cryptography

MDPI

Article

New Cryptanalytic Attack on RSA Modulus $N = pq$ Using Small Prime Difference Method

Muhammad Rezal Kamel Ariffin [1,2,†], Saidu Isah Abubakar [1,*,†], Faridah Yunos [1,2,†] and Muhammad Asyraf Asbullah [1,3,†]

1 Al-Kindi Cryptography Research Laboratory, Institute for Mathematical Research, Universiti Putra Malaysia, Selangor 43400, Malaysia; rezal@upm.edu.my (M.R.K.A.); faridahy@upm.edu.my (F.Y.); ma_asyraf@upm.edu.my (M.A.A.)

2 Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, Selangor 43400, Malaysia

3 Centre of Foundation Studies for Agriculture Science, Universiti Putra Malaysia, Selangor 43400, Malaysia

* Correspondence: siabubakar82@gmail.com

† These authors contributed equally to this work.

Received: 1 November 2018; Accepted: 15 December 2018; Published: 20 December 2018

Abstract: This paper presents new short decryption exponent attacks on RSA, which successfully leads to the factorization of RSA modulus $N = pq$ in polynomial time. The paper has two parts. In the first part, we report the usage of the small prime difference method of the form $|b^2p - a^2q| < N^{\gamma}$ where the ratio of $\frac{q}{p}$ is close to $\frac{b^2}{a^2}$, which yields a bound $d < \frac{\sqrt{3}}{\sqrt{2}} N^{\frac{3}{4}-\gamma}$ from the convergents of the continued fraction expansion of $\frac{e}{N-\lceil \frac{a^2+b^2}{ab}\sqrt{N}\rceil+1}$. The second part of the paper reports four cryptanalytic attacks on t instances of RSA moduli $N_s = p_s q_s$ for $s = 1, 2, \ldots, t$ where we use $N - \lceil \frac{a^2+b^2}{ab}\sqrt{N}\rceil + 1$ as an approximation of $\phi(N)$ satisfying generalized key equations of the shape $e_s d - k_s \phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s \phi(N_s) = z_s$, and $e_s d_s - k\phi(N_s) = z_s$ for unknown positive integers d, k_s, d_s, k_s, and z_s, where we establish that t RSA moduli can be simultaneously factored in polynomial time using combinations of simultaneous Diophantine approximations and lattice basis reduction methods. In all the reported attacks, we have found an improved short secret exponent bound, which is considered to be better than some bounds as reported in the literature.

Keywords: RSA modulus; primes difference; cryptanalysis; short decryption exponent; attacks; continued fraction

1. Introduction

The RSA cryptosystem is the most widely used public key cryptosystem, invented by three mathematicians, Rivest, Shamir, and Adleman [1] and since then has been extensively used for many applications in the government as well as commercial domain, which include e-banking, secure telephone, smart cards, and communications in different types of networks [2].

RSA key generation involves a random selection of two distinct large prime numbers such that their product is represented as $N = pq$ and called an RSA modulus. The Euler totient function $\phi(N)$ is computed as $\phi(N) = (p-1)(q-1)$. Additionally, choose an integer $e < \phi(N)$ such that $\gcd(e, \phi(N)) = 1$ and compute short decryption exponent d such that the relation $ed \equiv 1 \pmod{\phi(N)}$ is satisfied. Then, (e, N) are the public pair and (d, p, q) are private key tuple.

The encryption function is computed by choosing a message $M \in \mathbb{Z}_N$ and computing the ciphertext $C = M^e \pmod{N}$, while the plaintext can be recovered by computing the decryption exponent from equation $M = C^d \pmod{N}$. The primes p and q in most cases are considered to have same bit-length.

In simpler terms, an RSA cryptosystem involves three processes of key generation, encryption, and decryption algorithms as presented in Algorithms 1–3 below:

Algorithm 1 RSA key generation

Initialization: Input the size n and (e, N).
Choose two random and distinct $n - bit$ strong primes (p, q).
for each pair of the form (p, q) **do**
    $N := pq$
    $\phi(N) := (p-1)(q-1)$
end for
Choose a random integer e such that $1 < e < \phi(N)$ and $\gcd(e, \phi(N)) = 1$.
if d is an integer **then**
    $ed \equiv 1 \pmod{\phi(N)}$.
end if
return the public key pair (N, e) and the private key pair (N, d).

Algorithm 2 RSA encryption

Initialization: Input the public key pair (e, N) and the plaintext M.
Represents the plaintext message M as integer such that $M < N$ and $\gcd(M, N) = 1$.
for each triplet of the form (e, N, M) **do**
    $C := M^e \pmod{N}$
end for
return the ciphertext C.

Algorithm 3 RSA decryption

Initialization: Input the private key pair (d, N) and the ciphertext C.
for each triplet of the form (d, N, C) **do**
    $M := C^d \pmod{N}$
end for
return the message M.

The security of an RSA cryptosystem depends on the difficulty of solving the integer factorization problem, the failure of an adversary to compute the secret key d from RSA key equation $ed = 1 + k\phi(N)$, where only the public key e is given as outlined in Algorithm 1 and the difficulty of solving the e^{th}-root problem of $C = M^e \pmod{N}$ as outlined in Algorithm 2. The problem of computing d from (e, N) is equivalent to the problem of factoring RSA modulus N into its nontrivial prime factors of p and q, as proven by Reference [3]. 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.

In an RSA cryptosystem, there are public key pairs (e, N) and private key tuples $(d, p, q, \phi(N))$. Once the private key d is known, it can lead to the total break of RSA. It is often tempting to use a small decryption exponent so as to speed up computation in RSA decryption and signature verification. However, this poses a great security challenge to the system. A very small decryption exponent can be broken by a trivial brute force exhaustive search to find the correct decryption exponent. For instance, all private exponents $d < 2^{60}$ can be recovered easily, but it is computationally infeasible to recover all private exponents $d < 2^{80}$ by brute force attack [4].

The first attack on small decryption exponent was reported by Wiener in 1990. He showed that RSA is insecure if the small decryption exponent is $d < \frac{1}{3}N^{0.25}$ using the continued fractions method to recover d from the convergents of the continued fractions expansion of $\frac{e}{N}$, [5]. Since then, many attacks on short decryption exponents emerged, which improved the bound. Boneh and Durfee (1999) proposed an attack on the small decryption exponent using the Coppersmith lattice-based technique, in which they heuristically showed that RSA in insecure if $d < N^{0.292}$, as reported by Reference [6].

In another development, B. De Weger (2002) also used the primes difference method to carry out an attack on RSA modulus $N = pq$, where he proved that if $d < \frac{N^{\frac{3}{4}}}{|p-q|}$, then the RSA cryptosystem is considered to be insecure where primes p and q have the same bit-length, which is an improvement on Wiener's bound as reported by Reference [7]. In addition, Maitra and Sarkar (2008) improved the work of Reference [7] using the prime difference method of $|2q - p| < N^{\gamma}$ and showed that RSA is not secure if $d < N^{\frac{1-\gamma}{2}}$, as reported by Reference [8].

Furthermore, Chen's et al. (2009) have generalized the work of Reference [7], where they proposed an attack using the generalization method, in which they proved that RSA modulus $N = pq$ can be broken if $|ap - bq| = N^{\gamma}$ and $d < N^{\frac{3}{4}-\gamma}$, where the ratio of two primes $\frac{p}{q}$ is very near to the ratio $\frac{b}{a}$, where $p < q < 2p$, a, and b are small positive integers less than $\log N$, then the RSA modulus can be factored from the convergents of the continued fraction expansion of $\frac{e}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}+1}$. Substituting $a = b = 1$ gave the approximation of $\phi(N)$ as reported by [7]. Also, taking $a = 2$ and $b = 1$ gave approximation of $\phi(N)$ as reported by Reference [8]. In their experiment result, they used the value of $\gamma = 0.5$ to justify their theorem, as reported by Reference [9] .

Nitaj (2013) improved Wiener's bound to $d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$, as reported by Reference [10]. Asbullah (2015) also improved Wiener's bound to $d < \frac{1}{2}N^{\frac{1}{4}}$, as reported [11].

This paper reports the use of the small prime difference method to factor the RSA modulus N and its relation to further extend the bound of weak decryption exponents. Given public key pair (e, N), we exploited RSA key equation $ed = 1 + k\phi(N)$ and broke the instances of RSA by factoring the modulus N into its nontrivial prime factors p and q. We also reported four cryptanalytic attacks on factoring t RSA moduli using a system of equations where, in one instance, the moduli (e_s, N_s) shared a common decryption exponent d and, in another scenario, every pair (e_s, N_s) had its own unique decryption exponent d_s. The method uses $|b^2p - a^2q| < N^{\gamma}$ such that if the ratio of $\frac{q}{p}$ is close to the ratio of $\frac{b^2}{a^2}$, where a and b are small positive integers and $0.25 < \gamma \leq 0.5$, then private key $d < \frac{\sqrt{3}}{\sqrt{2}}N^{\frac{3}{4}-\gamma}$ can be efficiently recovered from the convergents of the continued fraction expansion of $\frac{e}{N-\lceil\frac{a^2+b^2}{ab}\sqrt{N}\rceil+1}$. Our bound is considered to be an improved bound of that of References [5,9,11]. This paper also presents an experimental result which shows that taking $\gamma = \frac{15}{32}$, we can recover primes p and q if the private key $d < \frac{\sqrt{3}}{\sqrt{2}}N^{0.28125}$. This is an improvement of the result of Reference [9], as they did not give an experiment result of $\gamma < 0.5$.

The second part of the paper presents t instances of factoring RSA moduli $N_s = p_sq_s$ for $t = 1, 2, \ldots, t$ by transforming generalized key equations of the form $e_sd - k_s\phi(N_s) = 1$, $e_sd_s - k\phi(N_s) = 1$, $e_sd - k_s\phi(N_s) = z_s$, and $e_sd_s - k\phi(N_s) = z_s$ for unknown parameters d, k_s, d_s, k_s, and z_s into simultaneous Diophantine problem and applying the lattice basis reduction and LLL methods to find the values of d, k_s, d_s, and k. We formulated a quadratic equation which enabled us to find t prime factors p_s and q_s and finally factorize t moduli $N_1, N_2, \ldots, N_t$ in polynomial time. We have found decryption exponents bounds that are greater than those of References [12,13].

The rest of the paper is organized as follows. In Section 2, we present a review of some preliminary results on continued fractions and state some theorems that are related to our work. Section 3 presents our proposed findings and discussion on the results. We give experimental results to illustrate our theorems, which show how an incorrect choice of d can lead to the factorization of RSA modulus $N = pq$ in polynomial time. Finally, in Section 4, we conclude the paper.

2. Preliminaries and Methods

In this section, we state some basics on continued fraction, the lattice basis reduction technique, simultaneous Diophantine approximations, and theorems related to our work.

Definition 1 (Continued fractions). *For any positive $x \in \mathbb{R}$, define $x_0 = x$ and for $i = 1, 2, \ldots, n$, do $x_i = \lfloor a_i \rfloor$, $x_{i+1} = \frac{1}{x_i - a_i}$ until $x_n \in \mathbb{Z}$. Then, x can be expanded as continued fraction in following form,*

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

This expression is often used in the form $x = [a_0, a_1, a_2, \ldots, a_n, \ldots]$. Any rational number $\frac{a}{b}$ can be expressed as a finite continued fraction $x = [a_0, a_1, a_2, \ldots, a_n]$. The convergents $\frac{a}{b}$ of x are the fractions denoted by $\frac{a}{b} = [a_0, a_1, a_2, \ldots, a_i]$ for $i \geq 0$. We note that if $x = \frac{a}{b}$ is a rational number, then the continued fraction expansion of x is finite with total number of convergents being polynomial in $\log(b)$.

Definition 2. *Let $b_1, b_2, \cdots, b_m \in V$ where V is a vector space subset of $\mathbb{R}^n$. The set of vectors $b_1, b_2, \cdots, b_m \in V$ are said to be linearly dependent if there exist $x_1, \ldots, x_m \in \mathbb{R}$, which are not all zero and such that:*

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

Otherwise, they are said to be linearly independent.

Definition 3. *(Lenstra et al. 1982) Let n be a positive integer. A subset $\mathcal{L}$ of an n-dimensional real vector space $\mathbb{R}^n$ is called a lattice and if there exists a basis $b_1, \ldots, b_n$ on $\mathbb{R}^n$ such that we have the following relation $\mathcal{L} = \sum_{i=1}^{n} \mathbb{Z} b_i = \sum_{i=1}^{n} r_i b_i$ for $r_i \in \mathbb{Z}, 1 \leq i \leq n$. In this situation, we say that $b_1, \ldots, b_n$ are the basis for $\mathcal{L}$ or that they span $\mathcal{L}$.*

Definition 4. *(Nitaj, 2013) (LLL Reduction) Let $\mathcal{B} = \langle b_1 \cdots b_n \rangle$ be a basis for a lattice $\mathcal{L}$ and suppose $B^* = \langle b_1^* \cdots b_n^* \rangle$ be the associated Gram–Schmidt orthogonal basis. Let:*

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

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

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

$$||b_i^*||^2 \geq (\frac{3}{4} - \mu_{i,i-1}^2)||b_{i-1}^*||^2.$$

Theorem 1. *(Legendre's Theorem). Let α be a positive real number. If the rational numbers $(a, b) \in \mathbb{Z}$ such that $\gcd(a, b) = 1$ and:*

$$\left| \alpha - \frac{a}{b} \right| < \frac{1}{2b^2},$$

then $\frac{a}{b}$ is one of the convergents of the continued fraction expansion α.

Proof. See Reference [14]. □

Theorem 2. *(Wang et al., 2016). 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:*

$$p_1 = a_1,\ p_2 = a_2a_1 + 1, p_k = a_k p_{k-1} + p_{k-2},$$

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

for $k \geq 3$.

Theorem 3. *(Wiener, 1990). Let* $N = pq$ *be an RSA modulus with* $q < p < 2q$*. Let* $e < \phi(N)$ *be a public exponent and* d *be the corresponding private key. If* $d < \frac{1}{3}N^{\frac{1}{4}}$*, then one can factor* N *in polynomial time.*

Theorem 4. *(B. de Weger, 2002). Let* $N = pq$ *be an RSA modulus with* $q < p < 2p$ *such that* $|p - q| < N^{\beta}$ *for* $\beta = [\frac{1}{4}, \frac{1}{2}]$*, and* $N > 8d$*. Let* e *and* d *be public and private keys respectively such that* $e < \phi(N)$*, with* $\phi(N) > \frac{3}{4}N$ *and* $d < N^{\delta}$*. If* $\delta < \frac{3}{4} - \beta$*, then the convergents can be found from the continued fraction of* $\frac{e}{N - 2\sqrt{N}+1}$*, which led to the factorization of* N*.*

Theorem 5. *(Maitra-Sarkar, 2008). Let* $N = pq$ *be an RSA modulus satistying* $q < p < 2q$*. Suppose that* $|\rho q - p| \leq \frac{N^{\gamma}}{16}$ *with* $\gamma < \frac{1}{2}, 1 \leq \rho \leq 2$ *and* $d = N^{\delta}$*. Then* N *can be factored in polynomial time if* $\delta < \frac{1-\gamma}{2}$ *from the convergents of the continued fraction expansion of* $\frac{e}{N - \frac{3}{\sqrt{2}}\sqrt{N}+1}$.

Theorem 6. *(Chen et al., 2009). Let* p *and* q *be RSA primes satisfying* $p < q < 2p$*. Let* $|ap - bq| = N^{\gamma}$*. If* $\frac{q}{q}$ *is close to* $\frac{b}{a}$ *such that* $(b(a^2 + 1)p - a(b^2 + 1)q)(ap - bq) > 0$*, then the secret key* $d < N^{\frac{3}{4}-\gamma}$ *can be discovered from the convergents of* $\frac{e}{N - \frac{a+b}{\sqrt{ab}}\sqrt{N}+1}$.

Theorem 7. *(Blomer-May, 2004). Let* (N, e) *be an RSA public pair with modulus* $N = pq$ *and the prime difference* $p - q \geq cN^{\frac{1}{2}}$*. Suppose that the public exponent* $e \in \mathcal{Z}_{\phi(N)}$ *satisfies* $ex + y = k\phi(N)$ *with* $0 < x < \frac{1}{3}N^{\frac{1}{4}}$ *and* $|y| \leq N^{\frac{-3}{4}}ex$ *for* $c \leq 1$*. Then,* N *can be factored in polynomial time.*

Theorem 8. *(Lenstra et al., 1982). Let* $\mathcal{L}$ *be a lattice basis of dimension* n *having a basis* $v_1 \cdots v_n$*. The LLL algorithm produces a reduced basis* $b_1 \cdots b_n$ *satisfying the following condition:*

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

for all $1 \leq j \leq n$.

Proof. See Reference [15]. □

We will use the following Theorem 9 in our proofs of Theorems 14–17.

Theorem 9. *(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:*

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

Theorem 10. *(Nitaj et al. 2014). Let* $N_i = p_i q_i$ *for* $1 \leq i \leq k$ *be* k *RSA moduli. Let* $N = \min\{N_i\}$ *and* e_i*,* $i = 1, \ldots, k$ *be* k *public exponents. Define* $\delta = \frac{k}{2(k+1)}$*. If there exist an integer* $x < N^{\delta}$ *and* k *integers* $y_i < N^{\delta}$ *and* $|z_i| < \frac{p_i - q_i}{3(p_i+q_i)} y_i N^{1/4}$ *such that* $e_i x - y_i\phi(N_i) = z_i$ *for* $i = 1, \ldots, k$*, then one can factor* k *RSA moduli* $N_1, \ldots, N_k$ *in polynomial time.*

Theorem 11. *(Nitaj et al., 2014). Let $N_i = p_iq_i$, for $1 \leq i \leq k$ be k RSA moduli N_i where p and p are balanced primes. Let e_i, $i = 1, \ldots, k$, be k public exponents with $\min\{e_i\} = N^{\alpha}$. Define $\delta = \frac{(2\alpha-1)k}{2(k+1)}$. If there exist an integer $y < N^{\delta}$ and k integers $x_i < N^{\delta}$ and $|z_i| < \frac{p_i-q_i}{3(p_i+q_i)}yN^{1/4}$ such that $e_ix_i - y\phi(N_i) = z_i$ for $i = 1, \ldots, k$, then one can factor the k RSA moduli $N_1, \ldots, N_k$ in polynomial time.*

Theorem 12. *(Asbullah, 2015). Let $N = pq$ with $q < p < 2q$. Let $e < \phi(N)$ and d satisfy $ed \equiv 1 \bmod \phi(N)$. If $d < \frac{1}{2}N^{\frac{1}{4}}$, then $\frac{k}{d}$ is a convergent of the continued fraction $\frac{e}{N}$.*

3. The Proposed Findings and Discussion

In this section, we present our findings. The first part reported a short secret exponent attack on RSA modulus $N = pq$, where p and q are prime numbers of the same bit-length. We show that if $d < \frac{\sqrt{3}}{\sqrt{2}}N^{\frac{3}{4}-\gamma}$, then one can find $\frac{k}{d}$ from the convergents of the continued fraction expansion of $\frac{e}{N-\lceil\frac{a^2+b^2}{ab}\sqrt{N}\rceil+1}$ which leads to the factorization of RSA modulus N in polynomial time. In the second part of the paper, we presented four cryptanalytic attacks using a generalized key equation of the shape $e_sd - k_s\phi(N_s) = 1$, $e_sd_s - k\phi(N_s) = 1$, $e_sd - k_s\phi(N_s) = z_s$, and $e_sd_s - k\phi(N_s) = z_s$ for unknown integers d, k_s, d_s, k_s, and z_s. We showed that t RSA moduli $N_s = p_sq_s$ can be simultaneously factored in polynomial time where $s = 1, 2, \ldots, t$.

3.1. A Short Decryption Exponent Attack Using $|b^2p - a^2q| < N^{\gamma}$

In this section, we present two lemmas and a theorem with numerical examples.

Lemma 1. *Let p and q be prime numbers, where $q < p < 2q$ and $N = pq$. If a and b are small positive integers such that $\frac{b^2}{a^2}$ is close to $\frac{q}{p}$ for $a > b$ and $b^2p - a^2q \neq 0$, then $\phi(N) > N - \frac{a^2+b^2}{ab}\sqrt{N} + 1$.*

Proof of Lemma 1. Let $(b^2p - a^2q)(a^2p - b^2q) < 0$, then we get,

$$a^2b^2p^2 - a^4pq - b^4pq + a^2b^2q^2 < 0$$
$$a^2b^2(p^2 + q^2) < (a^4 + b^4)pq.$$

Adding $2a^2b^2pq$ to both sides we have,

$$a^2b^2(p+q)^2 < a^4 + 2a^2b^2 + b^4)pq$$
$$p + q < \frac{a^2+b^2}{ab}\sqrt{N}.$$

Then $\phi(N) > N + 1 - \frac{a^2+b^2}{ab}\sqrt{N}$. □

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

$$(a^2(b^4+1)p - b^2(a^4+1)q)(b^2p - a^2q) > 0,$$

then,

$$\frac{a^2+b^2}{ab}\sqrt{N} - (p+q) < \frac{(b^2p - a^2q)^2}{(\frac{a^2+b^2}{ab} + 2)\sqrt{N}}.$$

Proof of Lemma 2. We first compute,

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

$$
\begin{aligned}
&= \frac{(a^2+b^2)^2}{a^2b^2}N + \frac{(a^2+b^2)}{ab}\sqrt{N}(p+q) - \frac{(a^2+b^2)}{ab}\sqrt{N}(p+q) - (p+q)^2 - (b^2p-a^2q)^2 \\
&= \frac{-(a^2b^6+a^2b^2)p^2 + (a^4+2a^4b^4+b^4)pq - (a^6b^2-a^2b^2)q^2}{a^2b^2} \\
&= \frac{-(a^2(b^4+1)p - b^2(a^4+1)q)(b^2p-a^2q)}{a^2b^2}.
\end{aligned}
$$

Since $(a^2(b^4+1)p - b^2(a^4+1)q)(b^2p-a^2q) > 0$, we get,

$$
\begin{aligned}
\left(\frac{a^2+b^2}{ab}\sqrt{N} - (p+q)\right)\left(\frac{a^2+b^2}{ab}\sqrt{N} + (p+q)\right) - (b^2p-a^2q)^2 &< 0 \\
\frac{a^2+b^2}{ab}\sqrt{N} - (p+q) &< \frac{(b^2p-a^2q)^2}{\frac{a^2+b^2}{ab}\sqrt{N} + (p+q)} \\
\frac{a^2+b^2}{ab}\sqrt{N} - (p+q) &< \frac{(b^2p-a^2q)^2}{(\frac{a^2+b^2}{ab}+2)\sqrt{N}}.
\end{aligned}
$$

□

Theorem 13. *Let p and q be prime numbers, where $q < p < 2q$ and $N = pq$. Given the pair (e, N) for $e < \phi(N)$ as a public key pair and (d,p,q) as a private key tuple, let $|b^2p - a^2q| < N^\gamma$. If $\frac{q}{p}$ is close to $\frac{b^2}{a^2}$ such that the relation $(a^2(b^4+1)p - b^2(a^4+1)q)(b^2p-a^2q) > 0$ holds and $d < \frac{\sqrt{3}}{\sqrt{2}}N^{\frac{3}{4}-\gamma}$, then $\frac{k}{d}$ can be calculated efficiently from the convergent of the continued fraction expansion of $\frac{e}{N-\lceil\frac{a^2+b^2}{ab}\sqrt{N}\rceil+1}$ for $k < d$ and (a, b) are positive integers less than* $\log N$.

Proof of Theorem 13. Since $(a^2(b^4+1)p - b^2(a^4+1)q)(b^2p-a^2q) > 0$ and $b^2p - a^2q < N^\gamma$, then from Lemma 2 we have,

$$
\begin{aligned}
\frac{a^2+b^2}{ab}\sqrt{N} - (p+q) &< \frac{(b^2p-a^2q)^2}{\frac{a^2+b^2}{ab}\sqrt{N} + 2\sqrt{N}} \\
\left(\frac{a^2+b^2}{ab}\sqrt{N} + \phi(N) - N - 1\right) &< \frac{N^{2\gamma}}{(\frac{a^2+b^2}{ab}+2)\sqrt{N}}.
\end{aligned}
$$

Using RSA key equation $ed - k\phi(N) = 1$, for some $k \in \mathbb{Z}$, this gives us,

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

Taking $N - \frac{a^2+b^2}{ab}\sqrt{N} + 1$ as approximation of $\phi(N)$, this becomes,

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

Finally,

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

Now, assuming that $N-\frac{a^2+b^2}{ab}\sqrt{N}+1>\frac{4ab}{(a+b)^2}N$, $\phi(N)>\frac{4}{5}N$ and $N>10d$, where a and b are small positive integers, plugging the conditions into above inequality (Equation (1)), we get,

$$\begin{aligned}\left|\frac{e}{\phi(N)}-\frac{k}{d}\right|&<\frac{N^{2\gamma}}{\frac{(4ab)}{(a+b)^2}N(\frac{a^2+b^2}{ab}\sqrt{N}+2\sqrt{N})}+\frac{1}{\frac{4}{5}(10d^2)}\\&<\frac{N^{2\gamma-\frac{3}{2}}}{4}+\frac{1}{8d^2}.\end{aligned}$$

Suppose that $d<\frac{\sqrt{3}}{\sqrt{2}}N^{\frac{3}{4}-\gamma}$, then,

$$\frac{N^{2\gamma-\frac{3}{2}}}{4}+\frac{1}{8d^2}<\frac{1}{2d^2}.$$

Hence, we have,

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

This shows that Theorem 13 produces $\frac{k}{d}$ as the convergent of the continued fraction expansion of $\frac{e}{N-\frac{a^2+b^2}{ab}\sqrt{N}+1}$. This terminates the proof. □

This is an improvement on the work of Reference [9], whose $d<N^{\frac{3}{4}-\gamma}$. Also taking the value of $\gamma=\frac{15}{32}$, we have our decryption exponent $d<\frac{\sqrt{3}}{\sqrt{2}}N^{0.28125}$, which is also an improvement on the results of References [5,11] whose decryption exponents were $d<\frac{1}{3}N^{\frac{1}{4}}$ and $d<\frac{1}{2}N^{\frac{1}{4}}$, respectively.

From Table 1 one can observe that our bound is an improvement of the abovementioned bounds.

Table 1. Comparison of the bounds on d for RSA modulus $N=pq$.

Authors	Bound for d	Assumed Interval for γ
[5]	$\frac{1}{3}N^{\frac{1}{4}}$	Not applicable
[7]	$d<\frac{1}{8}N^{\frac{3}{4}-\gamma}$	$0.25\leq\gamma<0.5$
[8]	$d<N^{\frac{1-\gamma}{2}}$	$0.25\leq\gamma<0.5$
[9]	$d<N^{\frac{3}{4}-\gamma}$	$0.25\leq\gamma<0.5$
[10]	$d<\frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$	Not applicable
[11]	$d<\frac{1}{2}N^{\frac{1}{4}}$	Not applicable
Our result	$d<\frac{\sqrt{3}}{\sqrt{2}}N^{\frac{3}{4}-\gamma}$	$0.25\leq\gamma<0.5$

Example 1. *In this example, we illustrate how to factor the RSA modulus $N=pq$ for the case $\gamma=\frac{15}{32}=0.46875$. Let,*

$$N=26165530044163,$$

$$e=20107848788311,$$

and $a=3$, $b=2$,$\gamma=\frac{15}{32}$. Taking the continued fraction expansion of $\frac{e}{N-\lceil\frac{13}{6}\sqrt{N}\rceil+1}$, we get,

$$[0,1,3,3,7,1,1,1,4,161,2,3,1,1,1,5,1,2,2,8,4,5,1,5,26,3]$$

and their corresponding convergents are as follows,

$$[0, 1, \frac{3}{4}, \frac{10}{13}, \frac{73}{95}, \frac{83}{108}, \frac{156}{203}, \frac{239}{311}, \frac{1112}{1447}, \frac{179{,}271}{233{,}278}, \frac{359{,}654}{468{,}003}, \frac{1{,}258{,}233}{1{,}637{,}287}, \frac{1{,}617{,}887}{2{,}105{,}290}, \frac{2{,}876{,}120}{3{,}742{,}577}, \cdots],$$

$\frac{k}{d} = \frac{1112}{1447}$ *and computing,*

$$\begin{aligned} \frac{1 + k\phi(N)}{d} &= 20107848788311 \\ \phi(N) &= 26165519061768 \\ N - \phi(N) + 1 &= 10982396. \end{aligned}$$

Finally, solving the quadratic equation $x^2 - (N - \phi(N) + 1)x + N = 0$ leads to the factorization of N. This reveals the factors of N as $p = 7488127$ and $q = 3494269$. Taking the value of $\gamma = 0.46875$, this shows that our bound increases to $d < \frac{\sqrt{3}}{\sqrt{2}} N^{0.28125}$, that is, $1447 < 7274.146806$. This shows that our private key is greater than the bounds of References [5,11], i.e., $753.8954627 < 1147 < 7274.146806$ (bound of Reference [5]) and $1130.843194 < 1147 < 7274.146806$ (bound of Reference [11]). This is an improvement on bounds stated in Table 1.

3.2. System of Equations Using $N - \frac{a^2+b^2}{ab}\sqrt{N} + 1$ as Approximation of $\phi(N)$

In this section, we present four cryptanalytic attacks on t RSA moduli $N_s = p_s q_s$ using a system of equations of the form $e_s d - k_s \phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s \phi(N_s) = z_s$, and $e_s d_s - k\phi(N_s) = z_s$ for $s = 1, \ldots, t$, in which we successfully factor t RSA moduli in polynomial time for unknown positive integers d, k_s, z_s, d_s, and k for $s = 1, \ldots, t$.

3.2.1. The Attack on t RSA Moduli $N_s = p_s q_s$ Satisfying $e_s d - k_s \phi(N_s) = 1$

Taking $t \geq 2$, let $N_s = p_s q_s$, $s = 1, \ldots, t$. The attack works for t instances (N_s, e_s) when there exist an integer d and t integers k_s satisfying equation $e_s d - k_s \phi(N_s) = 1$. We show that prime factors p_s and q_s of t RSA moduli N_s for $s = 1, \ldots, t$ can be found efficiently for $N = \max\{N_s\}$ and $d < N^\gamma$, $k_s < N^\gamma$, for all $\gamma = \frac{3t}{2(3t+1)}$. In this case, the RSA instances shared common decryption exponent d.

Theorem 14. *Let $N_s = p_s q_s$ be t RSA moduli for $s = 1 \ldots t$ and let (e_s, N_s) be a public key pair and (d, N_s) be a private key pair such that $e_s < \phi(N_s)$ and the relation $e_s d \equiv 1 \pmod{\phi(N)}$ is satisfied. Let also $N = \max\{N_s\}$; if there exist positive integers $d < N^\gamma$, $k_s < N^\gamma$, for all $\gamma = \frac{3t}{2(3t+1)}$ such that equation $e_s d - k_s \phi(N_s) = 1$ holds, then prime factors of t RSA moduli N_s can be successfully recovered in polynomial time.*

Proof of Theorem 14. For $t \geq 2$, and let $N_s = p_s q_s$, $1 \leq s \leq t$ be t moduli. Let $N = \max\{N_s\}$ and suppose that $k_s < N^\gamma$. Then equation $e_s d - k_s \phi(N_s) = 1$ can be rewritten as,

$$\begin{aligned} e_s d - k_s(N_s - (p_s + q_s) + 1) &= 1 \\ e_s d - k_s \left(N_s - \frac{a^2+b^2}{ab}\sqrt{N_s} + \frac{a^2+b^2}{ab}\sqrt{N_s} - (N_s - \phi(N_s) + 1) + 1 \right) &= 1 \\ \left| \frac{e_s}{N_s - \frac{a^2+b^2}{ab}\sqrt{N_s} + 1} d - k_s \right| &= \frac{\left| 1 - k_s \left(N_s - \phi(N_s) + 1 - \frac{a^2+b^2}{ab}\sqrt{N_s} \right) \right|}{N_s - \frac{a^2+b^2}{ab}\sqrt{N_s} + 1}. \end{aligned}$$

Let $N = \max\{N_s\}$ and suppose that $k_s < N^\gamma$ are positive integers and from Theorem 13, it was shown that,

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

$$N_s-\frac{a^2+b^2}{ab}\sqrt{N_s}+1 > \frac{4ab}{(a+b)^2}N$$

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

We therefore have,

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

Hence, to show the existence of integer d and t integers k_s we let $\varepsilon = bN^{3\gamma-\frac{3}{2}}$, with $\gamma = \frac{3t}{2(3t+1)}$. Then, we have,

$$N^{\gamma}\varepsilon^t = N^{\gamma}\left(bN^{3\gamma-\frac{3}{2}}\right)^t = b^tN^{\gamma+3\gamma t-\frac{3t}{2}} = b^t.$$

Following Theorem 9, we have $b^t < 2^{\frac{t(t-3)}{4}}\cdot 3^t$ for $t \geq 2$, then, we get $N^{\gamma}\varepsilon^t < 2^{\frac{t(t-3)}{4}} \times 3^t$. It follows that if $d < N^{\gamma}$, then $d < 2^{\frac{t(t-3)}{4}} \times 3^t \times \varepsilon^{-t}$ for $s = 1, \ldots, t$. Finally,

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

This clearly satisfies the conditions of Theorem 9, and we proceed to reveal the private key d and t integers k_s for $s = 1, \ldots, t$. Next, from equation $e_sd - k_s\phi(N_s) = 1$ we compute,

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

Finally, by finding the roots of the quadratic equation $x^2-(N_s-\phi(N_s)+1)x+N_s = 0$, 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,

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

Define,

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

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 we apply the LLL algorithm.

Example 2. *In what follows, we give an illustration of how Theorem 14 works on three RSA moduli and their corresponding public exponents,*

$$\begin{aligned} \text{Let } N_1 &= 359072092653124553811906103878007890140989 \\ N_2 &= 324883680116881280214836807152055627596063 \\ N_3 &= 382594344895631082046807051393818596023693 \\ e_1 &= 453754203447921688814555547793435800963 91 \\ e_2 &= 243789589028178310684702159604367474648551 \\ e_3 &= 310614049489189851372469759955479934011591. \end{aligned}$$

Observe that,

$$\begin{aligned} N &= \max\{N_1, N_2, N_3\} \\ &= 382594344895631082046807051393818596023693. \end{aligned}$$

By using $a = 3$, $b = 2$ and since $t = 3$, we will have from Algorithm 4 $\gamma = \frac{3t}{2(3t+1)} = 0.45$ and $\varepsilon = bN^{3\gamma-\frac{3}{2}} = 0.000001157761794$.

Algorithm 4 Theorem 14

1: Initialization: The public key tuple (N_s, e_s, γ) satisfying Theorem 14.
2: Choose a, b and t to be suitable small positive integers and $N = \max\{N_s\}$ for $s = 1, \ldots, t$.
3: **for any** (a, b, t, N, γ) **do**
4: $\quad \varepsilon := bN^{3\gamma-\frac{3}{2}}$
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 $\mathcal{L}$, we obtain 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).

Applying Theorem 9 and using Algorithm 4 for $n = t = 3$, we compute,

$$T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}] = 22541258940000000000000000. \quad (3)$$

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

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

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

$$K = \begin{pmatrix} 2578263109750711 & -2034699965866566690 & -2344404377412628796 & 2580976588820297660 \\ 2580976588820297660 & -7038163058258067570 & 1213053071081376612 & -4486161207788962020 \\ 4247153090969385088 & -4534704902749259520 & 12312546858704031232 & 7327527172122145280 \\ -8914983043342173506 & -11071823379597700260 & -645732543479046584 & -645732543479046584 \end{pmatrix}$$

Next, from Algorithm 4 we compute $Q = K \cdot J$,

$$Q = \begin{pmatrix} 2578263109750711 & 325811375370309 & 1934703841407202 & 2093195458460643 \\ 9287723537945650383 & 1173676173123327666 & 6969418419258590716 & 7540355619851993530 \\ 7540355619851993530 & 536706585430991758 & 3187022832955722161 & 3448104860897526334 \\ -8914983043342173506 & -1126573496618480874 & -6689717536897095223 & -7237741543135901521 \end{pmatrix}$$

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

$$d = 2578263109750711,\ k_1 = 325811375370309,\ k_2 = 1934703841407202,\ k_3 = 2093195458460643$$

Using Algorithm 4, we now compute $\phi(N_s) = \frac{e_s d - 1}{k_s}$ for $s = 1, 2, 3$.

$$\phi(N_1) = 359072092653124553810707267684522589776000$$

$$\phi(N_2) = 324883680116881280213619313059216656916880$$

$$\phi(N_3) = 382594344895631082045445951038518440638400.$$

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

$$W_1 = 1198836193485300364990$$

$$W_2 = 1217494092838970679184$$

$$W_3 = 1361100355300155385294.$$

Finally, solving the quadratic equation $x^2 - W_s x + N_s = 0$ 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,

$$p_1 = 614582596386772289501,\ q_1 = 584253597098528075489$$

$$p_2 = 822497570179231384793,\ q_2 = 394996522659739294391$$

$$p_3 = 964370894659814712593,\ q_3 = 396729460640340672701.$$

From our result, one can observe that we get $d \approx N^{0.3706}$, which is larger than Blömer–May's bound $x < \frac{1}{3}N^{0.25}$, as reported in Reference [12]. Our $d \approx N^{0.3706}$ is also larger than Nitaj et al.'s bound $d \approx N^{0.344}$, as reported in Reference [13] .

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

Theorem 15. *Let $N_s = p_s q_s$ be t RSA moduli for $s = 1, \ldots, t$ and let (e_s, N_s) be a public key pair and (d_s, N_s) be a private key pair with $e_s < \phi(N_s)$ and the given relation $e_s d_s \equiv 1 \pmod{\phi(N)}$ is satisfied. Let $e = \min\{e_s\} = N^\alpha$ be t public exponents; if there exist t integers $d_s < N^\gamma$, $k < N^\gamma$, for all $\gamma = \frac{(1+2\alpha)t}{2(3t+1)}$ such that equation $e_s d_s - k\phi(N_s) = 1$ holds, then t prime factors of RSA moduli N_s can be successfully recovered in polynomial time.*

Proof of Theorem 15. For $t \geq 3$ and $N_s = p_s q_s$, be t RSA moduli. Let $e = \min\{e_s\} = N^\alpha$ be t public exponents for $s = 1, \ldots, t$ and suppose that $d_s < N^\gamma$. Then, the equation $e_s d_s - k\phi(N_s) = 1$ can be rewritten as,

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

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

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

Let $N = \max\{N_s\}$ and $d_s < N^\gamma$, $k < N^\gamma$ be positive integers and from Theorem 13, it was shown that,

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

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

$$\begin{aligned}\frac{\left|1 - k\left(N_s - \phi(N_s) + 1 - \frac{a^2+b^2}{ab}\sqrt{N_s}\right)\right|}{e_s} &\leq \frac{\left|1 + k\left(\frac{a^2+b^2}{ab}\sqrt{N_s} - N_s + \phi(N_s) - 1\right)\right|}{e_s} \\ &< \frac{1 + N^\gamma\left(\frac{N^{2\gamma}}{(\frac{a^2+b^2}{ab}+2)\sqrt{N}}\right)}{N^\alpha} \\ &< \sqrt{8}N^{3\gamma - \frac{1}{2} - \alpha}.\end{aligned}$$

Hence, we get,

$$\left|k\frac{\left(N_s - \frac{a^2+b^2}{ab}\sqrt{N_s} + 1\right)}{e_s} - d_s\right| < \sqrt{8}N^{3\gamma - \frac{1}{2} - \alpha}.$$

We now proceed to show the existence of integer k and t integers d_s. Let $\varepsilon = \sqrt{8}N^{3\gamma - \frac{1}{2} - \alpha}$ and $\gamma = \frac{(1+2\alpha)t}{2(3t+1)}$. Then, we get,

$$N^\gamma \varepsilon^t = N^\gamma\left(\sqrt{8}N^{3\gamma - \frac{1}{2} - \alpha}\right)^t = 8^{\frac{t}{2}}N^{\gamma + 3\gamma t - \frac{t}{2} - \alpha t} = 8^{\frac{t}{2}}.$$

Following Theorem 9, we have $8^{\frac{t}{2}} < 2^{\frac{t(t-3)}{4}} \cdot 3^t$ for $t \geq 3$, then we get $N^{\gamma}\varepsilon^t < 2^{\frac{t(t-3)}{4}} \cdot 3^t$. It follows that if $k < N^{\gamma}$ and following Theorem 9, we have $k < 2^{\frac{t(t-3)}{4}} \times 3^t \times \varepsilon^{-t}$ for $s = 1, \ldots, t$. Finally,

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

This clearly satisfies the conditions of Theorem 9, and we proceed to reveal t integers of the private key d_s and integer k for $s = 1, \ldots, t$. Next, from equation $e_s d_s - k\phi(N_s) = 1$ we compute,

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

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

Let,

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

Define,

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

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 and b, the matrix M can be used in computing the reduced basis after we apply the LLL algorithm

Example 3. *In what follows, we give a numerical example to illustrate how our attack of Theorem 15 works on three RSA Moduli. We consider the following three RSA moduli and their corresponding public exponents,*

$$N_1 = 163889671902988443382883271210955564227203$$

$$N_2 = 114862300622228592060226444669830911962551 7$$

$$N_3 = 958230896880440803103514702761136188985911$$

$$e_1 = 102148699518319970718711207616780801429013$$

$$e_2 = 555369481273226483312414829199486063579195$$

$$e_3 = 294723806871316670179807860936827357565316 1.$$

Observe that ,

$$\begin{aligned} N &= \max\{N_1, N_2, N_3\} \\ &= 114862300622228592060226444669830911962551 7 \\ e_s &= \min\{e_1, e_2, e_3\} \\ &= 102148699518319970718711207616780801429013, \end{aligned}$$

with $e_s = \min\{e_1, e_2, e_3\} = N^{\alpha}$ with $\alpha = 0.9750133088$. By using $a = 3$, $b = 2$ and since $t = 3$, we will have from Algorithm 5 $\gamma = \frac{(1+2\alpha)t}{2(3t+1)} = 0.44250$ and $\varepsilon = \sqrt{8}N^{3\gamma-\frac{1}{2}-\alpha} = 0.000001768531652$.
Applying Theorem 9 and using Algorithm 5, we compute,

$$T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}] = 41400317860000000000000000.$$

Algorithm 5 Theorem 15

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

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

$$K = \begin{pmatrix} 1944662874609887749 & 739703099714239590 & 345516048415097753 & 75220223065832636 \\ -312939819716059 & 3078110579756278310 & -414033376574202823 & -67328478162817476 \\ 641396426019740525 & -1430247980684822250 & -660964237954996575 & -2681843509732748900 \\ -893602997419446810 & 1688910391195682900 & 3790386709273250430 & -350853801896118840 \end{pmatrix}$$

Next, from Algorithm 5, we compute $Q = K \cdot J$,

$$Q = \begin{pmatrix} 1944662874609887749 & 3120060871891740871 & 4021979227238758337 & 632265194403229474 \\ -312939819716059 & -502087688051741 & -647226555670387 & -101745633411641 \\ 641396426019740525 & 1029070857639965612 & 1326545148548731842 & 208536215341829039 \\ -893602997419446810 & -1433716755565101613 & -1848162342143902764 & -290535742857772536 \end{pmatrix}$$

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

$$k = 312939819716059,\ d_1 = 502087688051741,\ d_2 = 647226555670387,\ d_3 = 101745633411641.$$

Using Algorithm 5, we compute $\phi(N_s) = \frac{e_s d_s - 1}{k}$ for $s = 1, 2, 3$. That is,

$$\phi(N_1) = 16388967190298844338176344505858591755881248$$

$$\phi(N_2) = 11486230062222859206001198814621138724552 96$$

$$\phi(N_3) = 95823089688044080310154726446207463700 0800.$$

Next, from Algorithm 5 we proceed to compute W_s for $s = 1, 2, 3$.

$$W_1 = 1119826152363808345956$$

$$W_2 = 2144565236195247170222$$

$$W_3 = 1967438299061551985112.$$

Finally, solving the quadratic equation $x^2 - W_s x + N_s = 0$ 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,

$$p_1 = 946711448692045925137,\ q_1 = 173114703671762420819$$

$$p_2 = 1106444100091356676813,\ q_2 = 1038121136103890493409$$

$$p_3 = 1081045755724110472721,\ q_3 = 886392543337441512391.$$

From our result, one can observe that we get $\min\{d_1, d_2, d_3\} \approx N^{0.333}$, which is larger than Blömer–May's bound $x < \frac{1}{3} N^{0.25}$, as reported in Reference [12].

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

In this section, we consider 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 $s = 1, \ldots, t$.

For $t \geq 2$, let $N_s = p_s q_s$, for $= 1, \ldots, t$. The attack works for t instances (N_s, e_s) if there exist an integer d and t integers k_s such that $e_s d - k_s \phi(N_s) = z_s$ holds. We show that prime factors p_s and q_s of t RSA moduli N_s for $s = 1, \ldots, t$ can be found efficiently for $N = \max\{N_s\}$ and d, k_s, and $z_s < N^{\gamma}$ for all $\gamma = \frac{3t}{2(4t+1)}$ for unknown positive integers d, k_s, and z_s. In this case, the RSA instances shared a common decryption exponent d.

Theorem 16. *Let $N_s = p_s q_s$ be RSA moduli for $s = 1, \cdots, t$ and let the pair (e_s, N_s) be public keys and (d, N_s) bea private key with $e_s < \phi(N_s)$ and the given relation $e_s d \equiv z_s \pmod{\phi(N_s)}$ is satisfied. Let $N = \max\{N_s\}$ for $s = 1, \ldots, t$. If there exist integers $d < N^{\gamma}$, $k_s < N^{\gamma}$, for all $\gamma = \frac{3t}{2(4t+1)}$ such that equation $e_s d - k_s \phi(N_s) = z_s$ holds, then the prime factors of t RSA moduli N_s can be successfully recovered in polynomial time.*

Proof of Theorem 16. For $t \geq 2$, and let $N_s = p_s q_s, 1 \leq s \leq t$ be t RSA moduli. Let $N = \max\{N_s\}$ and suppose that $k_s < N^{\gamma}$. Then equation $e_s d - k_s \phi(N_s) = z_s$ can be rewritten as,

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

$$\left|\frac{e_s}{N_s - \frac{a^2+b^2}{ab}\sqrt{N_s} + 1}d - k_s\right| = \frac{\left|z_s - k_s\left(N_s - \phi(N_s) + 1 - \frac{a^2+b^2}{ab}\sqrt{N_s}\right)\right|}{N_s - \frac{a^2+b^2}{ab}\sqrt{N_s} + 1}. \tag{5}$$

Taking $N = \max\{N_s\}$ and suppose that $k_s < N^{\gamma}$, $z_s < N^{\gamma}$ are positive integers and from Theorem 13, it was shown that,

$$\left|\frac{a^2+b^2}{ab}\sqrt{N_s} + \phi(N_s) - N_s - 1\right| < \frac{N^{2\gamma}}{(\frac{a^2+b^2}{ab} + 2)\sqrt{N}}$$
$$N_s - \frac{a^2+b^2}{ab}\sqrt{N_s} + 1 > \frac{4ab}{(a+b)^2}N.$$

Plugging into Equation (5) yields,

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

Hence, we have,

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

Hence, to show the existence of integer d and t integers k_s, we let $\varepsilon = bN^{4\gamma-\frac{3}{2}}$, with $\gamma = \frac{3t}{2(4t+1)}$. Then,we have:

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

Following Theorem 9, we have $b^t < 2^{\frac{t(t-3)}{4}} \times 3^t$ for $t \geq 2$, then we get $N^{\gamma}\varepsilon^t < 2^{\frac{t(t-3)}{4}} \times 3^t$. It follows that if $d < N^{\gamma}$, then $d < 2^{\frac{t(t-3)}{4}} \times 3^t \times \varepsilon^{-t}$ for $s = 1, \ldots, t$. Finally,

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

This also satisfies the conditions of Theorem 9, and we next proceed to reveal the private key d and t integers k_s for $s = 1, \ldots, t$. Next, from equation $e_s d - k_s \phi(N_s) = z_s$ we compute,

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

Finally, by finding the roots of the quadratic equation $x^2 - (N_s - \phi(N_s) + 1)x + N_s = 0$, 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,

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

Define,

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

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 and b, the matrix M can be used in computing the reduced basis after we apply the LLL algorithm.

Example 4. *In what follows, we give a numerical example to illustrate how our attack of Theorem 16 works on t RSA Moduli. We consider the following three RSA moduli and their corresponding public exponents,*

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

Observe that,

$$\begin{aligned} N &= \max\{N_1, N_2, N_3\} \\ &= 330296126221226061978488805127502203372577. \end{aligned}$$

By using $a = 3$, $b = 2$ and since $t = 3$, we will have from Algorithm 6 $\gamma = \frac{3t}{2(4t+1)} = 0.346$ and $\varepsilon = bN^{3\gamma - \frac{3}{2}} = 0.00003240252930$. Applying Theorem 9 and Algorithm 6 for $n = t = 3$ we compute,

$$T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}] = 36740018900000000000.$$

Algorithm 6 Theorem 16

Initialization: The public key tuple (N_s, e_s, z_s, γ) satisfying Theorem 16.
Choose a, b and t to be suitable small positive integers and $N = \max\{N_s\}$ for $s = 1, \ldots, t$.
for any (a, b, t, N, γ) **do**
    $\varepsilon = bN^{3\gamma - \frac{3}{2}}$
    $T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}]$ for $t \geq 2$.
end for
Consider the lattice $\mathcal{L}$ spanned by the matrix M as stated above.
Applying the LLL algorithm to $\mathcal{L}$, we obtain 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).

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

$$K = \begin{pmatrix} 221202829045687 & 93563315351041 & 100537693381434 & 43249006678519 \\ 219137979005996 & 215228853099828 & -366048772777528 & 36384754276652 \\ -15192444691558 & -450517287777994 & 9761598838844 & 503486112156954 \\ 337933481607001 & -490633444109457 & -161755868358618 & -208327724754663 \end{pmatrix}$$

Next, from Algorithm 6, we compute $Q = K \cdot J$,

$$Q = \begin{pmatrix} 221202829045687 & 202366218737588 & 107651873220345 & 165704724042021 \\ 219137979005996 & 200477201781543 & 106646981123572 & 164157929150241 \\ -15192444691558 & -13898726335799 & -7393644723707 & -11380776032563 \\ 337933481607001 & 309156628568763 & 164460700958544 & 253148544961339 \end{pmatrix}$$

From the first row of matrix Q, one can observe that 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 6, we compute $\phi(N_s) = \frac{e_s d - z_s}{k_s}$ for $s = 1, 2, 3$ where z_1, z_2, 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 6, we compute W_s for $s = 1, 2, 3$.

$$W_1 = 1201930848666443078622$$

$$W_2 = 998486676567755264568$$

$$W_3 = 1211972451664108229712.$$

Finally, solving the quadratic equation $x^2 - W_s x + N_s = 0$ 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–May's bound $x < \frac{1}{3}N^{0.25}$, as reported in Reference [12]. Our $d \approx N^{0.3455}$ is also larger than Nitaj et al.'s bound $x \approx N^{0.344}$, as reported in Reference [13].

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

In this section, we present 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 17. *Let $N_s = p_s q_s$ be t RSA moduli for $s = 1, \cdots, t$ and let (e_s, N_s) be a public key pair and (d_s, N_s) be a private key pair with condition $e_s < \phi(N_s)$ and the given relation $e_s d_s \equiv z_s \pmod{\phi(N_s)}$ is satisfied. Let $e = \min\{e_s\} = N^{\alpha}$ be t public exponents. If there exist positive integers $d_s < N^{\gamma}$, $k < N^{\gamma}$, for all $\gamma = \frac{(1+2\alpha)t}{2(4t+1)}$ such that the equation $e_s d_s - k\phi(N_s) = z_s$ holds, then t prime factors of RSA moduli N_s can be found successfully in polynomial time.*

Proof of Theorem 17. For $t \geq 3$ and suppose $N_s = p_s q_s$ to be t RSA moduli for $s = 1, \ldots, t$. Suppose that $e = \min\{e_s\} = N^{\alpha}$ are t public exponents and suppose that $d_s < N^{\gamma}$. Then, equation $e_s d_s - k\phi(N_s) = z_s$ can be rewritten as,

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

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

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

Let $N = \max\{N_s\}$ for $s = 1, \cdots, t$, and $d_s < N^\gamma$, $k < N^\gamma$, $z_s < N^\gamma$ be positive integers and $\left|\frac{a^2+b^2}{ab}\sqrt{N_s} + \phi(N_s) - N_s - 1\right| < \frac{N^{2\gamma}}{(\frac{a^2+b^2}{ab}+2)\sqrt{N}}$, $e = \min\{e_s\} = N^\alpha$, then we have,

$$\begin{aligned}\frac{\left|z_s - k\left(N_s - \phi(N_s) + 1 - \frac{a^2+b^2}{ab}\sqrt{N_s}\right)\right|}{e_s} &\leq \frac{\left|z_s + k\left(\frac{a^2+b^2}{ab}\sqrt{N_s} - N_s + \phi(N_s) - 1\right)\right|}{e_s} \\ &< \frac{N^\gamma + N^\gamma\left(\frac{N^{2\gamma}}{(\frac{a^2+b^2}{ab}+2)\sqrt{N}}\right)}{N^\alpha} \\ &< \sqrt{\frac{a}{b}}N^{3\gamma-\frac{1}{2}-\alpha}.\end{aligned}$$

Hence, we get,

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

We now proceed to show the existence of integer k and t integers d_s. Let $\varepsilon = \sqrt{\frac{a}{b}}N^{3\gamma-\frac{1}{2}-\alpha}$ and $\gamma = \frac{(1+2\alpha)t}{2(4t+1)}$. Then, we get,

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

Following Theorem 9, we have $\left(\frac{a}{b}\right)^{\frac{t}{2}} < 2^{\frac{t(t-3)}{4}} \times 3^t$ for $t \geq 2$, then we get $N^\gamma\varepsilon^t < 2^{\frac{t(t-3)}{4}} \times 3^t$. It follows that if $k < N^\gamma$, then $k < 2^{\frac{t(t-3)}{4}} \times 3^t \times \varepsilon^{-t}$ for $s = 1, \ldots, t$. Finally,

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

This satisfies the conditions of Theorem 9 and we proceed to find the values of d_s and k for $s = 1, \ldots, t$. Next, from the equation $e_s d_s - k\phi(N_s) = z_s$ we compute,

$$\begin{aligned}\phi(N_s) &= \frac{e_s d_s - z_s}{k} \\ p_s + q_s &= N_s - \phi(N_s) + 1\end{aligned}$$

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

Let,

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

Define,

$$T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}]. \tag{7}$$

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 and b, the matrix M can be used in computing the reduced basis after we apply the LLL algorithm.

Algorithm 7 Theorem 17

Initialization: The public key tuple $(N_s, e_s, z_s, \alpha, \gamma)$ satisfying Theorem 17.
Choose a, b and t to be suitable small positive integers and $N = \max\{N_s\}$ for $s = 1, \ldots, t$.
for any (a, b, t, N, γ) **do**
    $\varepsilon = \sqrt{\frac{a}{b}} N^{3\gamma - \frac{1}{2} - \alpha}$
    $e =: \min\{e_s\} := N^{\alpha}$
    $T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}]$ for $t \geq 2$.
end for
Consider the lattice $\mathcal{L}$ spanned by the matrix M as stated above.
Applying the LLL algorithm to $\mathcal{L}$, we obtain 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 5. *In what follows, we give a numerical example to illustrate how our attack of Theorem 17 works on t RSA Moduli. We consider the following three RSA moduli and their corresponding public exponents,*

$$N_1 = 336942490676287248746778854034851937369893$$

$$N_2 = 668105444816109132056919917066428038906749$$

$$N_3 = 639755280744251044114047220423078131849607$$

$$e_1 = 216385769902449684764280685469492987883161$$

$$e_2 = 277165607451140973127254619964081652815328 7$$

$$e_3 = 198763531608436442410709911720743893687588 5.$$

Observe that,

$$\begin{aligned} N &= \max\{N_1, N_2, N_3\} \\ &= 668105444816109132056919917066428038906749 \\ e_s &= \min\{e_1, e_2 e_3\} \\ &= 216385769902449684764280685469492987883161, \end{aligned}$$

with $e_s = \min\{e_1, e_2, e_3\} = N^{\alpha}$ for $\alpha = 0.9882936490$. By using $a = 3$, $b = 2$ and since $t = 3$, we will have from Algorithm 7 $\gamma = \frac{(1+2\alpha)j}{2(4t+1)} = 0.3434523805$ and $\varepsilon = \sqrt{\frac{a}{b}} N^{3\gamma - \frac{1}{2} - \alpha} = 0.00001994181860$.

Applying Theorem 9 and using Algorithm 7, we compute,

$$T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}] = 256091979900000000000.$$

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

$$K = \begin{pmatrix} 475374059459089 & -261893631007311 & -36395361888534 & -199732740251281 \\ -1289880599128957 & -2285004592985757 & -1543204053684258 & 795956829369853 \\ -1037212131324544 & 196749388649856 & -1127770407188736 & -2527706537969024 \\ 1215125997180921 & 973858878471321 & -2293826172011526 & 1849797988697991 \end{pmatrix}$$

Next, from Algorithm 7 we compute $Q = K \cdot J$,

$$Q = \begin{pmatrix} 475374059459089 & 740222980786823 & 114588530795597 & 153007476978677 \\ -1289880599128957 & -2008522011135318 & -310924670404006 & -415170689585032 \\ -1037212131324544 & -1615082355210807 & -250019141530540 & -333844912543661 \\ 1215125997180921 & 1892118784706700 & 292905134341853 & 391109610085597 \end{pmatrix}$$

From the first row of matrix J, one can observe that we obtain k, d_1, d_2, and d_3 as follows,

$$k = 475374059459089,\ d_1 = 740222980786823,\ d_2 = 114588530795597,\ d_3 = 153007476978677.$$

Using Algorithm 7, 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,

$$z_1 = 254677352608291,\ z_2 = 170274159918143,\ z_3 = 138475454795345$$

$$\phi(N_1) = 336942490676287248745614825672641206658508$$

$$\phi(N_2) = 668105444816109132055284112629804447897564$$

$$\phi(N_3) = 639755280744251044112444603349851200819200.$$

Next, from Algorithm 7 we compute W_s for $s = 1, 2, 3$.

$$W_1 = 1164028362210730711386$$

$$W_2 = 1635804436623591009186$$

$$W_3 = 1602617073226931030408.$$

Finally, solving the quadratic equation $x^2 - (N_s - W_s x + N_s = 0$ 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,

$$p_1 = 624417203774295157627,\ q_1 = 539611158436435553759$$

$$p_2 = 847203991351099142923,\ q_2 = 788600445272491866263$$

$$p_3 = 849683014443852067207,\ q_3 = 752934058783078963201.$$

From our result, one can observe that we get $\min\{d_1, d_2, d_3\} \approx N^{0.336}$, which is larger than Blömer–May's bound $x < \frac{1}{3}N^{0.25}$, as reported in Reference [12].

4. Conclusions

In this paper, it has been shown that our proposed cryptanalytic attacks on RSA modulus $N = pq$ using the prime difference method can be used efficiently. The use of $N - \frac{a^2+b^2}{ab}\sqrt{N} + 1$ as a good approximation of $\phi(N)$ is necessary as we have discovered a short decryption exponent bound $d < \frac{\sqrt{3}}{\sqrt{2}}N^{\frac{3}{4}-\gamma}$ as a right candidate from the convergents of the continued fraction expansion of $\frac{e}{N-\frac{a^2+b^2}{ab}\sqrt{N}+1}$ that led to the successful factorization of the RSA modulus in polynomial time. This paper also reported instances of factoring t RSA moduli by transforming generalized key equations $e_s d - k_s\phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s\phi(N_s) = z_s$, and $e_s d_s - k\phi(N_s) = z_s$, where $s = 1, \ldots, t$ into a simultaneous Diophantine approximations problem and later applied the LLL and lattice basis reduction methods, which produced a reduced basis that yielded the values of d, k_s, d_s k, and z_s. Finally, we computed $\phi(N_s)$ and solved a system of quadratic equation $x^2 - (N_s - \phi(N_s) + 1)x + N_s = 0$ for $s = 1, 2, 3$, which produce the roots (p_1, q_1), (p_2, q_2), and (p_3, q_3) as prime factors of t RSA moduli N_1, N_2, N_3. In all the four attacks presented on t instances of RSA moduli $N_s = p_s q_s$, we have improved the short secret exponent bound.

Author Contributions: All the authors made substantial contributions in the development of this paper. M.R.K.A. and S.I.A. oversaw the paper from its introduction to its conclusion. M.A.A. provided insight into the conceptualization of the paper and also into running the Maple for numerical examples, as contained in the paper. F.Y. provided thorough revision, including punctuations of the paper and made useful suggestions in improving the quality of the paper.

Funding: This research work is funded by the Fundamental Research Grant Scheme [02-01-15-1745FR] provided by the Ministry of Higher Education, Malaysia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
2. Dubey, M.K.; Ratan, R.; Verma, N.; Saxena, P.K. Cryptanalytic Attacks and Countermeasures on RSA. In *Proceedings of the Third International Conference on Soft Computing for Problem Solving*; Springer: New Delhi, India, 2014; pp. 805–819.
3. Bach, E.; Miller, G.; Shallit, J. Sums of divisors, perfect numbers and factoring. *SIAM J. Comput.* **1986**, *15*, 1143–1154. [CrossRef]
4. Hinek, M.J. *Cryptanalysis of RSA and Its Variants*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2009.
5. Wiener, M. Cryptanalysis of Short RSA Secret Exponents. *IEEE Trans. Inform. Theory* **1990**, *36*, 553–558. [CrossRef]
6. Boneh, D.; Glenn, D. Cryptanalysis of RSA with private key d less than $N^{0.292}$. *IEEE Trans. Inf. Theory* **2000**, *46*, 1339–1349. [CrossRef]
7. De Weger, B. Cryptanalysis of RSA with small prime difference. *Appl. Algebra Eng. Commun. Comput.* **2002**, *13*, 17–28. [CrossRef]

8. Maitra, S.; Sarkar, S. Revisiting Wiener's attack–new weak keys in RSA. In *International Conference on Information Security*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 228–243.
9. Chen, C.Y.; Hsueh, C.C.; Lin, Y.F. A Generalization of de Weger's Method. In Proceedings of the 2009 Fifth International Conference on Information Assurance and Security, Xi'an, China, 18–20 August 2009; Volume 1, pp. 344–347.
10. Nitaj, A. Diophantine and lattice cryptanalysis of the RSA cryptosystem. In *Artificial Intelligence, Evolutionary Computing and Metaheuristics*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 139–168.
11. Asbullah, M.A. Cryptanalysis on the Modulus $N = p^2q$ and the Design of Rabin Cryptosystem without Decryption Failure. Ph.D. Thesis, Universiti Putra Malaysia, Selangor, Malaysia, 2015.
12. Blömer, J.; May, A. A generalized Wiener attack on RSA. In *International Workshop on Public Key Cryptography*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 1–13.
13. Nitaj, A.; Ariffin, M.R.; Nassr, D.I.; Bahig, H.M. New attacks on the RSA cryptosystem. In *International Conference on Cryptology in Africa*; Springer, Cham, Switzerland, 2014; pp. 178–198.
14. Wang, X.; Xu, G.; Wang, M.; Meng, X. *Mathematical Foundations of Public Key Cryptography*; CRC Press: Boca Raton, FL, USA, 2016.
15. Lenstra, A.K.; Lenstra, H.W.; Lovász, L. Factoring polynomials with rational coefficients. *Mathematische Annalen* **1982**, *261*, 515–534. [CrossRef]