma}$, then

$$\frac{1}{a^j+b^i}N^{2\gamma-\frac{3}{2}} + \frac{1}{b^i d^2} < \frac{1}{2d^2}.$$

Hence, we have

$$\left|\frac{e}{N - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N}+1} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

This shows that Theorem 3.1 produces $\frac{k}{d}$ as the convergent of the continued fraction expansion of $\frac{e}{N-\frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N}+1}$. This terminates the proof. □

Author(s)	Bounds for d	Assumed Interval for γ
Wiener (1990)	$d < \frac{1}{3}N^{\frac{1}{4}}$	Not applicable
de Weger (2002)	$d < \frac{1}{8}N^{\frac{3}{4}-\gamma}$	$0.25 \leq \gamma \leq 0.5$
Maitra and Sarkar (2008)	$d < N^{\frac{1}{4}}$	Not applicable
Chen C.Y. Hsueh and Lin (2009)	$d < N^{\frac{3}{4}-\gamma}$	$0.25 \leq \gamma \leq 0.5$
Nitaj (2013)	$d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$	Not applicable
Asbullah (2015)	$d < \frac{1}{2}N^{\frac{1}{4}}$	Not applicable
Our result of Theorem 3.1	$d < \sqrt{\frac{a^j+b^i(b^i-2)}{2b^i}}N^{\frac{3}{4}-\gamma}$	$0.25 \leq \gamma \leq 0.5$

Table 1: Comparison of the bounds on d for RSA modulo $N = pq$

From Table 1 one can observe that our bound of Theorem 3.1 is an improvement of the above mentioned bounds.

Example 3.1. *This example gives an illustration of how Theorem 3.1 works in factoring $N = pq$ for $\gamma = \frac{1}{2}$. Let*

$$N = 685483800920548702890289$$

$$e = 617682506652768172655511.$$

Taking $a = 3$, $b = 2$, $j = 3$, $i = 4$ and the continued fraction expansion of $\frac{e}{N-\left\lfloor \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N}\right\rfloor+1}$ gives the following:

$$[0, 1, 9, 9, 13, 3, 1, 9, 6, 1, 1, 238, 122, 1, 40, 2, 1, 2, 10,$$

$$2, 1, 14, 1, 4, 4, 3, 39, 2, 1, 1, 1, 1, 4, 5, 1, 2, 1, 3, 1, 3, 3]$$

Also taking the convergents of continued fraction expansion of $\frac{e}{N-\left\lfloor \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N}\right\rfloor+1}$ gives the following:

$$\left[0, 1, \frac{9}{10}, \frac{82}{91}, \frac{1075}{1193}, \frac{3307}{3670}, \frac{4382}{4863}, \frac{42745}{4737}, \frac{260852}{289485}, \frac{303597}{336922}, \frac{564449}{626407}, \frac{134642459}{149421788}, \ldots\right].$$

Taking $\frac{k}{d} = \frac{564449}{626407}$ we compute

$$\begin{aligned}\frac{1+k\phi(N)}{d} &= 617682506652768172655511\\ \phi(N) &= 685483800918843957077824\\ N-\phi(N)+1 &= 1704745812466.\end{aligned}$$

Finally, solving the quadratic equation $x^2-(N-\phi(N)+1)x+N=0$ leads to the factorization of N. This successfully reveals prime factors p and q as $p = 1054995141833$ and $q = 649750670633$.

Also, taking the value of $\gamma = 0.5$ this shows that the bound $d < \sqrt{\frac{a^j+b^i(b^i-2)}{2b^i}}N^{0.25}$, that is $626407 < 1054771.867$. Also, the result shows that the short decryption exponent found is greater than Wiener's original bound $d < \frac{1}{3}N^{0.25}$, as reported in Wiener (1990). This can be seen from $\frac{1}{3}N^{0.25} < d < \sqrt{\frac{a^j+b^i(b^i-2)}{2b^i}}N^{0.25}$, numerically as follows

$$303303.9347 < 626407 < 1054771.867.$$

The result also shows that the secret exponent found is greater than Asbullah and Ariffin's bound $d < \frac{1}{2}N^{0.25}$, as reported in Asbullah (2015). This can be seen from $\frac{1}{2}N^{0.25} < d < \sqrt{\frac{a^j+b^i(b^i-2)}{2b^i}}N^{0.25}$, numerically as follows

$$454955.9020 < 626407 < 1054771.867.$$

3.2 System of Equation Using $N - \frac{a^j+b^i}{a^{\frac{i}{2}}b^{\frac{j}{2}}}\sqrt{N}+1$ as an Approximation of $\phi(N)$

This section presents four cryptanalytic attacks on t RSA moduli $N_s = p_sq_s$ using system of equations of the form $e_sd-k_s\phi(N_s)=1$, $e_sd_s-k\phi(N_s)=1$, $e_sd-k_s\phi(N_s)=z_1$ and $e_sd_s-k\phi(N_s)=z_1$ for $s=1,\ldots,t$, $j=3,\ldots,i$ which successfully factor t RSA moduli in polynomial time.

3.2.1 The Attack on t RSA Moduli $N_s = p_sq_s$ Satisfying $e_sd-k_s\phi(N_s)=1$

Taking $t \geq 2$, let $N_s = p_sq_s$, for $s = 1,\ldots,t$. The attack works for t instances of (N_s, e_s) when there exists integer d and t integers k_s satisfying equation

$e_s d - k_s\phi(N_s) = 1$. It shows that prime factors p_s and q_s of t RSA moduli N_s for $s = 1, \ldots, t,$, $j = 3, \ldots, i$ can be found efficiently for $N = \max\{N_s\}$ and $d, k_s < N^\gamma$, for all $\gamma = \frac{3t}{2(3t+1)}$ for $\frac{1}{4} \leq \gamma \leq \frac{1}{2}$. In this case, the RSA instances shared common decryption exponent d.

Theorem 3.2. *Let $N_s = p_s q_s$ be RSA moduli for $j = 3 \ldots, i$, $s = 1 \ldots t$ and $t \geq 2$. Let (e_s, N_s) be public key pair and (d, N_s) be private key pair such that $e_s < \phi(N_s)$ and $e_s d \equiv 1 \pmod{\phi(N_s)}$ is satisfied. Let $N = \max\{N_s\}$, if there exists positive integers $d, k_s < N^\gamma$, for all $\gamma = \frac{3t}{2(3t+1)}$ such that $e_s d - k_s\phi(N_s) = 1$ holds, then t RSA moduli N_s can be successfully factored in polynomial time for $\frac{1}{4} \leq \gamma \leq \frac{1}{2}$..*

Proof. For $t \geq 2$, $j = 3, \ldots, i$ and let $N_s = p_s q_s$, $1 \leq s \leq t$ be t moduli. Let $N = \max\{N_s\}$ and suppose that $k_s < N^\gamma$ for $s = 1, \cdots, t$. Then equation $e_s d - k_s\phi(N_s) = 1$ can be rewritten as

$$e_s d - k_s(N_s - (p_s + q_s) + 1) = 1$$

$$e_s d - k_s\left(N_s - \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} + \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} - (N_s - \phi(N_s) + 1) + 1\right) = 1.$$

Then, we get

$$\left|\frac{e_s}{N_s - \frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} + 1} d - k_s\right| = \frac{\left|1 + k_s\left(\frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} - N_s + \phi(N_s) - 1\right)\right|}{N_s - \frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} + 1}. \tag{3}$$

Taking $N = \max\{N_s\}$ and suppose that $k_s < N^\gamma$, for $s = 1, \ldots, t$. From Theorem 3.1, it was shown that

$$\begin{aligned} \left|\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} + \phi(N_s) - N_s - 1\right| &< \frac{N^{2\gamma}}{\left(\frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} + 2\right)\sqrt{N}} \\ N_s - \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_i} + 1 &> \frac{a^j + b^i}{2a^j} N. \end{aligned}$$

Plugging the conditions into equation (3) yields

$$\begin{aligned}\frac{\left|1+k_s\left(\frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_s}-N_s+\phi(N_s)-1\right)\right|}{N_s-\frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_s}+1} &< \frac{1+N^{\gamma}\left(\frac{N^{2\gamma}}{(\frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}+2)\sqrt{N}}\right)}{\frac{a^j+b^i}{2a^j}N}\\ &< \frac{2a^j+N^{3\gamma-\frac{1}{2}}}{N}\\ &< \sqrt{\frac{a^j}{b^i}}N^{3\gamma-\frac{3}{2}}\\ \left|\frac{e_s}{N_s-\frac{a^J+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_s}+1}d-k_s\right| &< \sqrt{\frac{a^j}{b^i}}N^{3\gamma-\frac{3}{2}}.\end{aligned}$$

Hence, to show the existence of the integer d and t integers k_s, let $\varepsilon = \sqrt{\frac{a^j}{b^i}}N^{3\gamma-\frac{3}{2}}$, with $\gamma = \frac{3t}{2(3t+1)}$. Then it yields

$$N^{\gamma}\varepsilon^t = N^{\gamma}\left(\sqrt{\frac{a^j}{b^i}}N^{3\gamma-\frac{3}{2}}\right)^t = \left(\frac{a^j}{b^i}\right)^{\frac{t}{2}}N^{\gamma+3\gamma t-\frac{3t}{2}} = \left(\frac{a^j}{b^i}\right)^{\frac{t}{2}}.$$

Following Theorem 2.4, we get $\left(\frac{a^j}{b^i}\right)^{\frac{t}{2}} < 2^{\frac{t(t-3)}{4}}\cdot 3^t$ for $t \geq 2$, which yields $N^{\gamma}\varepsilon^t < 2^{\frac{t(t-3)}{4}}\cdot 3^t$. It follows that if $d < N^{\gamma}$ then $d < 2^{\frac{t(t-3)}{4}}\cdot 3^t\cdot\varepsilon^{-t}$ for $s = 1,\ldots,t$, gives

$$\left|\frac{e_s}{N_s-\frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_s}+1}d-k_s\right| < \varepsilon.$$

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 $e_sd-k_s\phi(N_s) = 1$, we make the following computations :

$$\begin{aligned}\phi(N_s) &= \frac{e_sd-1}{k_s}\\ p_s+q_s &= N_s-\phi(N_s)+1.\end{aligned}$$

Finally, by finding the roots of $x^2 - (N_s - \phi(N_s) + 1)x + N_s = 0$, the prime factors p_s and q_s can be revealed which lead to the factorization of t RSA moduli N_s for $s = 1, \ldots, t$ in polynomial time. □

Let

$$X_1 = \frac{e_1}{N_1 - \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_1} + 1},$$
$$X_2 = \frac{e_2}{N_2 - \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_2} + 1}$$
$$X_3 = \frac{e_3}{N_3 - \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_3} + 1}.$$

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 suitable small positive integers a and b, the matrix M can be used in computing the reduced basis after applying the LLL algorithm.

Algorithm 1 Theorem 3.2

1: Initialization: The public key tuple (N_s, e_s, γ) satisfying Theorem 3.2.
2: Choose a, b, i, j and t to be suitable small positive integers and $N = \max\{N_s\}$ for $s = 1, \ldots, t$.
3: **for any** $(a, b, j, i, t, N, \gamma)$ **do**
4: $\quad \varepsilon := \sqrt{\frac{a^j}{b^i}} N^{3\gamma - \frac{3}{2}}$
5: $\quad T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}]$ for $t \geq 2$.
6: **end for**
7: Consider the lattice $\mathcal{L}$ spanned by the matrix M as stated above.
8: Applying the LLL algorithm to $\mathcal{L}$ yields the reduced basis matrix K.
9: **for any** (M, K) **do**
10: $\quad J := M^{-1}$
11: $\quad Q = JK$.
12: **end for**
13: Produce d, k_s from Q
14: **for each** triplet (d, k_s, e_s) **do**
15: $\quad \phi(N_s) := \frac{e_s d - 1}{k_s}$
16: $\quad W_s := N_s - \phi(N_s) + 1$.
17: **end for**
18: Solve the quadratic equation $x^2 - W_s x + N_s = 0$
19: **return** the prime factors (p_s, q_s).

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

$$\begin{aligned}
N_1 &= 313296722483694348869118218800108664339857\\
N_2 &= 243057446386924151991041341567942883769227\\
N_3 &= 627593708207414307209298238491831299270237\\
e_1 &= 749621981125367930591616128994928126565 3\\
e_2 &= 167584613561508555407564322088296772905073\\
e_3 &= 536037461585975554491800236835143553077957.
\end{aligned}$$

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

$$N = 627593708207414307209298238491831299270237.$$

By using $a = 3$, $b = 2$, $j = 3$, $i = 4$ *and since* $t = 3$, *we have from Algorithm 1,* $\gamma = \frac{3t}{2(3t+1)} = 0.45$ *and* $\varepsilon = \sqrt{\frac{a^j}{b^i}} N^{3\gamma - \frac{3}{2}} = 0.0000006981843403$.
Applying Theorem 2.4 and using Algorithm 1, for $n = t = 3$ *we compute*

$$T = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}] = 17044120980000000000000000000.$$

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

$$M = \begin{pmatrix} 1 & -[TX_1] & -[TX_2] & -[TX_3] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{pmatrix}$$

Therefore, by applying LLL algorithm to $\mathcal{L}$, we obtain the reduced basis with the following matrix:

$$K = \begin{pmatrix} -1050590551029817 & -980192508667440107 & -80803053781452532 & -10936250900571415826 \\ 27694966597117771359 & 36467682502142580189 & -45378575342858626836 & -3994752216699011298 \\ -21764529693552634884 & -78590202542256797964 & -37931866156286954064 & -37931866156286954064 \\ -68906978215743699234 & 10740574764790428186 & -62239616909978186664 & 124439360191399548 \end{pmatrix}$$

Next, from Algorithm 1 we compute $Q = K \cdot J$,

$$Q = \begin{pmatrix} -1050590551029817 & -25137376604875 & -724367075038833 & -897325586243953 \\ 27694966597117771359 & 662654737117871222 & 19095281151717704826 & 23654697934799994364 \\ -21764529693552634884 & -520757757623588053 & -15006330199963036526 & -18589420347867530064 \\ -68906978215743699234 & -1648730478696173557 & -47510370439726361420 & -58854512410312596083 \end{pmatrix} \quad (4)$$

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

$$d = 1050590551029817,\ k_1 = 25137376604875$$

$$k_2 = 724367075038833,\ k_3 = 897325586243953.$$

Using Algorithm 1, we now compute $\phi(N_s) = \frac{e_s d - 1}{k_s}$ for $s = 1, 2, 3$.

$$\phi(N_1) = 313296722483694348867888562983387518790436$$

$$\phi(N_2) = 243057446386924151990021227446103936135080$$

$$\phi(N_3) = 627593708207414307207614412569114919302556.$$

Next, from Algorithm 1, we proceed to compute W_s for $s = 1, 2, 3$.

$$W_1 = 1229655816721145549422$$

$$W_2 = 1020114121838947634148$$

$$W_3 = 1683825922716379967682.$$

Finally, solving $x^2 - W_s x + N_s = 0$ for $s = 1, 2, 3$ yields (p_1, q_1), (p_2, q_2), and (p_3, q_3), which lead to the factorization of three RSA moduli N_1, N_2, N_3. That is,

$$p_1 = 869222551416087064319,\ q_1 = 360433265305058485103,$$
$$p_2 = 640826931328860063517,\ q_2 = 379287190510087570631$$
$$p_3 = 1126910726780136395479,\ q_3 = 556915195936243572203.$$

From our result, one can observe that we get $d \approx N^{0.3593}$ which is larger than Blömer and May's bound of $x < \frac{1}{3}N^{0.25}$ as reported by Blömer and May (2004). Our $d \approx N^{0.3593}$ is also larger than Nitaj et al.'s bound $x \approx N^{0.344}$, as reported by Nitaj et al. (2014).

3.2.2 The Attack on t RSA Moduli $N_s = p_s q_s$ Satisfying $e_s d_s - k\phi(N_s) = 1$

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

Theorem 3.3. *Let $N_s = p_s q_s$ be t RSA moduli for $s = 1, \cdots, t$ and $t \geq 2$, pairs (e_s, N_s) be public keys and (d_s, N_s) be private keys with $e_s < \phi(N_s)$ and $e_s d_s \equiv 1 \pmod{\phi(N_s)}$ is satisfied. Let $e = \min\{e_s\} = N^{\alpha}$ be public exponent. If there exists integers $d_s, k < N^{\gamma}$, for all $\gamma = \frac{t(1+2\alpha)}{2(3t+1)}$ such that $e_s d_s - k\phi(N_s) = 1$ holds, then prime factors p_s and q_s of t RSA moduli N_s can be successfully recovered in polynomial time for $j = 3, \ldots, i$, $\frac{1}{4} \leq \gamma \leq \frac{1}{2}$ and $0 < \alpha < 1$.*

Proof. For $t \geq 2$, $j = 3, \ldots, i$, $N_s = p_s q_s$ be t moduli, $e = \min\{e_s\} = N^{\alpha}$ be public exponent for $s = 1, \ldots, t$, and suppose that $d_s < N^{\gamma}$ is a positive integer. Then equation $e_s d_s - k\phi(N_s) = 1$ can be rewritten as

$$e_s d_s - k(N_s - (p_s + q_s) + 1) = 1$$

$$e_s d_s - k\left(N_s - \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} + \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} - (N_s - \phi(N_s) + 1) + 1\right) = 1.$$

Then, we get:

$$\left| k\frac{\left(N_s - \frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} + 1\right)}{e_s} - d_s \right| = \frac{\left|1 + k\left(\frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} - N_s + \phi(N_s) - 1\right)\right|}{e_s}.$$

Let $N = \max\{N_s\}$ and suppose that $d_s, k < N^{\gamma}$ are positive integers for $s = 1, \ldots, t$. From Theorem 3.1, it has been shown that

$$\left|\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} + \phi(N_s) - N_s - 1\right| < \frac{N^{2\gamma}}{(\frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} + 2)\sqrt{N}}.$$

Suppose also $e = \min\{e_s\} = N^{\alpha}$, for $s = 1, \cdots, t$, then

$$\frac{\left|1 + k\left(\frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} - N_s + \phi(N_s) - 1\right)\right|}{e_s} < \frac{1 + N^{\gamma}\left(\frac{N^{2\gamma}}{(\frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}+2)\sqrt{N}}\right)}{N^{\alpha}}$$

$$< \sqrt{\frac{a^j}{b^i}} N^{3\gamma - \frac{1}{2} - \alpha}.$$

Hence, we get

$$\left| k\frac{\left(N_s - \frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} + 1\right)}{e_s} - d_s \right| < \sqrt{\frac{a^j}{b^i}} N^{3\gamma - \frac{1}{2} - \alpha}.$$

We proceed to show the existence of integer k and t integers d_s. Let $\varepsilon = \sqrt{\frac{a^j}{b^i}} N^{3\gamma - \frac{1}{2} - \alpha}$ and $\gamma = \frac{t(2\alpha+1)}{2(3t+1)}$. Then, we get

$$N^{\gamma}\varepsilon^s = N^{\gamma}\left(\sqrt{\frac{a^j}{b^i}} N^{3\gamma - \frac{1}{2} - \alpha}\right)^t = \left(\frac{a^j}{b^i}\right)^{\frac{t}{2}} N^{\gamma + 3\gamma t - \alpha t - \frac{t}{2}} = \left(\frac{a^j}{b^i}\right)^{\frac{t}{2}}.$$

Following Theorem 2.4, $\left(\frac{a^j}{b^i}\right)^{\frac{t}{2}} < 2^{\frac{t(t-3)}{4}} \cdot 3^t$ for $t \geq 3$, which gives $N^{\gamma}\varepsilon^t < 2^{\frac{t(t-3)}{4}} \cdot 3^t$. It follows that if $k < N^{\gamma}$ then $k < 2^{\frac{t(t-3)}{4}} \cdot 3^t \cdot \varepsilon^{-t}$ $s = 1, \ldots, t$, yields

$$\left| k\frac{\left(N_s - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_s}+1\right)}{e_s} - d_s \right| \quad < \quad \varepsilon. \tag{5}$$

This clearly satisfies the conditions of Theorem 2.4, and proceeds to reveal t integers of the private key d_s and integer k for $s = 1, \ldots, t$. Next, from equation $e_s d_s - k\phi(N_s) = 1$ it computes

$$\phi(N_s) = \frac{e_s d_s - 1}{k}$$
$$p_s + q_s = N_s - \phi(N - s) + 1$$

Finally, by finding the roots of $x^2 - (N_s - \phi(N_s) + 1)x + N_s = 0$, the prime factors p_s and q_s can be revealed, which lead to the factorization of t RSA moduli N_s for $s = 1, \ldots, t$ in polynomial time. □

Let

$$X_1 = \frac{N_1 - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_1}+1}{e_1}, X_2 = \frac{N_2 - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_2}+1}{e_2},$$
$$X_3 = \frac{N_3 - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_3}+1}{e_3}.$$

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 suitable small positive integers a ,b, i and j, 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 $(N_s, e_s, \alpha, \gamma)$ satisfying Theorem 3.3.
Choose a, b, i, j and t to be suitable small positive integers and $N = \max\{N_s\}$ for $s = 1, \ldots, t$.
for any $(a, b, i, j, t, N, \alpha, \gamma)$ **do**
    $\varepsilon = \sqrt{\frac{a^j}{b^i}} N^{3\gamma - \frac{1}{2} - \alpha}$
    $e =: \min\{e_s\} := N^{\alpha}$
    $T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}]$ 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**
    $\phi(N_s) := \frac{e_s d_s - 1}{k}$
    $W_s := N_s - \phi(N_s) + 1$.
end for
Solve the quadratic equation $x^2 - W_s x + N_s = 0$
return the prime factors (p_s, q_s).

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

$$N_1 = 508565684954735704742859784656696946682831034301$$

$$N_2 = 538297617783655149718818584876174245121129308529$$

$$N_3 = 806652571994509083587232759066368614950521970341$$

$$e_1 = 402089808843533444904596100065217739786701579763$$

$$e_2 = 266594837211606419072917791334185782377107161886 7$$

$$e_3 = 77889826929125521984112854311060356924922908720 5.$$

Observe that

$$\begin{aligned} N =& \max\{N_1, N_2, N_3\} \\ =& 80665257199450908358723275906636861495052197034 1 \end{aligned}$$

$$\begin{aligned} e_s =& \min\{e_1, e_2, e_3\} \\ =& 40208980884353344490459610006521773978670157976 3 \end{aligned}$$

with $e_s = \min\{e_1, e_2, e_3\} = N^{\alpha}$ *with* $\alpha = 0.9936884923$. *We have from Algorithm 2,* $\gamma = \frac{t(2\alpha+1)}{2(3t+1)} = 0.4481065478$ *and* $\varepsilon = \sqrt{\frac{a^j}{b^i}} N^{3\gamma-\frac{1}{2}-\alpha} = 0.00000000975180072$.
Applying Theorem 2.4 and using Algorithm 2 yields

$$T = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}] = 59708205450000000000000000000000. \quad (6)$$

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 $\mathcal{L}$, we obtain the reduced basis with the following matrix,

$$K = \begin{pmatrix} 8051197063831403672974 & -3316380041905576226082 & -7576826145122107544902 & -9125191037758557249748 \\ -103794926253749172 & 18949362994951243653996 & -100228550582566088 2044 & -4749905122361928365256 \\ -8263862147578873962789 & -870743310198078857373 & 116814601892234447318 97 & -2666682545953491710 5122 \\ 1942608954800067181 9143 & 4545536643713249211951 & 171578911820217476504 61 & -1003520731256162001 7386 \end{pmatrix}$$

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

$$Q = \begin{pmatrix} 8051197063831403672974 & 10183203999249594565037 & 162566546490440512 5824 & 8338083515173059332873 \\ -103794926253749172 & -131280466711866427 & 20957855795262523 & -107493426964156141 \\ -8263862147578873962789 & 10452184116634451867331 & -16686059468598602341 43 & -8558326444887642738452 \\ 1942608954800067181 9143 & 2457023858770669410 5398 & 392243819719606680 0948 & 2011829492437969962 3746 \end{pmatrix}$$

From the second row of matrix Q we obtain k d_1, d_2 and d_3 as follows:

$$k = 103794926253749172,\ d_1 = 131280466711866427$$

$$d_2 = 20957855795262523,\ d_3 = 107493426964156141.$$

Using Algorithm 2, we compute $\phi(N_s) = \frac{e_s d_s - 1}{k}$ for $s = 1, 2, 3$. That is,

$$\phi(N_1) = 508565684954735704742858186345678007454703934400$$

$$\phi(N_2) = 538297617783655149718817110111669468997568641520$$

$$\phi(N_3) = 806652571994509083587230960661198002649532119232.$$

Next, from Algorithm 2 we proceed to compute W_s for $s = 1, 2, 3$.

$$W_1 = 1598311018939228127099902$$

$$W_2 = 1474764504776123560667010$$

$$W_3 = 179840517061230098985111 0.$$

Finally, solving $x^2 - W_s x + N_s = 0$ for $s = 1, 2, 3$ yields (p_1, q_1), (p_2, q_2), and (p_3, q_3) which lead to the factorization of three RSA moduli N_1, N_2, N_3. That is,

$$p_1 = 1159826888096893980482861\ q_1 = 438484130842334146617041$$
$$p_2 = 663660014540611073510141,\ q_2 = 811104490235512487156869$$
$$p_3 = 942937210338906570661877,\ q_3 = 855467960273394419189233.$$

From our result, one can observe that we get $\min\{d_1, d_2, d_3\} \approx N^{0.340}$ which is larger than Blömer and May's bound of $x < \frac{1}{3}N^{0.25}$, as reported in Blömer and May (2004). Our $\min\{d_1, d_2, d_3\} \approx N^{0.340}$ is also greater than $\min\{d_1, d_2, d_3\} \approx N^{0.337}$, as reported in Nitaj et al. (2014).

3.2.3 The Attack on t RSA Moduli $N_s = p_s q_s$ Satisfying $e_s d - k_s \phi(N_s) = z_s$

This section considers another case in which t RSA moduli satisfies t 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 $s \geq 2$, let $N_s = p_s q_s$, $s = 1, \ldots, t$. The attack works for t instances of public key pair (N_s, e_s) if there exists integer d and t integers k_s, such that equation $e_s d - k_s \phi(N_s) = z_s$ is satisfied. It shows that the prime factors p_s and q_s of t RSA moduli N_s can be factored efficiently for $N = \max\{N_s\}$ and $d, k_s, z_s < N^{\gamma}$, for all $\gamma = \frac{3t}{2(4t+1)}$ where $\frac{1}{4} \leq \gamma \leq \frac{1}{2}$. In this case, the RSA instances shared common decryption exponent d.

Theorem 3.4. *Let $N_s = p_s q_s$ be RSA moduli, (e_s, N_s) be public key pair and $(d,\ p_s, q_s)$ be private keys with $e_s < \phi(N_s)$ and $e_s d \equiv 1 \pmod{\phi(N_s)}$ is satisfied. Let $N = \max\{N_s\}$. If there exists positive integers $d, k_s, z_s < N^{\gamma}$, for all $\gamma = \frac{3t}{2(4t+1)}$ such that $e_s d - k_s \phi(N_s) = z_s$ holds, then prime factors p_s and q_s of t moduli N_s can be recovered successfully in polynomial time for $s = 1, \ldots, t$, $t \geq 2$, $j = 3, \ldots, i$ and $\frac{1}{4} \leq \gamma \leq \frac{1}{2}$..*

Proof. For $t \geq 2$, $j = 3, \ldots, i$ and suppose $N_s = p_s q_s$, be t moduli. Let $N = \max\{N_s\}$ and suppose that $k_s < N^{\gamma}$ for $s = 1, \ldots, t$. Then equation $e_s d - k_s \phi(N_s) = z_s$ can be rewritten as

$$e_s d - k_s(N_s - (p_s + q_s) + 1) = z_s$$

$$e_s d - k_s \left(N_s - \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N_s} + \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N_s} - (N_s - \phi(N_s) + 1) + 1 \right) = z_s.$$

Then,

$$\left| \frac{e_s}{N_s - \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N_s} + 1} d - k_s \right| = \frac{\left| z_s + k_s \left(\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N_s} - N_s + \phi(N_s) - 1 \right) \right|}{N_s - \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N_s} + 1}. \tag{7}$$

Taking N= $\max\{N_s\}$ and suppose that $k_s, z_s < N^{\gamma}$ are positive integers. From Theorem 3.1, it has been established that

$$\begin{aligned} \left| \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N_s} + \phi(N_s) - N_s - 1 \right| &< \frac{N^{2\gamma}}{(\frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} + 2)\sqrt{N}} \\ N_s - \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N_s} + 1 &> \frac{a^j + b^i}{2a^j} N. \end{aligned}$$

Putting the conditions into equation (7) yields

$$\begin{aligned}
&\frac{\left|z_s - k_s\left(N_s - \phi(N_s) + 1 - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_s}\right))\right|}{N_s - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_s} + 1} \\
&\leq \frac{\left|z_s + k_s\left(\frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_s} - N_s + \phi(N_s) - 1\right)\right|}{N_s - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_s} + 1} \\
&< \frac{N^\gamma + N^\gamma\left(\frac{N^{2\gamma}}{(\frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}+2)\sqrt{N}}\right)}{\frac{a^j+b^i}{2a^j}N} \\
&< \frac{N^{4\gamma-\frac{1}{2}}}{N} \\
&< \sqrt{\frac{a^j}{b^i}}N^{4\gamma-\frac{3}{2}}.
\end{aligned}$$

Then

$$\left|\frac{e_s}{N_s - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_s} + 1}d - k_s\right| < \sqrt{\frac{a^j}{b^i}}N^{4\gamma-\frac{3}{2}}.$$

We now proceed to show the existence of integer d and t integers k_s, let $\varepsilon = \sqrt{\frac{a^j}{b^i}}N^{4\gamma-\frac{3}{2}}$, with $\gamma = \frac{3t}{2(4t+1)}$. Then it gives

$$N^\gamma\varepsilon^t = N^\gamma\left(\sqrt{\frac{a^j}{b^i}}N^{4\gamma-\frac{3}{2}}\right)^t = \left(\sqrt{\frac{a^j}{b^i}}\right)^t N^{\gamma+4\gamma t-\frac{3t}{2}} = \left(\frac{a^j}{b^i}\right)^{\frac{t}{2}}.$$

Following Theorem 2.4, $\left(\frac{a^j}{b^i}\right)^{\frac{t}{2}} < 2^{\frac{t(t-3)}{4}}\cdot 3^t$ for $t \geq 3$, which gives $N^\gamma\varepsilon^t < 2^{\frac{t(t-3)}{4}}\cdot 3^t$. It follows that if $d < N^\gamma$ then $d < 2^{\frac{t(t-3)}{4}}\cdot 3^t\cdot\varepsilon^{-t}$ for $s = 1, \ldots, t$, yields

$$\left|\frac{e_s}{N_s - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_s} + 1}d - k_s\right| < \varepsilon, \qquad d < 2^{\frac{t(t-3)}{4}}\cdot 3^t\cdot\varepsilon^{-t}.$$

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:

$$\phi(N_s) = \frac{e_s d - z_s}{k_s}$$
$$p_s + q_s = N_s - \phi(N_s) + 1.$$

Finally, by finding the roots of $x^2 - (N_s - \phi(N_s) + 1)x + N_s = 0$, the prime factors p_s and q_s can be revealed, which lead to the factorization of t RSA moduli N_s for $s = 1, \ldots, t$ in polynomial time. □

Let

$$X_1 = \frac{e_1}{N_1 - \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_1} + 1},$$
$$X_2 = \frac{e_2}{N_2 - \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_2} + 1},$$
$$X_3 = \frac{e_3}{N_3 - \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_3} + 1}.$$

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,

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

Taking suitable small positive integers a, b, i and j 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, z_s, γ) satisfying Theorem 3.4.
Choose a, b, i, j and t to be suitable small positive integers and $N = \max\{N_s\}$ for $s = 1, \ldots, t$.
for any $(a, b, i, j, t, N, \gamma)$ **do**
    $\varepsilon = \sqrt{\frac{a^j}{b^i}} N^{4\gamma - \frac{3}{2}}$
    $T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}]$ 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, z_s) **do**
    $\phi(N_s) := \frac{e_s d - z_s}{k_s}$
    $W_s := N_s - \phi(N_s) + 1$.
end for
Solve the quadratic equation $x^2 - W_s x + N_s = 0$
return the prime factors (p_s, q_s).

Example 3.4. *In what follows, we give a numerical example to illustrate how Theorem 3.4 works on three RSA moduli and their corresponding public exponents:*

$$\begin{aligned} Let\ N_1 &= 330296126221226061978488805127502203372577 \\ N_2 &= 187396362359066080307391868109309718740567 \\ N_3 &= 216436372402461777072305279786697609409967 \\ e_1 &= 302169635060396919768302245253373846319703 \\ e_2 &= 911994187853057959476450048099985565326 21 \\ e_3 &= 162134135066593548250015517503190950433936. \end{aligned}$$

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

$$N = 330296126221226061978488805127502203372577.$$

By using $a = 3$, $b = 2$, $j = 3$, $i = 4$ *and since* $t = 3$, *we have from Algorithm 3,* $\gamma = \frac{3t}{2(4t+1)} = 0.3461538462$ *and* $\varepsilon = \sqrt{\frac{a^j}{b^i}} N^{4\gamma - \frac{3}{2}} = 0.00002104606015$. *Using Algorithm 3, for* $n = t = 3$ *we compute*

$$T = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}] = 206429515900000000000. \tag{8}$$

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

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

Therefore, by applying LLL algorithm to $\mathcal{L}$, we obtain the reduced basis with the following matrix:

$$K = \begin{pmatrix} 221202829045687 & 185504894439445 & 185504894439445 & 57393070403596 \\ -223267679085378 & 501267471654170 & -2635612410692192 & -2635612410692192 \\ 648416042445503 & -1951421870899795 & 149685816490192 & 3013842083722924 \\ 1886353284926810 & -1977885223309650 & -1608797804624160 & -1052325529382520 \end{pmatrix}$$

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

$$Q = \begin{pmatrix} 221202829045687 & 202366218737588 & 107651873220345 & 165704724042021 \\ -223267679085378 & -204255235693633 & -108656765317118 & -167251518933801 \\ 648416042445503 & 593199929876965 & 315561974937328 & 485733396093500 \\ 1886353284926810 & 1725720159731879 & 918023813500959 & 1413081613255486 \end{pmatrix}$$

From the first row of matrix Q, we obtain $d,\ k_1, k_2$ and k_3 as follows:

$$d = 221202829045687,\ k_1 = 202366218737588,$$
$$k_2 = 107651873220345,\ k_3 = 165704724042021.$$

Using Algorithm 3, we compute $\phi(N_s) = \frac{e_s d - z_s}{k_s}$ for $s = 1, 2, 3$ where z_1, z_2 and z_3 are:

$$z_1 = 78214488852833,\ z_2 = 81546995635627,\ z_3 = 268274979696656$$

$$\phi(N_1) = 330296126221226061977286874278835760293956$$

$$\phi(N_2) = 187396362359066080306393381432741963476000$$
$$\phi(N_3) = 216436372402461777071093307335033501180256.$$

Next, from Algorithm 3, we compute W_s for $s = 1, 2, 3$.

$$W_1 = 1201930848666443078622$$
$$W_2 = 998486676567755264568$$
$$W_3 = 1211972451664108229712.$$

Finally, solving $x^2 - W_s x + N_s = 0$ for $s = 1, 2, 3$ yields (p_1, q_1), (p_2, q_2), and (p_3, q_3) which lead to the factorization of three RSA moduli N_1, N_2, N_3. That is

$$p_1 = 776645004884812569823 \; q_1 = 425285843781630508799$$
$$p_2 = 747935011770876784817, \; q_2 = 250551664796878479751$$
$$p_3 = 994294007747013311743 \; q_3 = 217678443917094917969.$$

From our result, one can observe that we get $d \approx N^{0.3455}$ which is larger than Blömer and May's bound of $x < \frac{1}{3}N^{0.25}$, as reported in Blömer and May (2004). Our $d \approx N^{0.3455}$ is also greater than $d \approx N^{0.344}$, as reported by Nitaj et al. (2014).

3.2.4 The Attack on t RSA Moduli $N_s = p_s q_s$ Satisfying $e_s d_s - k\phi(N_s) = z_s$

This section presents another case in which t RSA moduli satisfies t 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 $s = 1, \ldots, t$ which can be simultaneously factored in polynomial time. In this case, every pair of the RSA instances has its own unique decryption exponent d_s.

Theorem 3.5. *Let $N_s = p_s q_s$ be t RSA moduli for $s = 1, \ldots, t$, $t \geq 2$ and $j = 3, \ldots, i$. Let (e_s, N_s) be public key pair, (d_s, N_s) be private key pair with $e_s < \phi(N_s)$ and $e_s d_s \equiv z_s \pmod{\phi(N_s)}$ is satisfied. Let $e_= \min\{e_s\} = N^\alpha$ be public exponent. If there exists positive integers $d_s, k, z_s < N^\gamma$,for all $\gamma = \frac{t(2\alpha+1)}{2(3t+1)}$ such that $e_s d_s - k\phi(N_s) = z_s$ holds, then prime factors p_s and q_s of t RSA moduli N_s can be successfully recovered in polynomial time for $s = 1, \ldots, t$, $\frac{1}{4} \leq \gamma \leq \frac{1}{2}$ and $0 < \alpha < 1$.*

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

$$e_s d_s - k(N_s - (p_s + q_s) + 1) = z_s$$

$$e_s d_s - k\left(N_s - \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} + \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} - (N_s - \phi(N_s) + 1) + 1\right) = z_s.$$

Then, we get

$$\left| k\frac{\left(N_s - \frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} + 1\right)}{e_s} - d_s \right| = \frac{\left| z_s + k\left(\frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} - N_s + \phi(N_s) - 1\right)\right|}{e_s}.$$

Taking $N = \max\{N_s\}$, $d_s, k, z_s < N^{\gamma}$ be positive integers for $s = 1, \ldots, t$. From Theorem 3.1, it was shown that:

$$\left| \frac{a^j + b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} + \phi(N_s) - N_s - 1 \right| < \frac{N^{2\gamma}}{(\frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} + 2)\sqrt{N}}.$$

Also, suppose $e = \min\{e_s\} = N^{\alpha}$, then we have:

$$\frac{\left| z_s + k\left(\frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} - N_s + \phi(N_s) - 1\right)\right|}{e_s} < \frac{N^{\gamma} + N^{\gamma}\left(\frac{N^{2\gamma}}{(\frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}+2)\sqrt{N}}\right)}{N^{\alpha}}$$

$$< \sqrt{\frac{a^j}{b^i}} N^{3\gamma - \frac{1}{2} - \alpha}.$$

Hence,we get

$$\left| k\frac{\left(N_s - \frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N_s} + 1\right)}{e_s} - d_s \right| < \sqrt{\frac{a^j}{b^i}} N^{3\gamma - \frac{1}{2} - \alpha}.$$

We now proceed to show the existence of integer k and t integers d_s. Let $\varepsilon = \sqrt{\frac{a^j}{b^i}} N^{3\gamma - \frac{1}{2} - \alpha}$ and $\gamma = \frac{t(2\alpha+1)}{2(3t+1)}$. Then it gives

$$N^{\gamma}\varepsilon^t = N^{\gamma}\left(\sqrt{\frac{a^j}{b^i}} N^{3\gamma - \frac{1}{2} - \alpha}\right)^t = \left(\sqrt{\frac{a^j}{b^i}}\right)^t N^{3\gamma t - \frac{t}{2} - t\alpha} = \left(\frac{a^j}{b^i}\right)^{\frac{t}{2}}.$$

Following Theorem 2.4, $\left(\frac{a^j}{b^i}\right)^{\frac{t}{2}} < 2^{\frac{t(t-3)}{4}} \cdot 3^t$ for $t \geq 2$, which gives $N^{\gamma}\varepsilon^t < 2^{\frac{t(t-3)}{4}} \cdot 3^t$. It follows that if $k < N^{\gamma}$ then $k < 2^{\frac{t(t-3)}{4}} \cdot 3^t \cdot \varepsilon^{-t}$ for $s = 1, \cdots, t$, yields

$$\left| k\frac{\left(N_s - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_s} + 1\right)}{e_s} - d_s \right| < \varepsilon.$$

This clearly satisfies 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 $e_s d_s - k\phi(N_s) = z_s$, we compute:

$$\phi(N_s) = \frac{e_s d_s - z_s}{k}$$
$$p_s + q_s = N_s - \phi(N - s) + 1.$$

Finally, by finding the roots of $x^2 - (N_s - \phi(N_s) + 1)x + N_s = 0$, the prime factors p_s and q_s can be revealed, which lead to the factorization of t RSA moduli N_s for $s = 1, \ldots, t$ in polynomial time. □

Let

$$X_1 = \frac{N_1 - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_1} + 1}{e_1},$$
$$X_2 = \frac{N_2 - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_2} + 1}{e_2},$$
$$X_3 = \frac{N_3 - \frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N_3} + 1}{e_3}.$$

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,

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

Taking suitable small positive integers a, b, i and j, 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 $(N_s, e_s, z_s, \alpha, \gamma)$ satisfying Theorem 3.5.
Choose a, b, i, j and t to be suitable small positive integers and $N = \max\{N_s\}$ for $s = 1, \ldots, t$.
for any $(a, b, i, j, t, N, \gamma)$ **do**
    $\varepsilon = \sqrt{\frac{a^j}{b^i}} N^{3\gamma - \frac{1}{2} - \alpha}$
    $e =: \min\{e_s\} := N^{\alpha}$
    $T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}]$ 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**
    $\phi(N_s) := \frac{e_s d_s - z_s}{k}$
    $W_s := N_s - \phi(N_s) + 1$.
end for
Solve the quadratic equation $x^2 - W_s x + N_s = 0$
return the prime factors (p_s, q_s).

Example 3.5. *In what follows, we give a numerical example to illustrate how Theorem 3.5 works on three RSA Moduli and their corresponding public exponents:*

$$\begin{aligned}
N_1 &= 23547757941627229475592099212811204040914831 1\\
N_2 &= 83117499153465873111806329950673253331346816 9\\
N_3 &= 97737298192120643035019005945418825197014374 3\\
e_1 &= 38796943249846315733671518375477598229207909\\
e_2 &= 58672293873164211628641295459464906640454441\\
e_3 &= 49895674246929693821750986970186909558125828.
\end{aligned}$$

Observe that

$N = \max\{N_1, N_2N_3\} = 977372981921206430350190059454188251970143743.$

$e_s = \min\{e_1, e_2e_3\} = 38796943249846315733671518375477598229207909$

with $e_s = \min\{e_1, e_2e_3\} = N^{\alpha}$ *for* $\alpha = 0.9688539474$. *Since* $t = 3$, *we have* $\gamma = \frac{t(2\alpha+1)}{2(3t+1)} = 0.4406561842$, Applying Theorem 2.4 and using Algorithm 4, we compute

$$T = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}] = 385921063000000000000000000. \quad (9)$$

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

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

Taking $a = 3, b = 2, j = 3, i = 4, t = 3$.
Therefore, by applying the LLL algorithm to $\mathcal{L}$, we obtain the reduced basis with the following matrix,

$$K = \begin{pmatrix} -258385025665326 & 37991546648123867848 & 27196940459134138062 & -30693403032299059072 \\ -446111740960603908141 & 245661989555708003468 & 89550637443021325283 & 247534007918421869248 \\ -765709654369103205185 & -368855289174869031620 & -54097411326677039345 & -54097411326677039345 \\ -145325909385583133694 & -531251521480873120888 & -169844573607345559 5678 & 87445594955809691 7632 \end{pmatrix}$$

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

$$Q = \begin{pmatrix} -258385025665326 & -1568264798833691 & -3660384780324555 & -5061331404572551 \\ -446111740960603908141 & -2707669834555799110441 & -631979590431589598 2054 & -873858443870124431 6363 \\ -765709654369103205185 & -464746551771758854 8099 & -108473467368444396 35557 & -149989741489992626 83205 \\ -145325909385583133694 & -882053855331017641771 & -205874448618714521 2854 & -284669201389414322 0284 \end{pmatrix}$$

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

$$k = 258385025665326,\ d_1 = 1568264798833691,$$
$$d_2 = 3660384780324555,\ d_3 = 5061331404572551.$$

Using Algorithm 4, we compute $\phi(N_s) = \frac{e_s d_s - z_s}{k}$ for $s = 1, 2, 3$, where z_1, z_2, z_3 are :

$$z_1 = 1077318360002647,\ z_2 = 722423181715659\ z_3 = 1957330455972268$$

$$\phi(N_1) = 23547757941627229475588776707565084721550607 2$$
$$\phi(N_2) = 83117499153465873111800525492769622627573939 6$$
$$\phi(N_3) = 97737298192120643035012691725617854628623796 0.$$

Next, from Algorithm 4 we compute W_s for $s = 1, 2, 3$.

$$W_1 = 33225052461193193642240$$
$$W_2 = 58044579036307037728774$$
$$W_3 = 63142198009705683905784.$$

Finally, solving $x^2 - (N_s - W_s x + N_s = 0$ for $s = 1, 2, 3$ yields (p_1, q_1), (p_2, q_2), and (p_3, q_3), which lead to the factorization of three RSA moduli N_1, N_2, N_3. That is,

$$p_1 = 22976365350655154588653\ q_1 = 10248687110538039053587$$
$$p_2 = 32356700611714851032147\ q_2 = 25687878424592186696627$$
$$p_3 = 35971247917448150598803\ q_3 = 27170950092257533306981.$$

From our result, one can observe that we get $\min\{d_1, d_2, d_3\} \approx N^{0.337}$ which is larger than Blomer and May's bound of $x < \frac{1}{3}N^{0.25}$, as reported in Blömer and May (2004).

4 CONCLUSION

This paper proposed and mounted a successful cryptanalysis attack on RSA moduli $N = pq$ using generalized prime difference method which produced an improved decryption exponent bound $d < \sqrt{\frac{a^j+b^i(b^i-2)}{2b^i}}N^{\frac{3}{4}-\gamma}$. The paper also presented four attacks that successfully led to the factorization of t RSA moduli $N_s = p_s q_s$ using simultaneous Diophantine approximations and LLL algorithm. In all the reported attacks, we improved the decryption exponent bound.

ACKNOWLEDGMENTS

This research work is funded by the Fundamental Research Grant Scheme provided by Institute For Mathematical Research, Univesiti Putra Malaysia.

REFERENCES

Asbullah, M. A. (2015). *Cryptanalysis on the Modulus $N = p^2q$ and Design of Rabin-like Cryptosystem without Decryption failure*. PhD thesis, Universiti Putra Malaysia.

Bach, E. Miller, G. and Shallit, J. (1986). Sums of divisors, perfect numbers and factoring. *SIAM Journal on Computing*, 15(4):1143–1154.

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

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

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

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

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

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

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

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

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

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

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