Malaysian Journal of Mathematical Sciences 19(4): 1237–1256 (2025)
https://doi.org/10.47836/mjms.19.4.03

Malaysian Journal of Mathematical Sciences

Journal homepage: https://mjms.upm.edu.my

Cryptanalysis of The RSA Variant Cryptosystem: Exploiting Weaknesses in Digital Certificates Generated via Compromised Certificate Authority

Mahad, Z.*[1,3], Kamel Ariffin, M. R.[2,3], Abd Ghafar, A. H.[1,2,3], and Salim, N. R.[1]

[1]*Institute for Mathematical Research, Universiti Putra Malaysia,*
43400 UPM Serdang, Selangor, Malaysia
[2]*Faculty of Science, Universiti Putra Malaysia,*
43400 UPM Serdang, Selangor, Malaysia
[3]*Malaysia Cryptology Technology and Management Centre,*
c/o Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia

E-mail: zaharimahad@upm.edu.my
**Corresponding author*

Received: 23 October 2024
Accepted: 5 May 2025

Abstract

A fake or unauthorized digital certificate allows attackers to impersonate trusted websites, tricking users into believing they are on a legitimate site. This enables them to steal sensitive information, spy on communications, or pretend to be someone else on-line. Such certificates are typically created when a Certificate Authority (CA)–the trusted authority entity responsible for issuing secure digital certificates–is compromised or makes a mistake in the key generation process, resulting in certificates that meet security standards but contain vulnerabilities. This study examines the RSA variant cryptosystem known as Murru-Saettone scheme, which the compromised CA has generated the key pairs and used as a digital certificate. We demonstrate that the public parameter $N = pq$ used in this RSA variant cryptosystem can be factorized. Specifically, we show that if an approximation of $\psi(N) = (q^2 + q + 1)(p^2 + p + 1)$, denoted as Ω, is determined and satisfies $|\psi(N) - \Omega| < \alpha N^{\frac{3}{2}}$, the modulus $N = pq$ can be efficiently factorized using continued fractions combined with Coppersmith's method.

Keywords: integer factorization problem; RSA; cubic Pell equation; continued fractions; Coppersmith's method.

1 Introduction

Every day, we inevitably use online digital facilities. Financial transactions, messaging and video conferencing, and storage of important data are some examples of these facilities. Whether we realize it or not, the services we use employ cryptographic methods-either symmetric or asymmetric. For instance, the secure transmission of secret keys between parties in a communication system has a significant impact on the security of symmetric/private key encryption methods. As a result, if the keys are stolen or compromised, it can lead to the exposure of sensitive information and serious security threats. Therefore, modern communication systems typically use asymmetric encryption, such as RSA and ECC, instead of direct interaction between parties. This is also why research on the asymmetric cryptosystem used in our communication system protocol is essential to ensure that symmetric encryption remains secure. Certificate Authority (CA) is the authority entity responsible for generating key pairs, public and private keys in an asymmetric cryptosystem, which ultimately leads to the creation of digital certificates. It is imperative that all parties place complete trust to CA to produce secure public and private keys for their use. However, in today's digital world, it is necessary to perform self-checks on the key pairs obtained from the CA.

The RSA encryption and digital signing mechanisms are widely recognized as the prevailing public-key cryptosystem in contemporary technology, including their prominent application in blockchain technology [17]. Key generation, encryption, and decryption are the three distinct algorithms that comprise the basic RSA cryptosystem [14, 19]. The complexity of breaking down the multiplication of prime pairs (p, q), with equal bit sizes–or, more commonly expressed as $N = pq$, serves as the foundation of RSA security design. To ensure RSA maintains its security strength, the public parameter and private parameter–denoted as (N, e) and (d, p, q), respectively–must satisfy several critical prerequisites during key generation process [18, 1]. From existing literature in [18], the RSA cryptosystem is vulnerable by using continued fractions if the private exponent d is less than $\frac{1}{3}N^{\frac{1}{4}}$. Additionally, if $d < 2\sqrt{2}N^{\frac{3}{4}-\frac{t}{2}}$ for some $t < 1$ and explicitly for $d < 2\sqrt{2}N^{\frac{1}{4}}$, Bunder and Tonien [2] has successfully recovered the secret exponent. Eventually, Boneh and Durfee [1] used Coppersmith's method to improve the limitation of $d < N^{0.292}$ to generate compact solutions of modular univariate polynomials. From that point, Susilo et al. [15] showed that the bound may be expanded from $d < \frac{1}{3}N^{\frac{1}{4}}$ to $d < \frac{1}{\sqrt[4]{18}}N^{\frac{1}{4}}$. The updated bound is partly generated by the requirement that both primes, p and q, possess nearly equal bit lengths.

Numerous strategies employing diverse methodologies have been established to improve the RSA cryptosystem's implementation. Consequently, several RSA variants have been developed. For instance, the work by Takagi [16] introduced a fast RSA-type cryptosystem with modulo $N = p^k q$, while Quisquater and Couvreur [13] proposed a faster RSA decryption algorithm by utilizing the Chinese remainder theorem and more efficient modular multiplication algorithms. Furthermore, Kamel Ariffin et al. [7] introduced an RSA-type cryptosystem with modulo $N = p^2q$, and Elkamchouchi et al. [5] presented an approach that extends the RSA cryptosystem to the realm of Gaussian integers.

Given the existence of fake or unauthorized digital certificates as a reality in today's digital landscape, this serves as motivation to identify the presence of such digital certificates. A fake or unauthorized digital certificate allows attackers to impersonate trusted websites, tricking users into believing they are on a legitimate site. This enables them to steal sensitive information, spy on communications, or pretend to be someone else online. Such certificates are typically created when a Certificate Authority (CA)–the trusted authority entity responsible for issuing secure digital certificates–is compromised or makes a mistake in the key generation process, resulting in certificates that meet security standards but contain vulnerabilities. The authenticity of these fake or unauthorized digital certificates can be trusted based on the fact that the weak key generated meets the criteria outlined in the key generation process, allowing the cryptosystem to continue operating discreetly. Suppose an adversary realizes of the existence of such digital certificates; in that case, they can certainly discover the private keys based on the public parameters retrieved from the digital certificate.

In light of the preceding information, this paper presents a methodology for identifying potential fake or unauthorized digital certificates generated by the CA upon an RSA variant cryptosystem created by Murru-Saettone [8]. Based on the conditions we identify in this work, an adversary is able to successfully factor N using continued fractions combined with Coppersmith's method as the primary approach, particularly if the user has been provided with a fake or unauthorized digital certificate by the CA due to their negligence.

This paper has the following structure. In Section 2, we provide a summary of the Murru-Saettone scheme, including key generation procedure, encryption procedure, and decryption procedure. Next, we describe some helpful lemmas and essential tools that help the cryptanalysis work in Section 3. Furthermore, Section 4 unveils our primary finding, asserting that the Murru-Saettone scheme lacks security under the circumstances outlined in our novel discoveries, thus enabling an adversary to factorize $N = pq$. Additionally, we also present a numerical example to demonstrate our cryptanalysis. Last but not least, we draw our conclusions in Section 5 of the paper.

2 The RSA Variant Cryptosystem Created by Murru-Saettone

The Murru-Saettone cryptosystem was invented in 2018 by Murru and Saettone [8]. They have introduced a variant of the RSA cryptographic system, utilizing the cubic Pell equation,

$$x^3 + cy^3 + c^2z^3 - 3cxyz = 1,$$

modulo an RSA modulus $N = pq$ as its foundation. Both e denoted as public exponent, d denoted as private exponent, satisfy the following equation,

$$ed - k\left(p^2 + p + 1\right)\left(q^2 + q + 1\right) = 1. \tag{1}$$

Let, $(\mathbb{G}, +, \cdot)$ be a field. Let $\mathbb{A}$ be the quotient field $\mathbb{A} = \mathbb{G}[t]/(t^3 - r)$ such that it contains elements in the form of $x + ty + t^2z$ where $(x, y, z) \in \mathbb{G}^3$. Then, a product $\bullet$ between elements in $\mathbb{A}$ can be defined by,

$$(x_1, y_1, z_1) \bullet (x_2, y_2, z_2) = \big(x_1x_2 + (y_2z_1 + y_1z_2)r, x_2y_1 + x_1y_2 + rz_1z_2, y_1y_2 + x_2z_1 + x_1z_2\big). \tag{2}$$

Next, consider the set,

$$\mathcal{A} = \left\{(x, y, z) \in \mathbb{G}^3, \quad x^3 + ry^3 + r^2z^3 - 3xyzr = 1\right\}. \tag{3}$$

Then, $(\mathcal{A}, \bullet)$ is a commutative group with $(1, 0, 0)$ as the identity element; and the inverse element of (x, y, z) is $(x^2 - ryz, rz^2 - xy, y^2 - xz)$. Let B be the quotient group defined by $B = \mathbb{F}^*/\mathbb{G}^*$, which consists elements in the following forms: $m + nt + t^2$, or $m + t$, or 1. Consider the point at infinity (α, α) for the addition operation $\odot$ defined by the following cases:

1. $(m, \alpha) \odot (p, \alpha) = (mp, m + p)$.

2. If $n + p = 0$,
   (a) and $m = n^2$, then $(m, n) \odot (p, \alpha) = (\alpha, \alpha)$.
   (b) and $m \neq n^2$, then $(m, n) \odot (p, \alpha) = \left(\dfrac{mp + r}{m - n^2}, \alpha \right)$.
3. If $n + p \neq 0$, then $(m, n) \odot (p, \alpha) = \left(\dfrac{mp + r}{n + p}, \dfrac{m + np}{n + p} \right)$.
4. If $m + p + nq = 0$,
   (a) and $np + mq + r = 0$, then $(m, n) \odot (p, q) = (\alpha, \alpha)$.
   (b) and $np + mq + r \neq 0$, then $(m, n) \odot (p, q) = \left(\dfrac{mp + (n + q)r}{np + mq + r}, \alpha \right)$.
5. If $m + p + nq \neq 0$, then $(m, n) \odot (p, q) = \left(\dfrac{mp + (n + q)r}{m + p + nq}, \dfrac{np + mq + r}{m + p + nq} \right)$.

Moreover, if k is a positive integer, the exponentiation $(m, n)^{\odot k}$ is defined by,

$$(m, n)^{\odot k} = (m, n) \odot (m, n) \odot \ldots (m, n), \quad (k \text{ times}). \tag{4}$$

Consequently, we can reduce B to

$$B = (\mathbb{G} \times \mathbb{G}) \cup (\mathbb{G} \times \{\alpha\}) \cup \{(\alpha, \alpha)\}. \tag{5}$$

Let, p be a prime. If we take $\mathbb{G} = \mathbb{Z}/p\mathbb{Z}$, then one can choose $\alpha = \infty$. In this case, $\mathbb{A} = \mathbb{G}_{p^3}$ is the finite field with p^e elements. It follows that B is a cyclic group of order $p^2 + p + 1$. As a consequence, we always have $(m, n)^{\odot p^2 + p + 1} = (\alpha, \alpha) \pmod{p}$ for all $(m, n) \in B$. We outline the Murru-Saettone cryptographic system, including its procedures for key generation, encryption, and decryption for this section.

Algorithm 1: Procedure for Murru-Saettone key generation.

```
Input: An integer $k$ bit size of two prime numbers.
Output: $(N, e)$–public parameters and $(p, q, d)$–private parameters.
Select two unique integer primes $(p, q)$ with a bit-size of $k$.
Define $N = pq$.
Define $\psi(N) = (q^2 + q + 1)(p^2 + p + 1)$.
Select an integer $e < \psi(N)$ with $\gcd(e, \psi(N)) = 1$ randomly.
Select $r$, a random integer that is non-cubic residue modulo $p$, $q$, and $N$.
Compute $d \equiv e^{-1} \pmod{\psi(N)}$.
return $(N, e)$–public parameters and $(p, q, d)$–private parameters.
```

Algorithm 2: Procedure for Murru-Saettone encryption.

```
Input: $(N, e)$–public parameters and $(m_1, m_2) \in \mathbb{Z}_N$–messages.
Output: $(c_1, c_2)$–ciphertexts.
Compute $(c_1, c_2) \equiv (m_1, m_2)^{\odot e} \pmod{N}$ using the additional operation $\odot$.
return $(c_1, c_2)$–ciphertexts.
```

Algorithm 3: Procedure for Murru-Saettone decryption.

```
Input: $(p, q, d)$–private parameters and $(c_1, c_2)$–ciphertexts.
Output: $(m_1, m_2) \in \mathbb{Z}_N$–messages.
Compute $(m_1, m_2) \equiv (c_1, c_2)^{\odot d} \pmod{N}$ using the additional operation $\odot$.
return $(m_1, m_2) \in \mathbb{Z}_N$–messages.
```

3 Preliminaries

This section present significant discoveries that will serve as foundational elements throughout this paper. We initiate by revisiting essential principles and relevant prior studies, providing valuable insights to construct our attack strategies.

3.1 Continued fraction expansion

One of an early cryptographic analytical tool applied to RSA is the continued fraction expansion method. It is defined as below.

Definition 3.1 (Continued fraction)**.** *The real number $\xi \in \mathbb{R}$ can be expressed through the continued fraction expansion as follows,*

$$\xi = u_0 + \cfrac{1}{u_1 + \cfrac{1}{u_2 + \cfrac{1}{u_3 + \cfrac{1}{u_4 + \cdots}}}}, \tag{6}$$

where it can be simplified as $\xi = [u_0, u_1, \ldots, u_i, \ldots]$. If ξ represents a rational number, it can be expressed as $[u_0, u_1, \ldots, u_i]$. Hence, for every $i \geq 0$, any rational number $\frac{v}{w}$ that satisfies the equation,

$$\frac{v}{w} = [u_0, u_1, \ldots, u_i],$$

constitutes a convergent of the continued fraction expansion of ξ. Additionally, v and w are coprime. The next theorem provides a technique to determine whether a rational number $\frac{v}{w}$ is a convergent of ξ.

Theorem 3.1 (Legendre's theorem)**.** *Suppose $\xi \in \mathbb{R}$, $\gcd(v, w) = 1$ and*

$$\left|\xi - \frac{v}{w}\right| < \frac{1}{2w^2}. \tag{7}$$

In such a case, $\frac{v}{w}$ is a convergent of the continued fractions expansion of ξ.

Proof. Please refer to [6]. □

3.2 Coppersmith's method

The Coppersmith's method, introduced by [3], is primarily used in order to determine the integer solutions of a univariate or bivariate polynomials modulo a given integer. Specifically, let consider the following polynomial $F(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \pmod N$ with a large integer $N = pq$. If there is a value $|x_0| < N^{1/n}$ such that $F(x_0) \equiv 0 \pmod N$, then Coppersmith [3] showed that the LLL algorithm can efficiently locate $|x_0|$. This algorithm generates a distinct polynomial f related to $F(x)$, which satisfies the criteria imposed for x_0 at smaller values. The method is formalized as in theorem below.

Theorem 3.2 (Coppersmith's method)**.** *Let, N be an integer and $F \in \mathbb{Z}[x]$ be a monic polynomial of degree n over the integers. Suppose $X = N^{\frac{1}{n}-\epsilon}$ for $\dfrac{1}{n} > \epsilon > 0$. Given N, F, then all integers $|x_0| < X$ satisfying $F(x_0) \equiv 0 \pmod N$ can be determined within a polynomial time frame.*

Proof. Please refer to [3]. □

The method is essentially a milestone in attacking RSA since it provides a method to factor modulus $N = pq$ within polynomial time by given a suitable polynomial F. Its running time is dominated by the time it takes to run the LLL algorithm on a lattice of dimension $O(w)$ with $w = \min\left\{\dfrac{1}{\epsilon}, \log_2 N\right\}$ [3]. The following theorem represents an application of Coppersmith's method where using an approximation of p, we can create a lattice that satisfies the condition required in Theorem 3.2.

Theorem 3.3 (Coppersmith's approximation of p)**.** *Consider $N = pq$ be the product of two unknown integers p and q satisfying $q < p < 2q$. If an approximation of p with additive error term at most $N^{1/4}$ is given, then both p and q can be determined in polynomial time.*

Proof. Please refer to [4]. □

Theorem 3.3 is significant throughout this paper, as we will use it as a tool to demonstrate that the obtained approximation of p leads to the factorization of $N = pq$.

3.3 Useful lemmas

The subsequent lemmas provides the bounds for summation $p + q$ with respect to N (Please refer to [10]).

Lemma 3.1. *Suppose $N = pq$, where p and q are two unknown integers satisfying $q < p < 2q$, then, $p+q$ satisfies the following inequalities,*

$$2N^{\frac{1}{2}} < p + q < \frac{3\sqrt{2}}{2}N^{\frac{1}{2}} < 3N^{\frac{1}{2}}.$$

The subsequent lemma indicates that any approximation of summation of $p + q$, will lead to an approximation of the parameter p.

Lemma 3.2. [12] *Consider $N = pq$ where p and q are two unknown integers satisfying $q < p < 2q$. Suppose we approximate $p + q$ as S, where $S > 2\sqrt{N}$, then,*

$$|p + q - S| < \frac{p - q}{3(p + q)}N^{\frac{1}{4}}.$$

Thus, $\tilde{P} = \dfrac{1}{2}\left(S + \sqrt{S^2 - 4N}\right)$ is an approximation of p satisfying $\left|p - \tilde{P}\right| < N^{\frac{1}{4}}$.

Proof. Please refer to [12]. □

The bounds for prime numbers (p, q) with respect to the modulus N is provides by the subsequent result (Please refer to [9]).

Lemma 3.3. *Consider $N = pq$ with (p, q) are two unknown integers satisfying $q < p < 2q$. Then,*

$$\frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N}.$$

The former lemma can assist in determining an upper bound, denoted as ψ_U and a lower bound, denoted as ψ_L for $\psi(N)$.

Proposition 3.1. *Consider $N = pq$ where p and q are two unknown integers satisfying $q < p < 2q$. Suppose $\psi(N) = (q^2 + q + 1)(p^2 + p + 1)$,*

$$(N + \sqrt{N} + 1)^2 < \psi(N) < \left(N + \frac{3}{4}\sqrt{2}\sqrt{N} + 1\right)^2 + \frac{3}{8}N.$$

Hence, $\left(N + \sqrt{N} + 1\right)^2$ is a lower bound ψ_L and $\left(N + \frac{3}{4}\sqrt{2}\sqrt{N} + 1\right)^2 + \frac{3}{8}N$ is an upper bound ψ_U for $\psi(N)$.

Proof. Please refer to [11]. □

We will proceed by establishing $\psi(N) = \left(q^2 + q + 1\right)\left(p^2 + p + 1\right)$. Next, a good approximation for $\psi(N)$ can be discovered with the aid of the former lemma. Subsequently, it is demonstrated in [11] that knowledge of $\psi(N)$ enables the factorization of the modulus $N = pq$.

Proposition 3.2. *Consider $N = pq$ product of two unknown integers that satisfying $q < p < 2q$. Given that, $\psi(N) = \left(q^2 + q + 1\right)\left(p^2 + p + 1\right)$, let us assume this is known. Then,*

$$p = \frac{1}{2}\left(S + \sqrt{S^2 - 4N}\right), \quad \text{and} \quad q = \frac{1}{2}\left(S - \sqrt{S^2 - 4N}\right), \tag{8}$$

where

$$S = \frac{1}{2}\left(\sqrt{(N+1)^2 + 4\left(\psi(N) - (N^2 - N + 1)\right)} - (N+1)\right). \tag{9}$$

Proof. Since,

$$\begin{aligned}\psi(N) &= \left(q^2 + q + 1\right)\left(p^2 + p + 1\right)\\ &= p^2q^2 + p^2q + pq^2 + pq + p^2 + q^2 + p + q + 1\\ &= N^2 + Np + Nq + N + p^2 + q^2 + p + q + 1.\end{aligned} \tag{10}$$

Replacing (10) in S, we get

$$\begin{aligned}
S &= \frac{\sqrt{(N+1)^2 + 4\left(\psi(N) - (N^2 - N + 1)\right)} - (N+1)}{2} \\
&= \frac{1}{2}\left(\sqrt{(N+1)^2 + 4\left(N^2 + Np + Nq + N + p^2 + q^2 + p + q + 1 - N^2 + N - 1\right)} - (N+1)\right) \\
&= \frac{1}{2}\left(\sqrt{(N+1)^2 + 4\left(Np + Nq + 2N + p^2 + q^2 + p + q\right)} - (N+1)\right) \\
&= \frac{1}{2}\left(\sqrt{N^2 + 2N + 4Np + 4Nq + 8N + 4p^2 + 4q^2 + 4p + 4q + 1} - (N+1)\right) \\
&= \frac{1}{2}\left(\sqrt{N^2 + 2N + 4N(p+q) + 4(p+q)^2 + 4(p+q) + 1} - (N+1)\right) \\
&= \frac{1}{2}\left(\sqrt{N(N + 2(p+q) + 1) + N + 2N(p+q) + 4(p+q)^2 + 4(p+q) + 1} - (N+1)\right) \\
&= \frac{1}{2}\left(\sqrt{N(N + 2(p+q) + 1) + 2(p+q)(N + 2(p+q) + 1) + (N + 2(p+q) + 1)} - (N+1)\right) \\
&= \frac{1}{2}\left(\sqrt{(N + 2(p+q) + 1)(N + 2(p+q) + 1)} - (N+1)\right) \\
&= \frac{1}{2}\left(\sqrt{(N + 2(p+q) + 1)^2} - (N+1)\right) \\
&= \frac{1}{2}\left((N + 2(p+q) + 1) - (N+1)\right) \\
&= p + q. \qquad (11)
\end{aligned}$$

Finally, by using S, the integers (p, q) can be discovered easily. □

The subsequent lemmas, along with the theorem, provide insights into the prerequisites that the parameters in the equation $eV - UW = \Omega - \psi_L$ must satisfy.

Lemma 3.4. *Consider $N = pq$ where p and q are two unknown integers satisfying $q < p < 2q$ and $U = \psi_L + \psi_U$. Suppose the positive integers e, V and W satisfy the equation $eV - UW = \Omega - \psi_L$. If*

$$1 \leq W < V < \left|\frac{U}{2(\psi(N) - \psi_L)}\right|, \quad \textit{and} \quad |\Omega - \psi(N)| < \alpha N^{\frac{3}{2}},$$

then, $\dfrac{V}{W}$ is a convergent function of $\dfrac{e}{U} - \dfrac{\alpha N^{\frac{3}{2}}}{2U}$.

Proof. Consider the following equation,

$$eV - UW = \Omega - \psi_L. \qquad (12)$$

Let, $|\Omega - \psi(N)| < \alpha N^{\frac{3}{2}}$. Next, when we divide (12) by UV, we get

$$\begin{aligned}
\left|\frac{e}{U} - \frac{W}{V}\right| &= \left|\frac{\Omega - \psi_L}{UV}\right| \\
&\leq \frac{\alpha N^{\frac{3}{2}} + \psi(N) - \psi_L}{UV} \\
&= \frac{\alpha N^{\frac{3}{2}}}{UV} + \frac{\psi(N) - \psi_L}{UV}, \qquad (13)
\end{aligned}$$

given that $V < \left|\dfrac{U}{2(\psi(N) - \psi_L)}\right|$, it follows that $\dfrac{1}{2V} > \left|\dfrac{(\psi(N) - \psi_L)}{U}\right|$. Since UV will always positive, rearranging (13) yields,

$$\begin{aligned}\left|\left(\frac{e}{U} - \frac{\alpha N^{\frac{3}{2}}}{2U}\right) - \frac{W}{V}\right| &< \left|\frac{\psi(N) - \psi_L}{UV}\right| \\ &= \left|\frac{\psi(N) - \psi_L}{U}\right| \cdot \frac{1}{V} \\ &< \frac{1}{2V} \cdot \frac{1}{V} \\ &= \frac{1}{2V^2},\end{aligned}$$

which satisfies Theorem 3.1 above, thereby concluding the argument. □

Theorem 3.4. *Consider $N = pq$ where p and q are two unknown primes satisfying $q < p < 2q$. Let the positive integers e, V, and W satisfy the equation $eV - UW = \Omega - \psi_L$ where $U = \psi_L + \psi_U$ which ψ_L and ψ_U is the lower and upper bound of $\psi(N)$. If $1 \leq W < V < \left|\dfrac{U}{2(\psi(N) - \psi_L)}\right|$, $|\psi(N) - \Omega| < \alpha N^{\frac{3}{2}}$, $\psi(N) - \alpha N^{\frac{3}{2}} < \Omega < N^2 + \dfrac{7}{2}N + \dfrac{3}{\sqrt{2}}\sqrt{N}\,(N+1) + 1$. Let S be an approximation of $p + q$ such that $|p + q - S| < \dfrac{p - q}{3(p + q)}N^{\frac{1}{4}}$, then N can be efficiently factored in polynomial time.*

Proof. Assuming that the integer e satisfies the equation $eV - UW = \Omega - \psi_L$ and that the integers V, W, and Ω meet the conditions outlined in Lemma 3.4, we are able to determine the integers V and W by calculating the convergents from the continued fractions of $\left(\dfrac{e}{U} - \dfrac{\alpha N^{\frac{3}{2}}}{2U}\right)$. Obtaining V and W, we can compute $\Omega = eV - UW + \psi_L$. Next, using the values of Ω, the approximate summation $p + q$ can be easily calculated as,

$$S = \frac{\sqrt{4\left(\Omega - (N^2 - N + 1)\right) + (N+1)^2} - (N+1)}{2}.$$

Since $\psi(N) - \alpha N^{\frac{3}{2}} < \Omega < N^2 + \frac{7}{2}N + \frac{3}{\sqrt{2}}\sqrt{N}\,(N+1) + 1$, then,

$$\begin{aligned}
S &= \frac{1}{2}\left(\sqrt{4\left(\Omega - (N^2 - N + 1)\right) + (N+1)^2} - (N+1)\right) \\
&< \frac{1}{2}\left(\sqrt{4\left(\left(N^2 + \frac{7}{2}N + \frac{3}{\sqrt{2}}\sqrt{N}\,(N+1) + 1\right) - (N^2 - N + 1)\right) + (N+1)^2} - (N+1)\right) \\
&= \frac{1}{2}\left(\sqrt{4\left(\frac{9}{2}N + \frac{3}{\sqrt{2}}\sqrt{N}(N+1)\right) + (N+1)^2} - (N+1)\right) \\
&= \frac{1}{2}\left(\sqrt{\left(18N + 6\sqrt{2}\sqrt{N}(N+1)\right) + (N+1)^2} - (N+1)\right) \\
&= \frac{1}{2}\left(\sqrt{N^2 + 20N + 6\sqrt{2}\sqrt{N}(N+1) + 1} - (N+1)\right) \\
&= \frac{1}{2}\left(\sqrt{\left(N + 3\sqrt{2}\sqrt{N} + 1\right)^2} - (N+1)\right) \\
&= \frac{1}{2}\left((N+1) + 3\sqrt{2}\sqrt{N} - (N+1)\right) \\
&= \frac{3}{\sqrt{2}}\sqrt{N}.
\end{aligned}$$

Observe that, $2\sqrt{N} < S < \frac{3}{\sqrt{2}}\sqrt{N}$. We have

$$\begin{aligned}
\left|(p-q)^2 - \left(\sqrt{S^2 - 4N}\right)^2\right| &= \left|(p-q)^2 - S^2 + 4N\right| \\
&= \left|(p+q)^2 - S^2\right|.
\end{aligned}$$

Dividing by $p - q + \sqrt{S^2 - 4N}$, we get

$$\begin{aligned}
\frac{\left|p - q - \sqrt{S^2 - 4N}\right|\left(p - q + \sqrt{S^2 - 4N}\right)}{p - q + \sqrt{S^2 - 4N}} &= \frac{|p + q - S|\,(p + q + S)}{p - q + \sqrt{S^2 - 4N}} \\
\left|p - q - \sqrt{S^2 - 4N}\right| &= \frac{|p + q - S|\,(p + q + S)}{p - q + \sqrt{S^2 - 4N}}.
\end{aligned}$$

Since $|p + q - S| < \frac{p-q}{3(p+q)}N^{\frac{1}{4}} < N^{\frac{1}{4}}$, then, $p + q + S < 2(p+q) + N^{\frac{1}{4}} < 3(p+q)$. Combining with $p - q < p - q + \sqrt{S^2 - 4N}$, we have

$$\begin{aligned}
\left|p - q - \sqrt{S^2 - 4N}\right| &= \frac{|p + q - S|\,(p + q + S)}{p - q + \sqrt{S^2 - 4N}} \\
&< \frac{|p + q - S|\,3(p+q)}{p - q} \\
&< \frac{p-q}{3(p+q)}N^{\frac{1}{4}} \cdot \frac{3(p+q)}{p-q} \\
&= N^{\frac{1}{4}}.
\end{aligned}$$

Now, we set $\tilde{P} = \frac{1}{2}\left(S + \sqrt{S^2 - 4N}\right)$. We have

$$\begin{aligned}
|p - \tilde{P}| &= \left| p - \frac{1}{2}(S + \sqrt{S^2 - 4N}) \right| \\
&= \frac{1}{2}\left| p + q - S + p - q - \sqrt{S^2 - 4N} \right| \\
&\leq \frac{1}{2}\left| p + q - S \right| + \frac{1}{2}\left| p - q - \sqrt{S^2 - 4N} \right| \\
&< \frac{1}{2} \cdot \frac{p - q}{3(p + q)} N^{\frac{1}{4}} + \frac{1}{2} N^{\frac{1}{4}} \\
&< N^{\frac{1}{4}}.
\end{aligned}$$

According to Theorem 3.3, the modulus N can be successfully factored in polynomial time. □

4 Generating A Fake or Unauthorized Digital Certificate Based on the RSA Variant Cryptosystem by Compromised CA

This section illustrates the process by which a compromised CA generates a fake or unauthorized digital certificate, based on the Murru-Saetton scheme. By utilizing the criteria detailed in Lemmas 3.2 and 3.4, along with the findings stated in Theorem 3.4, the compromised CA can devise an algorithm for generating vulnerable Murru-Saettone scheme public parameters. The algorithm is outlined as follows.

In Algorithm 4, we show a potential strategy that a compromised CA can use to generate a fake or unauthorized digital certificate based on the Murru-Saetton scheme. In this strategy, a compromised CA will choose the integers Ω and W as in Step $9 - 10$ that satisfy $\xi = \Omega - \psi_L + U \cdot W$ as in Step 11. Next, they will perform a checking process to ensure that the integer ξ is not a prime number. If the condition is satisfied, they will perform a factorization of ξ as in Step 15. The largest factor of ξ will be denoted as the public exponent e, and the rest will be collected as an integer V. All the parameters generated by the compromised CA satisfy the condition as in Lemma 3.2, Lemma 3.4 and Theorem 3.4. Based on this potential strategy, an adversary can factor the modulus N using public parameters (e, N) as shown in Subsection 4.1.

Algorithm 4: Producing vulnerable public key pairs of Murru-Saettone cryptosystem satisfying Lemmas 3.2 and 3.4 together with results from Theorem 3.4.

```
   Input: An integer $k$ bit size of two prime numbers.
   Output: Vulnerable Murru-Saettone scheme public parameters $(N, e)$.
1  Select two unique integer primes $(p, q)$ with a bit-size of $k$.
2  Calculate $N = pq$.
3  Calculate $\psi(N) = (p^2 + p + 1)(q^2 + q + 1)$.
4  Calculate $\psi_L = \left\lfloor (N + \sqrt{N} + 1)^2 \right\rfloor$.
5  Calculate $\psi_U = \left\lceil (N + \frac{3}{4}\sqrt{2}\sqrt{N} + 1)^2 - \frac{3}{8}N \right\rceil$.
6  Calculate $U = \psi_L + \psi_U$.
7  Calculate $\Omega_L = \left\lceil \psi(N) - \alpha N^{\frac{3}{2}} \right\rceil$.
8  Calculate $\Omega_U = \left\lfloor \psi(N) + \alpha N^{\frac{3}{2}} \right\rfloor$.
9  Choose an integer $\Omega \in (\Omega_L, \Omega_U)$ randomly.
10 Select an integer $W < \frac{U}{2(\psi(N) - \psi_L)}$ randomly.
11 Calculate $\xi = \Omega - \psi_L + U \cdot W$.
12 if $\xi$ == PRIME then
13     go to Step 9.
14 else
15     Assign $r_1^{s_1}, r_2^{s_2}, \ldots, r_n^{s_n}$ denoted as $\xi$ prime factors.
16 Calculate $V = \prod_{i=1}^{n} r_i^{s_i}$.
17 if $V < W$ then
18     go to Step 9.
19 else
20     Calculate $e = \xi / V$.
21 return $(N, e)$.
```

4.1 Finding corresponding private parameters from weak RSA variant key pairs by adversary

Based on Theorem 3.4, takes (N, e) which are generated in Algorithm 4, an adversary who is supposedly aware of the existence of these fake or an unauthorized digital certificates, can build an algorithm to find the corresponding private parameters and consequently factor N by employing the continued fraction method and Coppersmith's technique through the LLL algorithm. The algorithm is outlined as follows:

Algorithm 5: Algorithm for extracting private parameters from fake or unauthorized digital certificates through the factorization of the Murru-Saettone cryptosystem moduli.

```
Input: Given vulnerable public parameters, $(N, e)$ from fake or unauthorized digital
       certificates generating using Murru-Saettone cryptosystem that satisfying Theorem
       3.4.
Output: Factors of $N$, $p$ and $q$.
1  Execute the continued fraction method upon $\left(\frac{e}{U} - \frac{\alpha N^{3/2}}{2U}\right)$ to obtain the list of
     convergents $\frac{x_1}{y_1}, \frac{x_2}{y_2}, \ldots, \frac{x_i}{y_i}$.
2  while $1 \leq j \leq i$ do
3      Calculate $\Omega = ex_j - Uy_j + \psi_L$.
4      Calculate $S = \frac{1}{2}\left(\sqrt{4\left(\Omega - (N^2 - N + 1)\right) + (N+1)^2} - (N+1)\right)$.
5      Calculate $\tilde{P} = \frac{1}{2}\left(S + \sqrt{S^2 - 4N}\right)$.
6      Consider the polynomials $F(t) = (\tilde{P} + t)$.
7      Formulate a matrix $M$ comprised of coefficient vectors corresponding to elements of
         $\langle F(t), N \rangle$.
8      Apply the LLL algorithm to the matrix $M$.
9      Formulate the polynomial $M^{'}(t)$ using the initial output row obtained in step number
         8.
10     Calculate the roots of $M^{'}(t)$ to obtain small solution $t_0$.
11     if $\frac{N}{\tilde{P} + t_0}$ is an integer then
12         return $\left(p = \frac{N}{\tilde{P} + t_0},\ q = \frac{N}{p}\right)$.
13 return $\perp$.
```

In Algorithm 5, the convergences of $\left(\frac{e}{U} - \frac{\alpha N^{3/2}}{2U}\right)$ will produce a sequence, where the candidates of W and V denoted as x and y begin from the smallest integer. Since the process of continued fractions ends in polynomial time, the adversary can test all candidates for W and V in polynomial time as in Steps 2 to 13. Starting by computing possible Ω. With the calculated Ω, the adversary next calculates S and $\tilde{P}$ as in Steps 4 and 5 then proceed by constructing a matrix M of coefficient vectors of elements of $\langle F(t), N \rangle$. Next, using the Coppersmith's method via the LLL algorithm upon matrix M, a matrix $M^{'}(t)$ is produced. Calculate the roots of $M^{'}(t)$ to obtain a small solution t_0. Finally, N is factored if the condition as in Steps $11 - 12$ is satisfied.

4.2 Numerical example

We put an illustration of the aforementioned attack, let's examine the following Murru-Saettone cryptosystem public parameters (e, N), with N being $1024-$bits in size.

$$\begin{aligned} N = {} & 23865264217156980883971273067220476711134397430187788595870\\ & 9953408192488462598362701448144405715453127936870395931965881\\ & 7389163130307406817243097431688810216753209519728824861246 17\\ & 409562172376676045679626686045476402449185411211149224414294\\ & 883412467216437968359486376158872894988730881090696299068370\\ & 498091487, \end{aligned}$$

$$\begin{aligned} e = {} & 410545420384104023387623584791923863596402673123540300973043\\ & 793621420101758018692631218110715562019605904184609991123091\\ & 276779644751001591759292958270796703993946184523774226141769\\ & 615977099751746291740584569219701230374108638909590151974376\\ & 959399495908452875582514707306984236251404381225304479852358\\ & 116091639032325136488258412129413256125937744794174367810849\\ & 985028256732859370226543898983660093804231544734554056279060\\ & 558770225335797671226115544728909089451865348092821007867093\\ & 789434002204245611813873140502599604053318778835165098940154\\ & 224343629074685042506715505222941695424306927465304778453454\\ & 17154186438455753. \end{aligned}$$

Followed by computing parameters,

$$\begin{aligned} \psi_L & = \left(N+\sqrt{N}+1\right)\left(N+\sqrt{N}+1\right)\\ & = 569550836154713403635009946972077759305231309887732273487228\\ & \quad 866392632460074994057414140187858137780476828625538215975259\\ & \quad 460298955563410115347278031834233765125859305159714702724752\\ & \quad 476431111885170418919094991257622875397194551187195609197683\\ & \quad 285288480480567900829514760515687069060388620096880084962953\\ & \quad 775445243045047817688498417120907671247602616877261305692060\\ & \quad 281702650584574110970077500792088159214928999571847712677664\\ & \quad 406774223347316759870995954803581708570879695185535956390183\\ & \quad 675864906761385272768651952944141319460002857905093949468545\\ & \quad 877527765775582323810249105195125267589343355341152102665177\\ & \quad 06908992981262383, \end{aligned}$$

and

$$\begin{aligned}\psi_U &= \left(N + \frac{3}{4}\sqrt{2}\sqrt{N} + 1\right)^2 + \frac{3}{8}N \\ &= 5695508361547134036350099469720777593052313098877322734872288 \\ &\quad 866392632460074994057414140187858137780476828625538215975259 \\ &\quad 460298955563410115347278031834233769598695584344599401450453 \\ &\quad 254308114246702764076600109624192336052685607652950522467895 \\ &\quad 404830383549905580222372805987719249289695213159542599221358 \\ &\quad 072093514856549795775003621614928574527634276593893099092281 \\ &\quad 482613309143097841418189867741164505988273096255480065336754 \\ &\quad 870479355956192977883509619407219713380950112447392249983001 \\ &\quad 765720134636858974078016129951063701798766180022024309437957 \\ &\quad 440842506954372538331208779833199781302955967097859141701449 \\ &\quad 28002233529158102,\end{aligned}$$

which values are used to compute,

$$\begin{aligned}A &= \psi_L + \psi_U \\ &= 113910167230942680727001989394415551861046261977546454697445 \\ &\quad 773278526492014998811482828037571627556095365725107643195051 \\ &\quad 892059791112682023069455606366846753472455488950431410417520 \\ &\quad 573073922613187318299569510088181521144988015884014613166557 \\ &\quad 869011886403047348105188756650340631835008383325642268418431 \\ &\quad 184753875790159761346350203873583624577523689347115440478434 \\ &\quad 176431595972767195238826736853325266520320209582732777801441 \\ &\quad 927725357930350973775450557421080142195182980763292820637318 \\ &\quad 544158504139824424684666808289520502125876903792711825890650 \\ &\quad 331837027272995486214145788502832504889229932243901124436662 \\ &\quad 634911226510420485.\end{aligned}$$

By utilizing the integers (e, N, U) above, next computes the continued fraction expansion of $\left(\dfrac{e}{U} - \dfrac{\alpha N^{\frac{3}{2}}}{2U}\right)$ as,

$$\left[0, \frac{1}{2}, \frac{1}{3}, \frac{4}{11}, \frac{9}{25}, \frac{31}{86}, \frac{71}{197}, \frac{315}{874}, \ldots, \frac{51106}{141799}, \ldots\right].$$

The algorithm terminates at the 15th convergent $\dfrac{x_{15}}{y_{15}} = \dfrac{51106}{141799}$. Taking $\dfrac{x_{15}}{y_{15}} = \dfrac{51106}{141799}$, the adversary computes,

$$\begin{aligned}\Omega &= ex_{15} - Ay_{15} + \psi_L \\ &= 56955083615471340363500994697207775930523130988773227348722\\&\quad 8663926324600749940574141401878581377804768286255382159752 59\\&\quad 4602989555634101153472780318342337695986955843445994014504 53\\&\quad 2543081142467027640766001096241923360526856076529505228116 11\\&\quad 9597436618121499880665224604900976825658595843091207460501 77\\&\quad 1380070686694430505078883221440364838371989491914316078388 80\\&\quad 1720412709076141098762732243990216305974314631890508222742 54\\&\quad 1445327289526412700672473521660866234112250206827155944072 53\\&\quad 9828177679144155223470576387175800253590706021752188886388 14\\&\quad 9486287899667401322155019555246460490381784399847774232070 49\\&\quad 80249738019275620.\end{aligned}$$

Using value of Ω, the adversary computes,

$$\begin{aligned}S &= \frac{\sqrt{4\left(\Omega - (N^2 - N + 1)\right) + (N+1)^2} - (N+1)}{2} \\ &= 327709763322984342815492871200386428088169354011005779769113\\&\quad 406188943176612172660172094638041000423336494397127479473543\\&\quad 26060628535114818452360424299707330,\end{aligned}$$

and

$$\begin{aligned}\tilde{P} &= \frac{1}{2}\left(S + \sqrt{S^2 - 4N}\right) \\ &= 218473175548656228543661914133590952058779569340670519846075\\&\quad 604125962117741448442035046817471428715804353963653903684669\\&\quad 79154304323623741049878495826712645.\end{aligned}$$

Let $F(t) = \tilde{P} + t$ and assume the unknown upper bound of $\left|p - \tilde{P}\right|$ is $T = 10^{\gamma}$. The adversary considers the polynomials, N^2, $F(t)N$, $F(t)^2$, $F(t)^2T$ and $F(t)^2T^2$ and build a matrix, M corresponding to these polynomials. Particularly,

$$M = \begin{bmatrix} N^2 & 0 & 0 & 0 & 0 \\ N\tilde{P} & NT & 0 & 0 & 0 \\ \tilde{P}^2 & 2\tilde{P}T & T^2 & 0 & 0 \\ 0 & \tilde{P}^2T & 2\tilde{P}T^2 & T^3 & 0 \\ 0 & 0 & \tilde{P}^2T^2 & 2\tilde{P}T^3 & T^4 \end{bmatrix}.$$

With M_{LLL} as the LLL-reduced matrix. The adversary uses the coefficients from the first row of M_{LLL} to construct polynomials $M'(t)$ where

$$\begin{aligned} M'(t) = t^4 + &\\ &115219023526645706014801461934135042138457068331180128 31\\ &7248982927776144 6550t^3 + \\ &4978283768412651264636373361202805706625802908453083741 2\\ &068972930577564839211066391377915837852496303798940626 17\\ &01134990771176455083387908580689924273t^2 + \\ &955988324391759515848040818721185446416598426756911587 03\\ &476425165704632522219412883600686502461571393268514622 23\\ &850844772291459658569439038657818131311178244518047932 90\\ &674016571309660848177446821840839367685255236567421322 00t + \\ &688425257745579666926059469975918206968430918429389212 95\\ &883655875973905966485793862237020006344690484316062567 87\\ &037450595251537491193595874382256373219806253800159459 64\\ &849171863670847864033391926024609628745883754827734782 84\\ &743389968854282741654569299381568701054186813448345162 07\\ &536031711277256976. \end{aligned}$$

Through identifying the integer roots of $M'(t)$, the adversary successfully obtains,

$$\begin{aligned} t = &-2880475588166142650370036548353376053461426708279503207931 2\\ &2457319440361924. \end{aligned}$$

Observe,

$$\begin{aligned} p &= \tilde{P} + t\\ &= 2184731755486562285436619141335909520587795693406705198460 75\\ &604125962117741448439154571229305286065434317415300527631208\\ &364834763733029479274211763863507 21. \end{aligned}$$

The factorization of N can now be achieved by the adversary through computing,

$$\begin{aligned} q &= N/p\\ &= 109236587774328114271830957066795476029389784670335259923037\\ &802062981058870724219577285614652643032717158707650263815604\\ &182417381866514739637105881931756 47. \end{aligned}$$

Remark 4.1. *The selection of the parameters α and γ is presented in Table 1. By consulting this table, the adversary can execute Algorithm 5 to extract private parameters from fake or unauthorized digital certificates through the factorization of the Murru-Saettone cryptosystem moduli, as demonstrated in the numerical example above.*

Table 1: Values of parameters α and γ corresponding to length of modulus N.

Length of modulus N in bits	α	γ
64	$\frac{1}{10^6}$	4
128	$\frac{1}{10^{10}}$	9
256	$\frac{1}{10^{20}}$	19
512	$\frac{1}{10^{40}}$	38
1024	$\frac{1}{10^{80}}$	76
2048	$\frac{1}{10^{160}}$	150

As mention in Remark 4.1, an adversary is able to execute Algorithm 5 to extract private parameters from fake or unauthorized digital certificates through the factorization of the Murru-Saettone cryptosystem moduli, guided by Table 1. For instance, if the modulus N is 64 bits long, the parameters $\alpha = \dfrac{1}{10^6}$ and $\gamma = 4$ should be used to launch the attack. This principle extends to different sizes of N, requiring corresponding values for α and γ.

Remark 4.2. *The preceding examples involve two randomly selected prime numbers, characterized by $|p - q| \approx N^{0.49}$ and public parameter $e \approx N^2$. Utilizing the values of p and q presented in these examples, an adversary can readily determine the private exponent $d \approx N^2$. Consequently, through these examples, we can see clearly that it becomes challenging for the user to recognize the digital certificate is fake or unauthorized, as both public parameter and private parameter comply with security standards during the key generation process.*

5 Conclusions

We have developed a strategy to identify whether digital certificates generated by the Certificate Authority (CA) using the Murru-Saettone cryptosystem are fraudulent or unauthorized. This is crucial because such digital certificates can exist if the CA is hacked or makes an error in the key generation process. Our research findings demonstrate that the vulnerability of digital certificates based on the Murru-Saettone cryptosystem to attacks depends on the fulfillment of the condition $|\Omega - \psi(N)| < \alpha N^{3/2}$, where Ω represents an approximation of $\psi(N)$. By employing the continued fractions algorithm and Coppersmith's method as primary strategies, an adversary can effectively execute an attack in polynomial time to factor the modulus N, even without any information about the private parameters. Subsequently, the adversary can easily obtain the secret parameter $\psi(N)$ by calculating $\psi(N) = (q^2 + q + 1)(p^2 + p + 1)$. Finally, private exponent d can easily be determined by computing $d \equiv \dfrac{1}{e} \pmod{\psi(N)}$.

Acknowledgement This research was funded by Universiti Putra Malaysia under Putra Grant with project number GP-IPM/2024/9789000. The authors are also thankful to the referees for their useful comments and suggestions.

Conflicts of Interest The authors declare no conflict of interest.

References

[1] D. Boneh & G. Durfee (1999). Cryptanalysis of RSA with private key d less than $N^{0.292}$. In *Advances in Cryptology – EUROCRYPT '99: International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceedings*, volume 1592 of *Lecture Notes in Computer Science* pp. 1–11. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48910-X_1.

[2] M. Bunder & J. Tonien (2016). A new improved attack on RSA. In *Proceedings of the 5th International Cryptology and Information Security Conference 2016 (CRYPTOLOGY2016): Conference Proceedings Cryptology 2016, Kota Kinabalu, Sabah, Malaysia, May 31 - June 2, 2016*, volume 5 pp. 101–110. UPM Press, Selangor, Malaysia. Institute for Mathematical Research. https://mscr.org.my/proceedings.

[3] D. Coppersmith (1996). Finding a small root of a bivariate integer equation; Factoring with high bits known. In *Advances in Cryptology – EUROCRYPT '96: International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996 Proceedings*, volume 1070 of *Lecture Notes in Computer Science* pp. 178–189. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-68339-9_16.

[4] D. Coppersmith (1997). Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology*, *10*(4), 233–260. https://doi.org/10.1007/s001459900030.

[5] H. Elkamchouchi, K. Elshenawy & H. Shaban (2002). Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers. In *The 8th International Conference on Communication Systems, 2002. ICCS 2002*, volume 1 pp. 91–95. Singapore. IEEE. https://doi.org/10.1109/ICCS.2002.1182444.

[6] G. H. Hardy & E. M. Wright (1991). *An Introduction To The Theory Of Numbers*. Oxford University Press, Oxford, United Kingdom.

[7] M. R. Kamel Ariffin, M. A. Asbullah, N. A. Abu & Z. Mahad (2013). A new efficient asymmetric cryptosystem based on the integer factorization problem of $N = p^2q$. *Malaysian Journal of Mathematical Sciences*, *7*(S), 19–37.

[8] N. Murru & F. M. Saettone (2017). A novel RSA-like cryptosystem based on a generalization of the Rédei rational functions. In *Number-Theoretic Methods in Cryptology: First International Conference, NuTMiC 2017, Warsaw, Poland, September 11-13, 2017, Revised Selected Papers*, volume 10737 of *Lecture Notes in Computer Science* pp. 91–103. Springer, Cham. https://doi.org/10.1007/978-3-319-76620-1_6.

[9] A. Nitaj (2008). Another generalization of Wiener's attack on RSA. In *Progress in Cryptology - AFRICACRYPT 2008: First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008, Proceedings*, volume 5023 of *Lecture Notes in Computer Science* pp. 174–190. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-68164-9_12.

[10] A. Nitaj (2013). *Artificial Intelligence, Evolutionary Computing and Metaheuristics: In the Footsteps of Alan Turing*, volume 427 of *Studies in Computational Intelligence*, chapter Diophantine and lattice cryptanalysis of the RSA cryptosystem, pp. 139–168. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-29694-9_7.

[11] A. Nitaj, M. R. Kamel Ariffin, N. N. H. Adenan & N. A. Abu (2021). Classical attacks on a variant of the RSA cryptosystem. In *Progress in Cryptology – LATINCRYPT 2021: 7th International Conference on Cryptology and Information Security in Latin America, Bogotá, Colombia, October 6-8, 2021, Proceedings*, volume 12912 of *Lecture Notes in Computer Science* pp. 151–167. Springer, Cham. https://doi.org/10.1007/978-3-030-88238-9_8.

[12] A. Nitaj, M. R. Kamel Ariffin, D. I. Nassr & H. M. Bahig (2014). New attacks on the RSA cryptosystem. In *Progress in Cryptology–AFRICACRYPT 2014: 7th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 28-30, 2014. Proceedings*, volume 8469 of *Lecture Notes in Computer Science* pp. 178–198. Springer, Cham. https://doi.org/10.1007/978-3-319-06734-6_12.

[13] J. J. Quisquater & C. Couvreur (1982). Fast decipherment algorithm for RSA public-key cryptosystem. *Electronics Letters*, *18*(21), 905–907. https://doi.org/10.1049/el:19820617.

[14] R. L. Rivest, A. Shamir & L. Adleman (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342.

[15] W. Susilo, J. Tonien & G. Yang (2020). A generalised bound for the Wiener attack on RSA. *Journal of Information Security and Applications*, *53*, Article ID: 102531. https://doi.org/10.1016/j.jisa.2020.102531.

[16] T. Takagi (1998). Fast RSA-type cryptosystem modulo $p^k q$. In *Advances in Cryptology–CRYPTO'98: 18th Annual International Cryptology Conference Santa Barbara, California, USA August 23-27, 1998 Proceedings 18*, volume 1462 of *Lecture Notes in Computer Science* pp. 318–326. Springer, Berlin, Heidelberg. https://doi.org/10.1007/BFb0055738.

[17] N. A. Ugochukwu, S. B. Goyal, A. S. Rajawat, S. M. N. Islam, J. He & M. Aslam (2022). An innovative blockchain-based secured logistics management architecture: Utilizing an RSA asymmetric encryption method. *Mathematics*, *10*(24), Article ID: 4670. https://doi.org/10.3390/math10244670.

[18] M. J. Wiener (1990). Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory*, *36*(3), 553–558. https://doi.org/10.1109/18.54902.

[19] M. Zheng (2022). Revisiting the polynomial-time equivalence of computing the CRT-RSA secret key and factoring. *Mathematics*, *10*(13), Article ID: 2238. https://doi.org/10.3390/math10132238.