AIMS Mathematics

https://www.aimspress.com/journal/Math

AIMS Mathematics, 10(7): 15512–15538.
DOI:10.3934/math.2025696
Received: 31 December 2024
Revised: 23 April 2025
Accepted: 29 April 2025
Published: 08 July 2025

Research article

New approach of factoring the RSA cryptosystem

Nurul Nur Hanisah Adenan[1], **Muhammad Rezal Kamel Ariffin**[1,2,4,*], **Wan Nur Aqlili Ruzai**[3,4], **Muhammad Asyraf Asbullah**[1,4,5], **Sook-Chin Yip**[6,7,*] **and Terry Shue Chien Lau**[6]

[1] Institute for Mathematical Research, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia

[2] Department of Mathematics and Statistics, Universiti Putra Malaysia, 43400, Serdang, Selangor, Malaysia

[3] School of Distance Education, Universiti Sains Malaysia, 11800 Penang, Malaysia

[4] Malaysia Cryptology Technology and Management Center, c/o Universiti Putra Malaysia, 43400 UPM, Serdang, Selangor, Malaysia

[5] Centre for Foundation Studies in Science of Universiti Putra Malaysia, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia

[6] Centre for Cybersecurity and Quantum Computing, COE for Advanced Cloud, Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Selangor, Malaysia

[7] Faculty of Artificial Intelligence & Engineering, Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Selangor, Malaysia

* **Correspondence:** Email: rezal@upm.edu.my, scyip@mmu.edu.my.

Abstract: The invention of the Rivest–Shamir–Adleman (RSA) cryptosystem was a groundbreaking advancement in cryptography. While the RSA remains relevant in securing global communications and digital transactions, with widespread use in public parameter infrastructure (PKI) and secure online exchanges, its vulnerability to algebraic attacks must be addressed. In this paper, we propose an equation, thereby revealing its potential application in the factorization of the modulus N. By introducing this equation, we demonstrate a method in the first attack named the continued fraction for recovering the primes p and q without necessitating the original $\phi(N)$ used in the RSA encryption. The results were extended to the case where a condition exists such that multiple sets of public parameters were used against a constant private parameter. We retrieved the primes $p_i's$ and $q_i's$ of the moduli N_i via the lattice reduction technique. This breakthrough could potentially expose the prime factors while circumventing standard cryptographic barriers. Our findings open new possibilities for cryptographic analysis and challenge the presumed security of widely used RSA systems.

Keywords: RSA; Euler's totient function; integer factorization problem; continued fraction, Coppersmith's technique and lattice reduction
Mathematics Subject Classification: 11T71, 68P25, 94A60

1. Introduction

The genesis of the Rivest-Shamir-Adleman (RSA) [1] cryptosystem, which was named after its inventors Rivest, Shamir, and Adleman, solved the main problem that arose in the early 1970s, where symmetric keys used for decrypting data could not be effectively distributed due to the increasing number of users. The original RSA key generation process involves computing both public and private parameters. The public key consists of (N, e), while the private key includes $(p, q, \phi(N), d, k)$. To begin, two large, distinct prime numbers p and q are generated. These are used to compute the RSA modulus $N = pq$, which becomes part of the public key, and the Euler's totient function $\phi(N) = (p-1)(q-1)$, which is used in the private key. Next, an integer e, known as the encryption exponent, is chosen such that $\gcd(\phi(N), e) = 1$. This ensures the existence of the decryption exponent d, which satisfies $ed \equiv 1 \pmod{\phi(N)}$. Encryption is performed by computing the ciphertext $C \equiv M^e \pmod{N}$, where M is the plaintext message. Decryption then recovers the original message using $M \equiv C^d \pmod{N}$.

The elegance of this cryptosystem lies in its utilization of two distinct keys for encryption and decryption, thus enabling secure communication by ensuring that the decryption key remains confidential to the intended recipient. Meanwhile, the encryption key is deliberately made public to facilitate the seamless transmission of messages. However, the increment of the computational cost and efficiency are parallel to the increment of the key's size, thus leading to the usage of smaller keys. Wiener [2] identified the drawback of using a smaller decryption key, as it can be retrieved via the continued fraction expansion method. Through his work, he showed that the safe bound for d is $d < \frac{1}{3}N^{1/4}$. Since then, more research has been done to increase the safe bound of d, such as in [3]. Interestingly, the authors in [4] proposed a new technique which focused on finding a good approximation of $\phi(N)$. They generated several points within the interval of the upper bound and the lower bound of $\phi(N)$. They applied the continued fractions and multicore systems upon these values to obtain the actual $\phi(N)$. They showed that this approach works by presenting three different attacks on this case.

The exploration of secure bounds for d has inevitably led to increased computational costs, as larger values must be employed to ensure resilience against existing attacks. Consequently, researchers have shifted their focus toward developing RSA variants. For example, some studies have explored modifying the RSA modulus by employing multi-prime or multi-power moduli. The work from Takagi [5] demonstrated that adopting these moduli can enhance the efficiency of the RSA algorithm. However, subsequent research by [6] revealed that this RSA variant remains vulnerable to certain attacks under specific conditions.

An alternative approach in the RSA variant involves altering the Euler's Totient equation. Parallel with their goal of enhancing the RSA's security and improving the computational efficiency, the designers adopted modified forms of the Euler Totient function, such as $\phi_1(N) = (p^2-1)(q^2-1)$ proposed by [7], and $\phi_2(N) = (p^2+p+1)(q^2+q+1)$ proposed by [8] in their reengineered version of the RSA key generation. Their research demonstrated that this modification may improve the implementation of RSA. Notably, these RSA variant also exhibit a significant weakness in their susceptibility to the factorization of the modulus N. For the case of equation $\phi_1(N)$, Bunder et al. [9] illustrated that an attack on this RSA variant could be executed using the continued fraction expansion upon $\frac{e}{N^2-\frac{9}{4}N+1}$ provided $d < \sqrt{\frac{2N^3-18N^2}{e}}$. A year later, [10] worked on the generalized equation $ex - \phi_1(N)y = z$ and showed that if the parameters x, y, z satisfy the conditions such that $xy < 2N - 4\sqrt{2}N^{3/4}$ and $|z| < (p-q)N^{1/4}y$, then the modulus N can be factored in polynomial time.

Meanwhile, for the case $\phi_2(N)$, [11] proved that the RSA that employed this equation in their key generation was vulnerable against a continued fraction attack. They showed that one may factor the modulus N if $d < N^\delta$ for $\delta < \frac{5}{4} - \frac{1}{2}\alpha$. The vulnerability of this type of cryptosystem was further studied by [12]. They applied continued fractions in three distinct attacks, each focusing on different cases, mainly to find a good approximation of $\phi_2(N)$. The attack on the first case works when $d < \frac{N^{.75}}{p-q}$ while the other two attacks work when $d < \frac{N^{0.75}}{2q-p}$ and $d < \frac{N^{1-\alpha}}{2}$ respectively. However, the third attack requires an additional condition, which they assumed is that the approximation of p is known. Recently, [13] conducted another attack on this variant $\phi_2(N)$, thereby considering the case when a certain amount of the most significant bits of the prime p is known, such that $|p - p_0| = N^\beta$. They proved that this situation may lead to the factorization of the modulus N when $d < N^\delta$, where $\delta < 2 - \sqrt{2\alpha\beta}$.

To date, most cryptanalytic studies on the RSA cryptosystem have focused on exploiting the size of the decryption exponent, thus suggesting that the system remains highly secure as long as d is sufficiently large. Additionally, these attacks often utilize specific components from the key generation process to achieve their goals. For example, the continued fraction expansion is expected to yield a sequence of convergents. According to the conditions outlined by [14], there is a significant probability that $\frac{x}{y}$ could be one of the convergents of $\frac{e}{N}$ when d is small. This method takes advantage of the information in the public parameter (e, N) to deduce k and d, ultimately revealing $\phi(N)$, and allows for the factorization of N. As a defense, increasing the size of d is recommended. However, this raises the question: Is simply enlarging d sufficient to secure the cryptosystem, or could other convergents still be exploited to derive new equations leading to the factorization of the modulus N?

Using multiple sets of public parameters while keeping the private parameter fixed can pose a serious threat to the security of the RSA cryptosystem. In particular, scenarios where a single private exponent remains fixed, such that $e_i x - \phi(N_i)y_i = 1$ or $e_i x_i - \phi(N_i)y = 1$ are particularly risky, as adversaries could exploit these parameters to their advantage. The study by [15] showed that the RSA is vulnerable when the public parameters (e_i, N_i) are used in equations of the form $e_i x - \phi(N_i)y_i = z_i$ or $e_i x_i - \phi(N_i)y = z_i$. A more recent attack in 2022 by [16] expanded upon this by analyzing equations of the form $e_i x^2 - \phi(N_i)y_i^2 = z_i$. Their findings revealed that while x and y do not necessarily need to be integers, their squares x^2 and y^2 must be. As a result, they were able to improve the known insecure bounds on the private exponent d. Their research proved that the RSA cryptosystem becomes vulnerable whenever a collection of public parameters is associated with a shared private component.

Our contribution: In this study, we propose an alternative equation, $\psi(N) = (p + 1)(q + 1)$, and demonstrate how this formulation facilitates the factorization of the RSA modulus N, regardless of the original parameters used to generate it. Specifically, we show that the RSA can be broken without access to the original private parameters. In the first attack, we examine the continued fraction expansion of $\frac{e}{N}$. Although this expansion does not yield the true value of $\frac{k}{d}$ associated with Euler's totient function $\phi(N) = (p - 1)(q - 1)$—since d is typically large enough to resist such attacks—we show that a fraction $\frac{x}{y}$, which corresponds to the equation $\psi(N) = (p+1)(q+1)$ may still appear among the convergents of the same continued fraction. If such a convergent exists, then it enables recovery of the prime factors p and q without requiring knowledge of the private parameters k, d, or $\phi(N)$. The second and third attacks consider scenarios in which multiple public key sets share a common private parameter. In these cases, we construct a system of equations based on the available public data. By applying lattice reduction techniques to this system, the private components x and y can be recovered, thus ultimately leading to the factorization of each corresponding modulus N_i.

This article is structured into four sections. Section 2 introduces the key tools and techniques used to achieve our objectives; Section 3 presents the main results along with a detailed discussion; And finally, Section 4 concludes the study and summarizes the key findings.

2. Preliminaries

This section introduces several mathematical tools that will be employed throughout this work. We begin with the continued fraction expansion method, which plays a key role in the first attack. This technique is particularly important because it enables the recovery of private parameters solely using the public values (e, N), under specific conditions. In such cases, certain instances of the so-called RSA hard problems become solvable.

2.1. Continued fraction expansion

Consider the following rational number:

$$\xi = \frac{u}{v}.$$

The continued fraction of $\frac{u}{v}$ can be expressed in the form

$$\frac{u}{v} = \mu_0 + \cfrac{1}{\mu_1 + \cfrac{1}{\mu_2 + \cfrac{1}{\mu_3 + \cfrac{1}{\mu_4 + \cfrac{1}{\mu_5 + \dots}}}}},$$

where μ_0 and other μ_i are the respective integer and positive integers, respectively. They are called the partial quotient of the continued fraction. The continued fractions are finite for a rational number of ξ. In our attack, we apply this method to the public parameter (e, N) to find the candidate of $\frac{x}{y}$, which could lead to the factorization of N. The following theorem is essential to test whether the rational number (e, N) would yield the candidate $\frac{y}{x}$ as one of its convergents.

Theorem 2.1. *[14, Theorem 184] Let $\frac{e}{N} \in \mathbb{R}$ and x and y are coprime. If*

$$\left| \frac{e}{N} - \frac{y}{x} \right| < \frac{1}{2x^2},$$

then, $\frac{x}{y}$ is a convergent of the continued fraction of $\frac{e}{N}$.

2.2. Lattices

We begin this section by introducing the concepts of lattices and lattice reduction, which form the foundation for our second mathematical tool: simultaneous Diophantine approximation. This technique will be employed in both the second and third attacks.

Let $\{b_1, \dots, b_n\} \in \mathbb{R}^m$ denotes n linearly independent vectors where

$$n \leq m \in \mathbb{Z}^+.$$

A lattice $\mathcal{L}$ is constructed such that

$$\mathcal{L} = x_1 b_1 + \cdots + x_n b_n,$$

where $x_i \in \mathbb{Z}$.

The set $(b_1, \dots, b_n)$ constitutes a lattice basis for $\mathcal{L}$. The dimension of the lattice is given by $\dim(\mathcal{L}) = n$, while its determinant is defined as $\det(\mathcal{L}) = \sqrt{\det(B^T B)}$, where B represents the matrix composed of the vectors $b_i' s$ in the canonical basis of $\mathbb{R}^m$. Let $||v||$ denote the Euclidean norm of a vector $v \in \mathcal{L}$. The Lenstra–Lenstra–Lovász (LLL) algorithm, developed by [17], generates a reduced basis, providing a partial but affirmative solution to this problem. The subsequent result establishes constraints on the magnitude of the reduced basis vectors (see [18]).

Theorem 2.2. *[17] Consider a basis $\{v_1, \dots, v_\omega\}$ spanned a lattice $\mathcal{L}$ with dimension ω. A reduced basis $\{b_1, \dots, b_\omega\}$ is yield through the LLL algorithm which satisfies the following:*

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

An important application of the LLL algorithm lies in its capacity to resolve the problem of simultaneous Diophantine approximations. In [17], the authors presented a method to determine the simultaneous Diophantine approximations to rational numbers, thereby focusing on lattices with real-valued entries. Conversely, in the following theorem, [15] extended this result to lattices with integer entries, thus offering a comparable outcome.

Theorem 2.3. *[15, Theorem 4] Suppose for any rational numbers $\beta_1, \beta_2, \cdots, \beta_k$ and $0 < \epsilon < 1$, there exists an algorithm to output $p_i \in \mathbb{Z}$ where $i = 1, 2, \cdots, k$ and $q \in \mathbb{Z}$ in polynomial time when*

$$\max_i |q\beta_i - p_i| < \epsilon \ \text{ and } \ q \le 2^{k(k-3)/4} \cdot 3^k \cdot \epsilon^{-k}.$$

2.3. Bound of $\psi(N)$

We reformulate the lemma using our modified $\psi(N)$ to find its bound. Note that there is not much difference from the previous lemma that used the standard $\phi(N)$.

Lemma 2.4. *Suppose $N = pq$, where p and q are two large and balanced primes. Let $\psi(N) = (p+1)(q+1)$, then*

$$N + 2\sqrt{N} + 1 < \psi(N) < N + \frac{3}{\sqrt{2}}\sqrt{N} + 1.$$

Proof. Suppose from the equation

$$\psi(N) = (p+1)(q+1),$$

we have

$$f(p) = (p+1)(\frac{N}{p} + 1).$$

Utilizing

$$\sqrt{N} < p < \sqrt{2}\sqrt{N},$$

hence,

$$f(\sqrt{N}) < f(p) < f(\sqrt{2}\sqrt{N}),$$

which leads to

$$f\left(\sqrt{N}\right) = \left((\sqrt{N}) + 1\right)\left(\frac{N}{\sqrt{N}} + 1\right)$$

$$= N + 2\sqrt{N} + 1,$$

and

$$\begin{aligned} f\left(\sqrt{2}\sqrt{N}\right) &= \left((\sqrt{2}\sqrt{N}) + 1\right)\left(\frac{N}{\sqrt{2}\sqrt{N}} + 1\right) \\ &= N + \sqrt{2}\sqrt{N} + \frac{1}{\sqrt{2}}\sqrt{N} + 1. \end{aligned}$$

Thus, we have

$$N + 2\sqrt{N} + 1 < \psi(N) < N + \sqrt{2}\sqrt{N} + \frac{1}{\sqrt{2}}\sqrt{N} + 1,$$

which terminates the proof. □

Next, we present a lemma that will be needed in counting the weak exponents for which our attack applies.

Lemma 2.5. *Let $\mathcal{A}, \mathcal{B} \in \mathbb{Z}^+$. Then,*

$$\sum_{\substack{k=1 \\ \gcd(k,\mathcal{B})=1}}^{\mathcal{A}} 1 > \frac{c\mathcal{A}}{(\log\log\mathcal{B})^2}, \tag{2.1}$$

where $c \in \mathbb{Z}^+$.

The detailed proof was provided in [19]. The lemma is correct depending on the established condition from [14, Theorem 328], which stated that

$$\frac{\phi(N)}{N} > \frac{c_1}{\log\log N},$$

where $\phi(N) = (p-1)(q-1)$. In our case, we have $\psi(N) = (p+1)(q+1) > \phi(N)$, thus it leads to

$$\frac{\psi(N)}{N} > \frac{\phi(N)}{N} > \frac{c_1}{\log\log N}.$$

3. Results and discussions

This section presents the formulation of the proposed attacks along with a detailed discussion of their mechanisms and implications. Specifically, we outline how each attack is constructed, the mathematical principles involved, and the potential vulnerabilities they exploit within the RSA cryptosystem.

3.1. Attack on key equation using continued fraction

In this section, we present our first attack on the alternative totient-like function $\psi(N) = (p+1)(q+1)$ using the continued fraction method. We demonstrate that the RSA modulus N can be efficiently factored through this approach, provided that the private exponent x lies within a specific bound that we identify as insecure.

Theorem 3.1. *Let $N = pq$ denote the product of large unknown primes such that they are balanced primes. Suppose $ex - \psi(N)y = 1$ with $\psi(N) = (p+1)(q+1)$, $\quad e = N^{\alpha}$ and $\quad x = N^{\delta}$. Let $\psi_0(N) = N$. For $1 \le y < x < N^{\delta}$, the private parameter x is feasible to be found leading to factorization of N for $\frac{1}{2} < \alpha < \frac{3}{2}$ if*

$$\delta < \frac{3}{4} - \frac{\alpha}{2}.$$

Proof. Suppose that

$$ex - \psi(N)y = 1, \tag{3.1}$$

where $\psi(N) = (p+1)(q+1)$ and $\psi_0 = N$. Then, dividing (3.1) by $x\psi_0(N)$, we have

$$\begin{aligned}\left|\frac{y}{x} - \frac{e}{\psi_0(N)}\right| = \frac{|ex - \psi_0(N)y|}{x\psi_0(N)} &\le \frac{|ex - \psi(N)y| + |\psi(N)y - \psi_0(N)y|}{x\psi_0(N)} \\ &= \frac{|ex - \psi(N)y| + y|\psi(N) - \psi_0(N)|}{d\psi_0(N)}.\end{aligned}$$

We have

$$|ex - \psi(N)y| = 1$$

and

$$\psi(N) - \psi_0(N) < \frac{3}{\sqrt{2}}\sqrt{N} + 1 < 3\sqrt{N}.$$

Also, by Lemma 2.4,

$$\psi(N) > N + \frac{3}{\sqrt{2}}\sqrt{N} + 1 > N.$$

Utilising this, we have

$$\left|\frac{x}{y} - \frac{e}{\psi_0(N)}\right| < \frac{1 + 3y\sqrt{N}}{d\psi_0(N)} < \frac{x}{y} \cdot \frac{1 + 3\sqrt{N}}{\psi_0(N)}.$$

Suppose

$$\psi_0(N) = N.$$

Then,

$$\begin{aligned}\left|\frac{x}{y} - \frac{e}{\psi_0(N)}\right| &< \frac{x}{y} \cdot \frac{1 + 3\sqrt{N}}{\psi_0(N)} \\ &= \frac{x}{y} \cdot \frac{1 + 3\sqrt{N}}{N}.\end{aligned}$$

Now, we have

$$y\psi(N) = ex - 1 < ex.$$

Then,

$$\frac{y}{x} < \frac{e}{\psi(N)}. \tag{3.2}$$

Since

$$e < N^{\alpha}$$

and

$$\psi(N) > N,$$

thus we have the following inequality

$$\frac{e}{\psi(N)} < \frac{N^{\alpha}}{N}.$$

Then, we obtained the following:

$$\left|\frac{x}{y} - \frac{e}{\psi_0(N)}\right| < \frac{N^{\alpha}}{N} \cdot \frac{1 + 3\sqrt{N}}{N} = \frac{N^{\alpha}\left(1 + 3\sqrt{N}\right)}{N^2}. \tag{3.3}$$

Abiding by Legendre's theorem, Equation (3.3) must satisfy

$$\begin{aligned} \frac{N^{\alpha}\left(1 + 3\sqrt{N}\right)}{N^2} &< \frac{1}{2N^{2\delta}} \\ N^{\alpha} &< \frac{N^2}{2N^{2\delta}\left(1 + 3\sqrt{N}\right)} \\ &< \frac{N^2}{N^{2\delta+1/2}} \\ &< N^{3/2-2\delta}. \end{aligned}$$

□

Considering only the indices, we have

$$\alpha < \frac{3}{2} - 2\delta,$$

which then gives us

$$\delta < \frac{3}{4} - \frac{\alpha}{2}. \tag{3.4}$$

Since $\delta > 0$, then we have $\alpha < \frac{3}{2}$. Additionally, we need to consider the equality of

$$ex = 1 + \psi(N)y.$$

It can be seen that

$$\psi(N)y < ed$$

and since the size of

$$\psi(N) = N,$$

thus for

$$e = N^{\alpha}, \quad x = N^{\delta}$$

we have

$$\alpha + \delta > 1.$$

Substituting the value of δ from (3.4),

$$\begin{aligned} \alpha + \frac{3}{4} - \frac{\alpha}{2} &> 1 \\ \alpha &> \frac{1}{2}. \end{aligned}$$

Therefore, the continued fraction would yield the values of $\frac{y}{x}$ whenever the public parameter e satisfies the condition such that

$$e = N^{\alpha}$$

where

$$\frac{1}{2} < \alpha < \frac{3}{2}.$$

Given the value of $\frac{y}{x}$, we can find

$$\psi(N) = \frac{ex + 1}{y}.$$

Utilizing these pieces of information, we proceed to retrieve the prime factors of the modulus N. We expand and rearrange

$$\psi(N) = (p + 1)(q + 1),$$

to produce the following:

$$p + q = \psi(N) - N - 1. \tag{3.5}$$

Substituting the values from Eq (3.5) and the modulus N into a quadratic equation would give

$$\begin{aligned} X^2 - (\psi(N) - N - 1)X + N &= 0 \\ X^2 - (p + q)X + N &= 0 \end{aligned} \tag{3.6}$$

Solving (3.6) via the formula of finding roots would give us the primes p and q.

The following algorithm summarises the steps needed to factor the modulus N.

Algorithm 3.1 Prime decomposition via Theorem 3.1

```
Input: The public parameters $(N, e)$
Output: The prime factors $p$ and $q$
  1. Compute the continued fractions of $\frac{e}{N}$.
  2. For each convergent $\frac{y'}{x'}$ of $\frac{e}{N}$, compute $\psi(N)' = \frac{ex'-1}{y'}$.
  3. For $\psi(N)' \in \mathbb{Z}$, proceed to Step 4. Else, repeat Step 2.
  4. Solve the roots of the equation $X^2 - (\psi(N)' - N - 1)X + N = 0$.
  5. Return $p = X_1$ and $q = X_2$.
```

Next, we demonstrate the process of factoring the modulus given a pair of public parameter (N, e).

Example 3.1. *Consider the following public parameter.*

N =10113055574309732212192875545347890767386703595133424016075980350310991860/
70758624277966716499748084716383401583901712377262429305549312217487887921/
99137879854592950281052102501872807427624690495979504084202047534385785768/
51816145324744757730938119521732733125387832559952533560920245439388040977/
3289491731541,

e =691978343977415178495556425856087632484044960954964686585623957580789175345/
385961959805733763148221941714194140341874746603368885602028558168445178801/

$$\begin{aligned}&047615721099018445859278784696777441424067330423917118696078463702514050192/\\&146841874041434408115694596403285529058358366664162922762656630356776595080/\\&81294981.\end{aligned}$$

Applying continued fraction on $\frac{e}{N}$ we have the following lists of convergents

$$\left[0, 1, \frac{2}{3}, \frac{11}{16}, \frac{13}{19}, \frac{1116}{1631}, \frac{1129}{1650}, \frac{2245}{3281}, \frac{21334}{31179}, \frac{23579}{34460}, \frac{115650}{169019}, \frac{139229}{203479}, \frac{394108}{575977}, \frac{533337}{779456}, \frac{1994119}{2914345}, \dots, \frac{353986704116483578013901199523780882395940145607796444525139084556928637651 63}{517340931613544051147380291406938473607712695001124029438037386776273667075 53}\right].$$

We compute the

$$\psi(N)' = \frac{ex-1}{y}$$

by using 131^{st} *convergent,*

$$\begin{aligned}\psi(N)' =&1011305557430973221219287554534789076738670359513342401607598035031099/\\&1860707586242779667164997480847163834015839017123772624293055493122174/\\&8788792199137900183921040187597663661502934086097087777156964387331774/\\&9254676571082738480675349538549224330193938683910367720814860482612309/\\&5498068106856653503371864068 4.\end{aligned}$$

Next, we compute

$$p, q = \frac{-(\psi(N)' - N - 1) \pm \sqrt{(\psi(N)' - N - 1)^2 - 4N}}{2},$$

which would give us

$$\begin{aligned}p =&1164447464218134606274967217358355394916037497675506902014022865477004/\\&3603536010774603522859180159650170343905998413120740445267800805332335/\\&687746176028321,\\q =&8684853447725199498409957953074918448120802483548060707250853216569712 0/\\&8307827673167409019264401689088943898775747340218517648472548185582107 3/\\&998050880821.\end{aligned}$$

Since we have retrieved the primes of the modulus N, we can proceed to compute the original Euler Totient function

$$\phi(N) = (p-1)(q-1)$$

and

$$d \equiv e^{-1} \mod \phi(N),$$

which gives us

$$d = 673254313901459141092338295244477833226198595412079393994498041690063602474$$

9208211073669320965515810502269647008282417564328691524267877941929140562431458481238460418375516013710749504696583401980906568259383593290079090279815632080509249717377288616772654601038789570751515161939203186128392625183528671662 1.

3.1.1. Discussions

We start this section by presenting a comparison table that shows the parameters computed using the original Euler Totient function

$$\phi(N) = (p-1)(q-1)$$

and our equation

$$\psi(N) = (p+1)(q+1).$$

Note that we used the same public key (e, N) to generate the following parameters.

Table 1. Comparison of bounds between two private exponents.

Equation	$\phi(N) = (p-1)(q-1)$	$\psi(N) = (p+1)(q+1)$
Private exponent	d = 6732543139014591410923382952444778332 2/ 61985954120793939944980416900636024749208/ 21107366932096551581050226964700828241756/ 43286915242678779419291405624314584812384/ 60418375516013710749504696583401980906568/ 25938359329007909027981563208050924971737/ 72886167726546010387895707515151619392031/ 8612839262518352867166 21 $d < N^{\delta_1}; \delta_1 = 0.9994$	x = 51734093161354405114738029140693847360/ 77126950011240294380373867762736670755 3 $x < N^{\delta_2}; \delta_2 = 0.2491$
Private exponent	k = 46066928218277991986855849219800148537 24/ 27272456209107079125214850140262069344644 34/ 73554051120106318109246783857261733491847 35/ 31859506311548877060996975051191342451485 67/ 59383815032027442584167285344089566117454 58/ 78689237073758390066898242772003990119669 98/ 50706931844128654374525045520382814240502 37/ 6746635633	y = 35398670411648357801390119952378088239/ 59401456077964445251390845569286376516 3
Listed among the convergent	No	Yes
Security	The size of d is bigger than the unsafe bound thus secure from low exponent attack.	The size of x is within the unsafe bound thus vulnerable to low exponent attack.

From the sequence of convergents, it is evident that the ratio $\frac{k}{d}$ associated with $\phi(N)$ does not appear among the convergents of $\frac{e}{N}$, as the value of d is sufficiently large. However, certain values of x and y are small enough to manifest as convergents within the same expansion of $\frac{e}{N}$. The above table provides a comparative analysis of the bounds for d, which is calculated using both the traditional Euler Totient function and the new equation. Notably, the size of d ceases to be critical in ensuring the cryptosystem's resilience against attacks. Now, alternative considerations must be explored to guarantee the robustness of the cryptosystem.

Remark 1. *In our theorem, we demonstrated that the proposed attack is effective through the use of continued fractions when the private parameter satisfies*

$$\delta < \frac{3}{4} - \frac{\alpha}{2}.$$

For the range

$$\frac{1}{2} < \alpha < \frac{3}{2},$$

the private exponent x corresponds to

$$0 < \delta < \frac{1}{2}.$$

Through our example, we illustrated that it is possible to derive $\frac{y}{x}$ for the value of $x < N^{\delta}$ with $\delta < 0.2491$. *Note that, we only utilize our equation as a tool to retrieve the actual private parameters that are generated from the public key (e, N). Moreover, this result demonstrates that our bound extends beyond the threshold established by [2]. Consequently, careful consideration must be given to selecting the public parameter to ensure that continued fractions cannot produce a candidate $\frac{y}{x}$ within the outlined boundaries.*

3.1.2. Estimating the number of public exponent $e's$ satisfying $ex - \psi(N)y = 1$

In this section, we present the estimation number of public exponent e that satisfies

$$ex - \psi(N)y = 1.$$

We begin by presenting a corollary showing that

$$\gcd(x, y) = 1.$$

Corollary 3.1. *If*

$$\gcd(e, \psi(N)) = 1$$

and has solutions of $x, y \in \mathbb{Z}$, then $\gcd(x, y) = 1$.

Next, we present the following lemma which shows that the public parameter $e < \psi(N)$ satisfies at most one equation $ex - \psi(N)y = 1$, where the unknowns x, y satisfy the conditions stated in Theorem 3.1.

Lemma 3.2. *Suppose N is composed of the product of two large and balanced primes p and q. For $i = 1, 2$, let $e < \psi(N)$ be the public parameter satisfying $ex_i - y_i\psi(N) = 1$ with* $\gcd(x_i, y_i) = 1$, *then $x_1 = x_2$ and $y_1 = y_2$.*

Proof. Suppose that e satisfies two equations

$$ex_1 - \psi(N)y_1 = 1,$$
$$ex_2 - \psi(N)y_2 = 1.$$

Equating both of the above equations would give us

$$\frac{1 + \psi(N)y_1}{x_1} = \frac{1 + \psi(N)y_2}{x_2}. \tag{3.7}$$

Rearrange (3.7) to

$$x_2 - x_1 = \psi(N)\left(y_2x_1 - y_1x_2\right). \tag{3.8}$$

From the left-hand side of (3.8), it is straightforward that

$$x_2 - x_1 < \psi(N).$$

Thus, from the right-hand side (3.8), we deduce that

$$y_2x_1 - y_1x_2 = 0.$$

Since

$$\gcd(x_1, y_1) = \gcd(x_2, y_2) = 1,$$

it shows that $x_1 = x_2$ and $y_1 = y_2$. □

Now, we proceed with an estimation of the number of $e < \psi(N)$ for which the Theorem 3.1 works.

Theorem 3.3. *Consider Theorem 3.1. The number of the public parameter $e < \psi(N)$ such that $e = \frac{1+\psi(N)y}{x}$ and $\gcd(x, y) = 1$ with $1 \le y < x < N^{3/4-\alpha/2}$ for $\frac{1}{2} < \alpha < \frac{3}{2}$ is at least $N^{3/2-\epsilon}$ where $\epsilon > 0$ is arbitarily small for suitably large N.*

Proof. The number of the public parameter e which satisfies the equation

$$e = \frac{1 + \psi(N)y}{x}$$

with the conditions given in the theorem is

$$\mathcal{N} = \sum_{x=1}^{\mathcal{N}_1} \sum_{\substack{y=1 \\ \gcd(x,y)=1}}^{x-1} 1, \tag{3.9}$$

where

$$\mathcal{N}_1 = N^{3/4-\alpha/2}.$$

Building upon the result derived in [19], Lemma 3.3, the following inequality holds:

$$\sum_{\substack{y=1 \\ \gcd(x,y)=1}}^{x-1} 1 > \frac{Cx}{(\log\log N)^2}. \tag{3.10}$$

Since

$$\frac{\phi(N)}{N} > \frac{Cx}{(\log\log N)^2},$$

where C is a constant (see [14, Theorem 328]), and knowing that

$$\psi(N) > \phi(N),$$

it follows that

$$\frac{\psi(N)}{N} > \frac{Cx}{(\log\log N)^2}.$$

This implies that inequality (3.10) holds in our case. Next, we substitute the value from (3.10) into (3.9), which gives us:

$$\mathcal{N} > \sum_{x=1}^{\mathcal{N}_1} \frac{Cx}{(\log\log N)^2} = \frac{C}{(\log\log N)^2} \sum_{x=1}^{\mathcal{N}_1} x. \tag{3.11}$$

Following this, for $\sum_{x=1}^{\mathcal{N}_1} x$,

$$\sum_{x=1}^{\mathcal{N}_1} x = \frac{\mathcal{N}_1(\mathcal{N}_1+1)}{2} > \frac{1}{2}\mathcal{N}_1^2 = \frac{1}{2}\left(N^{3/4-\alpha/2}\right)^2 = \frac{1}{2}N^{3/2-\alpha}. \tag{3.12}$$

Then, by substituting (3.12) into (3.11), we have

$$\mathcal{N} > \frac{C}{(\log\log N)^2} \times \frac{1}{2}N^{3/2} > \frac{CN^{3/2-\alpha}}{2(\log\log N)^2} = N^{3/2-\epsilon},$$

where we set

$$N^{-\epsilon} = \frac{CN^{\alpha}}{2(\log\log N)^2}$$

for $\frac{1}{2} < \alpha < \frac{3}{2}$ and $\epsilon > 0$ is arbitaryly small for large N. □

3.2. *Attack on equation $e_ix - \psi(N_i)y_i = 1$*

This section describes an attack on the system of the equation of $e_ix - \psi_(N_i)y_i = 1$ for $1 \le i \le k$ where $k \ge 2$.

Theorem 3.4. *Suppose the modulus $N_i = p_iq_i$ for $1 \le i \le k$ be k moduli for $k \ge 2$. Let every modulus be in the same size where $N = \min\{N_i\}$ and e_i for $i, \dots, k$ be k public parameters. Define $\delta = \frac{k}{2(k+1)}$. If there exists integer $x < N^{\delta}$ and k integers $y_i < N^{\delta}$ such that $e_ix - \psi(N_i)y_i = 1$, then the modulus N_i is possible to be factored.*

Proof. Suppose $k \ge 2$ and $i = 1, \dots, k$, then the equation

$$e_ix - \psi(N_i)y_i = 1$$

can be rewritten as

$$\begin{aligned} e_ix - N_iy_i + N_iy_i - \psi(N_i)y_i &= 1, \\ e_ix - N_iy_i &= 1 + y_i(\psi(N_i) - N_i)). \end{aligned}$$

Dividing by N_i, we obtain:

$$\begin{aligned} \left|\frac{e_i}{N_i}x - y_i\right| &= \frac{|1 + y_i(\psi(N_i) - N_i)|}{N_i} \\ &< \frac{|y_i(1 + \psi(N_i) - N_i)|}{N_i}. \end{aligned}$$

From Lemma 2.4, we have the inequality

$$\psi(N) < N + \sqrt{2}\sqrt{N} + \frac{\sqrt{2}}{2}\sqrt{N} + 1.$$

Taking

$$N = \min\{N_i\},$$

we obtain the following:

$$\begin{aligned}\frac{|y_i(1+\psi(N_i)-N_i)|}{N_i} &< \frac{N^{\delta}(\sqrt{2}\sqrt{N}+\frac{\sqrt{2}}{2}\sqrt{N}+1)}{N_i}\\ &< \frac{N^{\delta}(\frac{3}{\sqrt{2}}\sqrt{N})}{N}\\ &= \frac{3}{\sqrt{2}}N^{\delta-\frac{1}{2}}.\end{aligned}$$

Thus, we have the following inequality:

$$\left|\frac{e_i}{N_i}x - y_i\right| < \frac{3}{\sqrt{2}}N^{\delta-\frac{1}{2}}. \tag{3.13}$$

It can be observed that the inequality in Eq (3.13) is related to the condition stated in Theorem 2.3, namely,

$$|q\alpha_i - p_i| < \epsilon.$$

Now, the existence of x, y_i needs to be proved. Assuming

$$\epsilon = \frac{3}{\sqrt{2}}N^{\delta-\frac{1}{2}}$$

and

$$\delta = \frac{k}{2(k+1)},$$

we have

$$\begin{aligned}N^{\delta}\cdot\epsilon^{k} &= N^{\delta}\left(\frac{3}{\sqrt{2}}N^{\delta-\frac{1}{2}}\right)^{k}\\ &= \left(\frac{3}{\sqrt{2}}\right)^{k}.\end{aligned}$$

Then, since

$$\left(\frac{3}{\sqrt{2}}\right)^{k} = 3^{k}\cdot 2^{-\frac{1}{2}k} < 2^{\frac{k(k-3)}{4}}\cdot 3^{k}$$

for $k \geq 2$, we get

$$N^{\delta}\epsilon^{k} < 2^{\frac{k(k-3)}{4}}\cdot 3^{k}.$$

Thus, if $x < N^{\delta}$ then,

$$x < 2^{\frac{k(k-3)}{4}}\cdot 3^{k}\cdot\epsilon^{-m}.$$

In summary, the following inequalities must be satisfied, as stated in Theorem 2.3, for the integers x and y_i to be determined:

$$\left|\frac{e_i}{N_i}x - y_i\right| < \epsilon, \quad x < 2^{\frac{k(k-3)}{4}}\cdot 3^{k}\cdot\epsilon^{-m}.$$

Using the values obtained, one can compute

$$\begin{aligned}\psi(N_i) &= \frac{e_i x - 1}{y_i}\\ &= (p_i + 1)(q_i + 1)\\ &= N_i + p_i + q_i + 1. \end{aligned} \tag{3.14}$$

By rearranging Eq (3.14), we have

$$p_i + q_i = \psi(N_i) - N_i - 1. \tag{3.15}$$

By transforming Eq (3.19) into a quadratic equation, we get

$$\begin{aligned}X^2 - (\psi(N_i) - N_i - 1)X + N_i &= 0\\ X^2 - (p_i + q_i)X + N_i &= 0\\ (X - p_i)(X - q_i) &= 0. \end{aligned} \tag{3.16}$$

Solving (3.16) would give us the roots of p_i and q_i. □

The following algorithm illustrates the steps needed to factor the modulus N_i.

Algorithm 3.2 Concurrent prime decomposition of k RSA moduli via Theorem 3.2

```
Input: Sets of public parameters $(N_i, e_i)$
Output: The prime factors $p_i$ and $q_i$
  1. Set $N = \min\{N_i\}$.
  2. Compute
     (a) $\delta = \frac{k}{2(k+1)}$.
     (b) $\epsilon = \frac{3}{\sqrt{2}} N^{\delta - \frac{1}{2}}$.
     (c) $C = 3^{k+1} \cdot 2^{\frac{(k+1)(k-4)}{4}} \cdot \epsilon^{-k-1}$.
     (d) lattice $\mathcal{L}$ composed of the span of the matrix rows $\mathcal{R}$ as shown in the proof of Theorem 2.3.
     (e) matrix $\mathcal{J}$ by performing the LLL algorithm onto $\mathcal{R}$.
  3. Appoint $\mathcal{G}_{1,1}, \mathcal{G}_{1,2}, \mathcal{G}_{1,3}, \ldots, \mathcal{G}_{1,k}$ as $X, Y_1, \ldots, Y_k$.
  4. for $i = 2, 3, \ldots, k$ do
  5. Calculate
     (a) $\psi(N_i) = \frac{e_i X - 1}{Y_i}$.
     (b) $p_i, q_i = \frac{S_i \pm \sqrt{S_i^2 - 4N_i}}{2}$ where $S_i = \psi(N_i) - N_i - 1$.
     (c)     if $p_i, q_i \in \mathbb{Z}$, then return $p_i, q_i$.
     (d)       else Algorithm fails.
     (e)     end if
     (f) end for
     (g)
```

Next, we demonstrate the process of factoring the modulus given a pair of public parameter (N_i, e_i).

Example 3.2. *Consider the following sets of public parameters*

$$\begin{aligned} N_1 &= 1760605066352527535933735355228984275 39, \\ e_1 &= 16099784177606318061323449381777038067, \\ N_2 &= 11377431971544839991259582890059190 2707, \\ e_2 &= 80228454580518272122138188469893552787, \\ N_3 &= 15081612433407523776795617108933232 7367, \\ e_3 &= 88264900429715776331790096540424504267. \end{aligned}$$

Setting

$$N = \min\{N_i\} = 11377431971544839991259582890059190 2707.$$

For $k = 3$, we obtain

$$\delta = \frac{k}{2(k+1)} = 0.375$$

and

$$\epsilon = \frac{3}{\sqrt{2}} N^{\delta - \frac{1}{2}} \approx 0.00003711938.$$

Then, applying Theorem 2.2, we compute

$$C = \left[3^{k+1} \cdot 2^{(k+1)(k+4)4} \cdot \epsilon^{-k-1} \right] = 21333009137526604445.$$

Computing

$$C_i = \left[-\frac{C \cdot e_i}{N_i} \right]$$

for $i = 1, \ldots, 3$ and obtain

$$\begin{aligned} C_1 &= -2228152243884 1032, \\ C_2 &= -17502990665879370 2772, \\ C_3 &= -11223322059098364439. \end{aligned}$$

Then, constructing lattice $\mathcal{L}$ composed of the span of the matrix rows

$$\mathcal{R} = \begin{bmatrix} 1 & C_1 & C_2 & C_3 \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}.$$

Performing the LLL algorithm to $\mathcal{R}$ would yield

$$\mathcal{J} = \begin{bmatrix} \mathcal{J}_{11} & \cdots & \mathcal{J}_{14} \\ \vdots & \ddots & \vdots \\ \mathcal{J}_{41} & \cdots & \mathcal{J}_{44} \end{bmatrix},$$

and

$$\mathcal{J}_{11} = 748062,$$

$$\begin{aligned}
\mathcal{J}_{12} &= -79984,\\
\mathcal{J}_{13} &= 16972136,\\
\mathcal{J}_{14} &= 1032782,\\
\mathcal{J}_{21} &= -99521795316979,\\
\mathcal{J}_{22} &= -113736368517672,\\
\mathcal{J}_{23} &= 32536150965788,\\
\mathcal{J}_{24} &= -471403033490219,\\
\mathcal{J}_{31} &= 373912680456304,\\
\mathcal{J}_{32} &= -216862778265728,\\
\mathcal{J}_{33} &= -5423909674688,\\
\mathcal{J}_{34} &= -198493206973456,\\
\mathcal{J}_{41} &= 330054618367440,\\
\mathcal{J}_{42} &= 827166475201920,\\
\mathcal{J}_{43} &= -4264742543680,\\
\mathcal{J}_{44} &= -104919931466160.
\end{aligned}$$

Next, computing matrix

$$\mathcal{G} = \mathcal{J} \cdot \mathcal{R}^{-1}$$

gives us

$$\mathcal{G} = \begin{bmatrix} \mathcal{G}_{11} & \cdots & \mathcal{G}_{14} \\ \vdots & \ddots & \vdots \\ \\ \mathcal{G}_{41} & \dots & \mathcal{G}_{44} \end{bmatrix},$$

where

$$\begin{aligned}
\mathcal{G}_{11} &= 748062,\\
\mathcal{G}_{12} &= 111607,\\
\mathcal{G}_{13} &= 876715801,\\
\mathcal{G}_{14} &= 56217043,\\
\mathcal{G}_{21} &= -99521795316979,\\
\mathcal{G}_{22} &= 14848139605998,\\
\mathcal{G}_{23} &= -116637832824395963,\\
\mathcal{G}_{24} &= -7479087357427335,\\
\mathcal{G}_{31} &= 373912680456304,\\
\mathcal{G}_{32} &= 55785847333091,\\
\mathcal{G}_{33} &= 438219232029304532,\\
\mathcal{G}_{34} &= 28099629757235766,\\
\mathcal{G}_{41} &= 330054618367440,\\
\mathcal{G}_{42} &= 49242450214200,
\end{aligned}$$

$$\begin{aligned} \mathcal{G}_{43} &= 386818337404866805, \\ \mathcal{G}_{44} &= 24803685621126276. \end{aligned}$$

Observe from the first row of the matrix $\mathcal{G}$,

$$\begin{aligned} X &= 748062, \\ Y_1 &= 79984, \\ Y_2 &= 16972136, \\ Y_3 &= 1032782. \end{aligned}$$

Next, we compute

$$\begin{aligned} \psi(N_i) &= \frac{e_iX - 1}{Y_i}, \\ \psi(N_1) &= 119710828891019891625065954936349534000, \\ \psi(N_2) &= 239380624874704970870465655772924454176, \\ \psi(N_3) &= 222474646280558827326647803549471452000. \end{aligned}$$

Since we know $\psi(N_i)$, we can solve for

$$p_i, q_i = \frac{S_i \pm \sqrt{S_i^2 - 4N_i}}{2},$$

where

$$S_i = \psi(N_i) - N_i - 1.$$

Finally, we have

$$\begin{aligned} p_1 &= 11007976237694954759, \\ p_2 &= 15782496099484854787, \\ p_3 &= 17930888138083739099, \\ q_1 &= 10874917087946682149, \\ q_2 &= 15167475623993242951, \\ q_3 &= 12407341151609823719. \end{aligned}$$

3.3. Attack on equation $e_ix_i - \psi(N_i)y = 1$

This section describes the attack on the system of equation $e_ix_i - \psi(N_i)y = 1$ for $1 \leq i \leq k$ where $k \geq 2$.

Theorem 3.5. *Suppose $N_i = p_iq_i$ for $i = 1, \dots, k$ be k moduli for $k \geq 2$, where $N = \min\{N_i\}$. Let e_i be k public parameters for $i = 1, \dots, k$. Define $\delta = \frac{k}{2(k+1)}$. For any k integers $x_i < N^\delta$ and an integer $y < N^\delta$ such that $e_ix_i - \psi(N_i)y = 1$, then the modulus N is possible to be factored.*

Proof. Suppose $k \geq 2$ and $i = 1, \dots, k$, then the equation

$$e_ix - \psi(N_i)y_i = 1$$

can be rewritten as

$$\begin{aligned} e_ix_i - N_iy + N_iy - \psi(N_i)y &= 1, \\ e_ix_i - N_iy &= 1 + y(\psi(N_i) - N_i). \end{aligned}$$

Dividing by e_i we would have,

$$\begin{aligned} \left|\frac{N_i}{e_i}y - x_i\right| &= \frac{|1 + y(\psi(N_i) - N_i)|}{e_i} \\ &< \frac{|y(1 + \psi(N_i) - N_i)|}{e_i}. \end{aligned}$$

From Lemma 2.4,

$$\psi(N) < N + \sqrt{2}\sqrt{N} + \frac{\sqrt{2}}{2}\sqrt{N} + 1$$

and taking

$$e = \min\{e_i\},$$

hence,

$$\begin{aligned} \frac{|y(1 + \psi(N_i) - N_i)|}{e_i} &< \frac{N^{\delta}(\sqrt{2}\sqrt{N} + \frac{\sqrt{2}}{2}\sqrt{N} + 1)}{e_i} \\ &< \frac{N^{\delta}(\frac{3}{\sqrt{2}}\sqrt{N})}{N^{\alpha}} \\ &= \frac{3}{\sqrt{2}}N^{\delta-\alpha+\frac{1}{2}}. \end{aligned}$$

Thus we have

$$\left|\frac{N_i}{e_i}x_i - y\right| < \frac{3}{\sqrt{2}}N^{\delta-\alpha+\frac{1}{2}}. \tag{3.17}$$

It can be seen that the inequality in Eq (3.17) relates to the condition stated in Theorem 2.3 which is

$$|q\alpha_i - p_i| < \epsilon.$$

Now, the existence of y, x_i needs to be proved. Assuming $\epsilon = \frac{3}{\sqrt{2}}N^{\delta-\alpha+\frac{1}{2}}$ and $\delta = \frac{(2\alpha-1)k}{2(k+1)}$,

$$\begin{aligned} N^{\delta} \cdot \epsilon^k &= N^{\delta}\left(\frac{3}{\sqrt{2}}N^{\delta-\alpha+\frac{1}{2}}\right)^k \\ &= \left(\frac{3}{\sqrt{2}}\right)^k. \end{aligned}$$

Then, since

$$\left(\frac{3}{\sqrt{2}}\right)^k = 3^k \cdot 2^{-\frac{1}{2}k} < 2^{\frac{k(k-3)}{4}} \cdot 3^k$$

for $k \geq 2$, we get

$$N^{\delta}\epsilon^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k.$$

Thus, if $x < N^{\delta}$ then,

$$x < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \epsilon^{-m}.$$

In summary, the following inequalities must be satisfied, as stated in Theorem 2.3, for the integers x and y_i to be found:

$$\left|\frac{e_i}{N_i}x - y_i\right| < \epsilon, \quad x < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \epsilon^{-m}.$$

Using the values obtained, for $i = 1, ..., k$, one can compute

$$\begin{aligned} \psi(N_i) &= \frac{e_i x_i - 1}{y} \\ &= (p_i + 1)(q_i + 1) \\ &= N_i + p_i + q_i + 1. \end{aligned} \tag{3.18}$$

By Rearranging Eq (3.18), we have

$$p_i + q_i = \psi(N_i) - N_i - 1. \tag{3.19}$$

By transforming Eq (3.15) into a quadratic equation, we get

$$\begin{aligned} X^2 - (\psi(N_i) - N_i - 1)X + N_i &= 0 \\ X^2 - (p_i + q_i)X + N_i &= 0 \\ (X - p_i)(X - q_i) &= 0. \end{aligned} \tag{3.20}$$

Solving Eq (3.20) would give us the roots of p_i and q_i. □

The following algorithm illustrates the steps needed to factor the modulus N_i.

Algorithm 3.3 Concurrent prime decomposition of k RSA moduli via Theorem 3.3

```
Input: Sets of public parameters $(N_i, e_i)$
Output: The prime factors $p_i$ and $q_i$
 1. Set $N = \max\{N_i\}$ and $e = \min\{e_i\}$.
 2. Compute
    (a) $\delta = \frac{(2\alpha-1)k}{2(k+1)}$.
    (b) $\epsilon = \frac{3}{\sqrt{2}}N^{\delta-\alpha+\frac{1}{2}}$.
    (c) $C = 3^{k+1} \cdot 2^{\frac{(k+1)(k-4)}{4}} \cdot \epsilon^{-k-1}$.
    (d) Lattice $\mathcal{L}$ composed of the span of the matrix rows $\mathcal{R}$ as shown in the proof of Theorem 2.3.
    (e) Matrix $\mathcal{J}$ by performing the LLL algorithm onto $\mathcal{R}$.
    (f) Matrix $\mathcal{G} = \mathcal{J}\mathcal{R}^{-1}$.
 3. Appoint $\mathcal{G}_{1,1}, \mathcal{G}_{1,2}, \mathcal{G}_{1,3}, \ldots, \mathcal{G}_{1,k}$ as $Y, X_1, \ldots, X_k$.
 4. for $i = 2, 3, \ldots, k$ do
 5. Calculate
    (a) $\psi(N_i) = \frac{e_i X_i - 1}{Y}$.
    (b) $p_i, q_i = \frac{S_i \pm \sqrt{S_i^2 - 4N_i}}{2}$ where $S_i = \psi(N_i) - N_i - 1$.
    (c)
      if $p_i, q_i \in \mathbb{Z}$, then return $p_i, q_i$.
 6.   else Algorithm fails.
 7.   end if
 8. end for
```

Next, we demonstrate the process of factoring the modulus given a pair of public parameter (N_i, e_i).

Example 3.3. *Consider the following sets of public parameters*

$$\begin{aligned} N_1 &= 119710828891019891603183061610707897091, \\ e_1 &= 802379080898815685116794541396108712743, \\ N_2 &= 239380624874704970839515684049446356437, \\ e_2 &= 204252676637935432760954971528801513, \\ N_3 &= 222474646280558827296309574259777889181, \\ e_3 &= 2960398127769320728726817047613562907. \end{aligned}$$

Then, we set

$$N = \max\{N_i\} = 239380624874704970839515684049446356437.$$

We also get

$$\min\{e_i\} = N^{\alpha}$$

with $\alpha = 0.927$. *Since* $k = 3$, *we obtain*

$$\delta = \frac{(2\alpha - 1)k}{2k + 1} = 0.3205$$

and

$$\epsilon = \frac{3}{\sqrt{2}} N^{\delta-\alpha+\frac{1}{2}} \approx 0.0001814809309.$$

Then, applying Theorem 2.2, we compute

$$C = [3^{k+1} \cdot 2^{(k+1)(k+4)4} \cdot \epsilon^{-k-1}] = 149345114900000000.$$

Computing

$$C_i = [-\frac{C \cdot e_i}{N_i}]$$

for $i = 1, \dots, 3$ *and obtain*

$$\begin{aligned} C_1 &= -17217660490514083453041148055005395162, \\ C_2 &= -74268257978949950023666474950894327291, \\ C_3 &= -73530011827616972608095990484858831074. \end{aligned}$$

Then, constructing the lattice $\mathcal{L}$ *composed of the span of the matrix rows:*

$$\mathcal{R} = \begin{bmatrix} 1 & C_1 & C_2 & C_3 \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}$$

Performing the LLL algorithm to $\mathcal{R}$ *would yield:*

$$\mathcal{J} = \begin{bmatrix} \mathcal{J}_{11} & \cdots & \mathcal{J}_{14} \\ \vdots & \ddots & \vdots \\ \mathcal{J}_{41} & \dots & \mathcal{J}_{44} \end{bmatrix}$$

and

$$\begin{aligned} \mathcal{J}_{11} &= 255929320328483, \\ \mathcal{J}_{12} &= -91972327270006, \\ \mathcal{J}_{13} &= 112017302482815, \\ \mathcal{J}_{14} &= 342005142641862, \\ \mathcal{J}_{21} &= -663502308951713181165929548783738, \\ \mathcal{J}_{22} &= -1344365126252074249927651644713064, \\ \mathcal{J}_{23} &= 24789888468766336065911918118090, \\ \mathcal{J}_{24} &= 126864785816002898843323125868456, \\ \mathcal{J}_{31} &= 1143405454046964905858869871231785, \\ \mathcal{J}_{32} &= 83670522297219340565303890700998, \\ \mathcal{J}_{33} &= -1099364657786459577190698136281427, \\ \mathcal{J}_{34} &= -473056467498166525473002268580634, \end{aligned}$$

$$\begin{aligned}
\mathcal{J}_{41} &= -13919722814777328115456712116223 20,\\
\mathcal{J}_{42} &= 61851474495887374613942005259224 4,\\
\mathcal{J}_{43} &= -94053338671445885451661309567580 8,\\
\mathcal{J}_{44} &= 15160262484037919144720073327955 16.
\end{aligned}$$

Next, computing matrix

$$\mathcal{G} = \mathcal{J} \cdot \mathcal{R}^{-1}$$

gives us:

$$\mathcal{G} = \begin{bmatrix} \mathcal{G}_{11} & \cdots & \mathcal{G}_{14} \\ \vdots & \ddots & \vdots \\ \mathcal{G}_{41} & \cdots & \mathcal{G}_{44} \end{bmatrix},$$

where

$$\begin{aligned}
\mathcal{G}_{11} &= 255929320328483,\\
\mathcal{G}_{12} &= 33337579844090,\\
\mathcal{G}_{13} &= 143801417249388,\\
\mathcal{G}_{14} &= 142371993081789,\\
\mathcal{G}_{21} &= -66350230895171318116592954878373 8,\\
\mathcal{G}_{22} &= -86428398172689044805623099481045,\\
\mathcal{G}_{23} &= -37280829040235197826436003184656 3,\\
\mathcal{G}_{24} &= -36910247727216423531318255533962 1,\\
\mathcal{G}_{31} &= 11434054540469649058588698712317 85,\\
\mathcal{G}_{32} &= 14894100671831614781748180077918 8,\\
\mathcal{G}_{33} &= 64245598969120719159455728451712 8,\\
\mathcal{G}_{34} &= 63606980702451825179075638569754 6,\\
\mathcal{G}_{41} &= -13919722814777328115456712116223 20,\\
\mathcal{G}_{42} &= -18131954171942335640056431456366 1,\\
\mathcal{G}_{43} &= -78212057372499838299856252113134 8,\\
\mathcal{G}_{44} &= -77434608810835077579597961639999 9.
\end{aligned}$$

Observe from the first row of the matrix $\mathcal{G}$,

$$\begin{aligned}
Y &= 255929320328483,\\
X_1 &= 33337579844090,\\
X_2 &= 143801417249388,\\
X_3 &= 142371993081789.
\end{aligned}$$

Next, we compute

$$\psi(N_i) = \frac{e_i X_i - 1}{Y},$$

which yield:

$$\psi(N_1) = 64120756234785767594964219830501213094365295994120307209008902091973140480000,$$
$$\psi(N_2) = 37989496689035971870436488709545762442152248655490732915220520237204475581440,$$
$$\psi(N_3) = 16252877109882969554525621517760249476535655248534830656603737748620159229760.$$

Since we know $\psi(N_i)$, we can solve for

$$p_i, q_i = \frac{S_i \pm \sqrt{S_i^2 - 4N_i}}{2},$$

where

$$S_i = \psi(N_i) - N_i - 1.$$

Finally, we have

$$\begin{aligned} p_1 &= 15028999435905310589, \\ p_2 &= 16708911996216745859, \\ p_3 &= 11565865260296943587, \\ q_1 &= 16848810653347327999, \\ q_2 &= 11664969248402573633, \\ q_3 &= 11022674864750634611. \end{aligned}$$

4. Conclusions

This paper studies novel cryptanalytic attacks on the RSA by introducing the following:

$$\psi(N) = (p + 1)(q + 1).$$

It is important to emphasize that this formulation strictly applies to cryptanalysis and cannot be employed for encryption or decryption processes, as it fails to meet the criteria outlined in Euler's theorem. Consequently, it does not yield the original plaintext after decryption. Nonetheless, this conceptual framework unveils new opportunities for further exploration within this attack vector.

Author contributions

Nurul Nur Hanisah Adenan: Writing-original draft, writing-review & editing, methodology; Muhammad Rezal Kamel Ariffin: supervision & validation; Wan Nur Aqlili Ruzai: conceptualization, validation, writing-review & editing; Muhammad Asyraf Asbullah: conceptualization, methodology, validation, writing-review & editing; Sook-Chin Yip: funding acquisition, validation, writing-review & editing; Terry Shue Chien Lau: formal analysis, validation, writing-review & editing. All authors have read and approved the final version of the manuscript for publication.

Use of Generative-AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

We acknowledged the support from the Ministry of Higher Education, Malaysia through the Fundamental Research Grant Scheme with reference code FRGS/1/2023/ICT07/MMU/03/1, which gives us the opportunity to do this research. The results of Terry Shue Chien Lau were supported by the Multimedia University Postdoc (MMUI/240034).

Conflict of interest

The authors declare no conflicts of interest in this paper.

References

1. R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM.*, **21** (1978), 17–28. https://doi.org/10.1145/359340.359342
2. M. J. Wiener, Cryptanalysis of short RSA secret exponents, *IEEE Trans. Inf. Theory*, **36** (1990), 553–558. https://doi.org/10.1109/18.54902
3. D. Boneh, Twenty years of attacks on the RSA cryptosystem, *Notices Amer. Math. Soc.* **46** (1999), 203–213.
4. H. M. Bahig, D. I. Nassr, M. A. Mahdi, H. M. Bahig Small private exponent attacks on RSA using continued fractions and multicore systems, *Symmetry*, **14** (2022), 1897. https://doi.org/10.3390/sym14091897
5. M. J. Hinek, *On the security of some variants of RSA*, Ph. D. thesis, Waterloo, 2007
6. S. Sarkar, Small secret exponent attack on RSA varian with modulus $N = p^r q$, *Des. Codes Cryptogr.*, **73** (2014), 383–392. https://doi.org/10.1007/s10623-014-9928-6
7. H. Kuwakado, K. Koyama, Y. Tsuruoka, A new RSA-type scheme based on singular cubic curves $y^2 = x^3 + bx^2 \mod n$, *IEICE Trans. Fundam.*, **E78–A** (1995), 27–33.
8. N. Murru, F. M. Saettone, A novel RSA-like cryptosystem based on a generalization of the R'edei rational functions, In: J. Kaczorowski, J. Pieprzyk, J. Pomykała, *Number-theoretic methods in cryptology*, Springer, 2018. https://doi.org/10.1007/978-3-319-76620-1_6
9. M. W. Bunder, A. Nitaj, W. Susilo, J. Tonien, A new attack on three variants of the RSA cryptosystem, In: J. K. Liu, R. Steinfeld, *Information security and privacy*, Springer, 2016, 258–268. https://doi.org/10.1007/978-3-319-40367-0_16
10. M. W. Bunder, A. Nitaj, W. Susilo, J. Tonien, A generalized attack on RSA type cryptosystems, *Theor. Comput. Sci.*, **704** (2017), 74–81. https://doi.org/10.1016/j.tcs.2017.09.009
11. A. Nitaj, M. R. K. Ariffin, N. N. H. Adenan, N. A. Abu, Classical attacks on a variant of the RSA cryptosystem, In: P. Longa, C. Ràfols, *Progress in Cryptology – LATINCRYPT 2021*, 2021, 151–167. https://doi.org/10.1007/978-3-030-88238-9_8
12. D. I. Nassr, M. Anwar, H. M. Bahig Improving small private exponent attack on the Murru-Saettone cryptosystem, *Theor. Comput. Sci.*, **923** (2022), 222–234. https://doi.org/10.1016/j.tcs.2022.05.010

13. Y. Feng, A. Nitaj, Y. Pan, Partial prime factor exposure attacks on some RSA variants, *Theor. Comput. Sci.*, **999** (2024), 114549. https://doi.org/10.1016/j.tcs.2024.114549

14. G. H. Hardy, E. M. Wright, *An introduction to theory of numbers*, Oxford University Press, 1979. https://doi.org/10.1093/oso/9780199219858.001.0001

15. A. Nitaj, M. R. K. Ariffin, D. I. Nassr, H. M. Bahig, New Attacks on the RSA Cryptosystem, In: D. Pointcheval, D. Vergnaud, *Progress in Cryptology – AFRICACRYPT 2014* 2014, 178–198. https://doi.org/10.1007/978-3-319-06734-6_12

16. W. N. A. Ruzai, A. Nitaj, M. R. K. Ariffin, Z. Mahad, M. A. Asbullah, Increment of insecure RSA private exponent bound through perfect square RSA diophantine parameters cryptanalysis, *Comput. Stand. Interfaces*, **80** (2022), 103584. https://doi.org/10.1016/j.csi.2021.103584

17. A. K. Lenstra, H. W. Lenstra, L. Lov'asz, Factoring polynomials with rational coefficients, *Math. Ann.*, **261** (1982), 515–534. https://doi.org/10.1007/BF01457454

18. A. May, *New RSA vulnerabilities using lattice reduction methods*, Ph. D. thesis, University of Paderborn, North Rhine-Westphalia ,Germany, 2003.

19. A. Nitaj, New weak RSA keys, *JP J. Algebra Number Theory Appl.* **23** (2011), 131–148.

AIMS Press