Cryptanalysis of RSA-Variant Cryptosystem Generated by Potential Rogue CA Methodology

Zahari Mahad 1, Muhammad Rezal Kamel Ariffin 1,2,*, Amir Hamzah Abd. Ghafar 2 and Nur Raidah Salim 1

Abstract: Rogue certificate authorities (RCA) are third-party entities that intentionally produce key pairs that satisfy publicly known security requirements but contain weaknesses only known to the RCA. This work analyses the Murru–Saettone RSA variant scheme that obtains its key pair from a potential RCA methodology. The Murru–Saettone scheme is based on the cubic Pell equation \( x^3 + ry^3 + r^2z^3 - 3xyz = 1 \). The public, \( e \), and private, \( d \) key generation process uses the secret parameter \( \psi = (p^2 + p + 1)(q^2 + q + 1) \) in place of the standard Euler–phi function \( \phi(N) = (p - 1)(q - 1) \), where \( ed \equiv 1 \pmod{\psi} \). We prove that, upon obtaining an approximation of \( \psi \), we are able to identify the provided key pair that was maliciously provided even if the private key \( d \) size is approximate to \( \psi \). In fact, we are able to factor the modulus \( N = pq \).

Keywords: RSA; factorization; continued fractions; cubic Pell equation; rogue certificate authority; secure symmetric encryption

1. Introduction

The security of a symmetric encryption scheme highly depends on the safety of the secret key transmission between parties involved in the communication. Other than direct interaction between parties, the utilization of asymmetric encryption schemes is the norm in modern communication. Central to the production of the public and private key pair of an asymmetric encryption scheme is the Certificate Authority (CA). Parties should have full trust in the CA to provide secure key pairs. Nevertheless, it is wise to conduct due diligence on the key pairs received. As such, for a communication topology with large participation, it is not surprising that the security of a symmetric encryption scheme will fall back on the strength of the asymmetric encryption scheme being utilized. As such, studies on the asymmetric cryptosystem utilized must be conducted to ensure that symmetric encryption remains secure.

RSA encryption/digital signing scheme is currently the world’s most widely used public-key cryptosystem. The standard RSA cryptosystem comprises three distinct algorithms: key generation, encryption, and decryption [1]. The security of RSA is mainly based on the hardness of factoring large composite integers, which is modulus \( N = pq \) where \( p \) and \( q \) are two large prime numbers of the same bit size. It is well known that RSA is not secure if the process of generating the public parameters \( (e, N) \) and the private parameters \( (p, q, d) \) do not satisfy certain conditions [2–6]. For instance, the RSA cryptosystem is vulnerable when employing continued fractions if such decryption exponent \( d \) is less than \( \sqrt[3]{N} \), by a classical finding in [2]. Additionally, [3] has recovered the secret key if \( d < 2\sqrt{N}^{\frac{3}{2} - \frac{1}{2}} \) and explicitly for \( d < 2\sqrt{N}^{\frac{3}{4}} \). Eventually, by using Coppersmith’s technique to obtain...
small solutions of modular univariate polynomials, ref. [5] refined the bound to \( d < N^{0.292} \). From then on, ref. [4] identified that it is possible to raise the bound from \( d < \frac{1}{3}N^{\frac{1}{2}} \) to \( d < \frac{1}{\sqrt{18}}N^{\frac{1}{2}} \). The new bound is generated in part from the constraint that both primes number of \( p \) and \( q \) will have almost the same size of bit length. Moreover, ref. [6] has maximized the small root bounds to small secret exponent RSA using linearization and applications. To the extent of improving the implementation of the RSA cryptosystem, many schemes with various techniques have been proposed. As a result, a lot of RSA variant cryptosystems arise [7–12].

The existence of RCA is the underlying motivation behind the identification of weak public keys. RCA is defined by [13] as an entity issuing legitimate certificates being trusted by web browsers and users but contains hidden weaknesses. There is a window of vulnerability with the existing public key infrastructure between the time a rogue certificate is issued and when it is discovered. Likewise, an RCA can publish a fraudulent RSA digital certificate using these keys without users noticing its anomaly. As the weak keys satisfy the conditions established in the key generation process, the validity of these fraudulent certificates can be convincing. Hence, the cryptosystem continues to operate discreetly using the keys, i.e., suppose an adversary knows about the existence of these specific certificates, then the adversary can find the private keys corresponding to the public keys without knowing any information about the private keys.

In relation to the above, this paper discloses potential RCA methodology upon an RSA variant cryptosystem constructed from a cubic field connected to the cubic Pell equation that was invented by Murru–Saettone [14]. Our identified conditions will allow an adversary to factor the modulus \( N \) if the user has been provided with keys through the potential RCA methodology.

The framework of this paper is as follows. In Section 2, we summarize the Murru–Saettone scheme. Section 3 describes some important tools and useful lemmas, respectively. Moreover, in the Sections 4 and 5, we present our main result, which says that the Murru–Saettone scheme is not secure with experimental results. Finally, we conclude the paper in Section 6.

2. The Scheme of Murru and Saettone

In this section, we summarize the Murru and Saettone cryptosystem [14] along with the key generation, encryption, and decryption procedures.

Key Generation:
- Choose two random prime numbers \( p \) and \( q \) of bit-size \( k \);
- Set \( N = pq \) and \( \psi = (p^2 + p + 1)(q^2 + q + 1) \);
- Choose a random integer \( e < \psi \) with \( \gcd(e, \psi) = 1 \);
- Choose a non-cube integer \( r \) in \( \mathbb{Z}_p, \mathbb{Z}_q \), and \( \mathbb{Z}_N \);
- Compute \( d \equiv e^{-1} \pmod{\psi} \);
- Return the public parameters as \( (N, e, r) \) and the private parameters as \( (p, q, d) \).

Encryption:
- Given a pair of messages \( m_1 \) and \( m_2 \) in \( \mathbb{Z}_N \);
- Compute \( (c_1, c_2) \equiv (m_1, m_2)^e \pmod{N} \);
- Return the ciphertext as \( (c_1, c_2) \).

Decryption:
- Given a pair of ciphertexts \( c_1 \) and \( c_2 \);
- Compute \( (m_1, m_2) \equiv (c_1, c_2)^d \pmod{N} \);
- Return the message as \( (m_1, m_2) \).

3. Preliminaries

In this section, we put forward preliminary concepts needed.
Definition 1. The expression of continued fractions expansion of $\xi \in \mathbb{R}$ can be written in these forms

$$\xi = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots}}}$$

which can also be written as $\xi = [a_0, a_1, \ldots, a_\mu]$. The process of calculating the continued fractions expansion would be executed in polynomial time if $\xi$ is a rational number and thus $\xi = [a_0, a_1, \ldots, a_\mu]$. The convergents $r_s$ of $\xi$ are the fractions denoted by $r_s = [a_0, a_1, \ldots, a_i]$ for $i \geq 0$. An important result on continued fractions that will be used is the following theorem.

Theorem 1. Let $\xi$ be a positive number. Suppose that $\gcd(r, s) = 1$ and

$$|\xi - \frac{r}{s}| < \frac{1}{2s^2}.$$ 

Then $\xi$ is a convergent of the continued fractions expansion of $\xi$.

The following result gives the bounds for $p$, and $q$ in terms of $N$ (See [15]).

Lemma 1. Let $N = pq$ be the product of two unknown integers with $q < p < 2q$. Then

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

In the following, we set $\psi = (p^2 + p + 1)(q^2 + q + 1)$. The former lemma can be used to find a good approximation for $\psi$. The following result shows that one can factor the modulus $N = pq$ if $\psi$ is known [15].

Proposition 1. Let $N = pq$ be the product of two unknown integers with $q < p < 2q$. Suppose that $\psi = (p^2 + p + 1)(q^2 + q + 1)$ is known. Then,

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

where

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

Definition 2. Let $\psi_L$ and $\psi_U$ be the lower bound and the upper bound of $\psi$. Then we define $A = \psi_L + \psi_U$.

The next remark shows how we can find the best current approximation values for $\psi_L$ and $\psi_U$.

Remark 1. From Nitaj [16], we know that $2\sqrt{N} < p + q < \frac{3}{\sqrt{N}}N$. This means

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

as $\psi = (p^2 + p + 1)(q^2 + q + 1)$. Hence, the best current approximation for $\psi_L$ is $(N + \sqrt{N} + 1)^2$ and for $\psi_U$ is $(N + \frac{3}{4}\sqrt{2N} + 1)^2 + \frac{3}{8}N$.

The following lemmas and theorem show conditions to be fulfilled by parameters in the equation $eX - AY = Z - \psi_L$. 


Lemma 2. Let $N = pq$ with $q < p < 2q$. Let $e$ satisfy the equation $eX - AY = Z - \psi_L$ where $X$ and $Y$ are positive integers. If

$$1 \leq Y < X < \left| \frac{A}{2(\psi - \psi_L)} \right| \text{ and } |Z - \psi| < \frac{p - q}{p + q} \frac{N^{1/4}}{2A}$$

then $\frac{X}{Y}$ is a convergent function of $\frac{Z}{A} - \frac{N^{1/4}}{2A}$.

Proof. Consider the following equation

$$eX - AY = Z - \psi_L. \quad (6)$$

Let $|Z - \psi| < \frac{p - q}{p + q} \frac{N^{1/4}}{2A}$, then, divide (8) by $AX$, we obtain

$$\left| \frac{e}{A} - \frac{Y}{X} \right| = \left| \frac{Z - \psi_L}{AX} \right|$$

$$\leq \frac{\frac{p - q}{p + q} \frac{N^{1/4}}{2A} + \psi - \psi_L}{AX}$$

$$< \frac{\frac{N^{1/2}}{2} \frac{N^{1/4}}{2A} + \psi - \psi_L}{AX}$$

$$< \frac{\frac{XN^{1/4}}{2A} + \psi - \psi_L}{AX}$$

$$\leq \frac{\frac{N^{1/4}}{2A} + \psi - \psi_L}{AX}$$

(7)

since $p - q < 2\sqrt{N}$, $p + q > 2\sqrt{N}$ and $X > 1$. If $X < \left| \frac{A}{2(\psi - \psi_L)} \right|$, then $\frac{1}{AX} > \frac{2(\psi - \psi_L)}{A}$. As $AX$ will always be a positive value, rearranging (9), we obtain

$$\left| \left( \frac{e}{A} - \frac{N^{1/4}}{2A} \right) - \frac{Y}{X} \right| < \left| \frac{\psi - \psi_L}{AX} \right|$$

$$< \frac{1}{2A^2}$$

which satisfies Theorem 1. This terminates the proof.

Theorem 2. Let $N = pq$ with $q < p < 2q$. Let $e$ satisfies the equation $eX - AY = Z - \psi_L$ where $X, Y$ are positive integers. If

- $1 \leq Y < X < \left| \frac{A}{2(\psi - \psi_L)} \right|$;
- $\psi + \frac{p - q}{p + q} N^{1/4} < N^2 + 8N + 3\sqrt{NN} + 3\sqrt{N} + 1$;
- $|Z - \psi| < \frac{p - q}{p + q} N^{1/4}$;

then $N$ can be factored in polynomial time.

Proof. Suppose $e$ satisfies an equation $eX - AY = Z - \psi_L$. Let $X, Y$ and $Z$ satisfy the conditions in Lemma 3, then we can find the values of $X$ and $Y$ by computing $\frac{e}{A} - \frac{N^{1/4}}{2A}$. From the values of $X$ and $Y$, we can have the value of $Z$ by computing $Z = eX - AY + \psi_L$. From the values of $Z$, we define Equation (5) as

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

Since, $\psi + \frac{p - q}{p + q} N^{1/4} < N^2 + 8N + 3\sqrt{NN} + 3\sqrt{N} + 1$ then
Symmetry 2022, 14, 1498

Generating weak Murru–Saettone cryptosystem public keys via Lemma 3 and Algorithm 1

Theorem 3

Two distinct primes, 

Input: A RCA can build an algorithm that produces such weak Murru–Saettone cryptosystem public keys. By using conditions in Lemma 3 coupled with results from Theorem 3, a RCA can build an algorithm that produces such weak Murru–Saettone cryptosystem public keys. The Algorithm 1 is as follows:

Algorithm 1 Generating weak Murru–Saettone cryptosystem public keys via Lemma 3 and Theorem 3

Input: Two distinct primes, \( p \) and \( q \) where \( p < q < 2q \)

Output: Weak Murru–Saettone cryptosystem public keys, \((N, e)\)

1. Compute \( N = p \cdot q \)
2. Compute \( \psi = (p^2 + p + 1)(q^2 + q + 1) \)
3. Compute \( \psi_L = \left( (N + \sqrt{N} + 1)^2 \right) \)
4. Compute \( \psi_U = \left( (N + \frac{3}{2}\sqrt{N} + 1)^2 - \frac{3}{2}N \right) \)
5. Compute \( A = \psi_L + \psi_U \)
6. Compute \( Z_L = \left[ \psi - \frac{p-q}{p+q} N^{1/4} \right] \)
7. Compute \( Z_U = \left[ \psi + \frac{p-q}{p+q} N^{1/4} \right] \)
8. Choose an integer \( Z \) randomly between \( Z_L \) and \( Z_U \)
9. Choose an integer \( Y < \left( \frac{A}{2 \sqrt{\psi - \psi_L}} \right) \)
10. Compute \( Z = Z - \psi_L + A \cdot Y \)
11. if \( Z = \) prime number then return to Step 8.
12. else Assign \( r_1^Z, r_2^Z, \ldots, r_n^Z \) to be all the small prime factors of \( Z \)
13. end if
14. Compute \( X = \prod_{i=1}^n r_i^Z \)
15. if \( X < Y \) then return to Step 8.
16. else Compute \( e = \frac{Z}{X} \)
17. end if
18. Output \( N, e \)

Based on Proposition 1, we can factor \( N \) in polynomial time. \( \square \)

4. Generating Weak Murru–Saettone Cryptosystem Public Keys by RCA: Case

In this section, we show how a RCA can generate weak Murru–Saettone cryptosystem public key pairs. By using conditions in Lemma 3 coupled with results from Theorem 3, a RCA can build an algorithm that produces such weak Murru–Saettone cryptosystem public keys. The Algorithm 1 is as follows:

\[
S = \frac{1}{2} \left( \sqrt{(N+1)^2 + 4(Z - (N^2 - N + 1))} - (N+1) \right)
\]

\[
< \frac{1}{2} \left( \sqrt{(N+1)^2 + 4 \left( (N^2 + 8N + 3\sqrt{N}N + 3\sqrt{N} + 1) - (N^2 - N + 1) \right)} - (N+1) \right)
\]

\[
= \frac{1}{2} \left( \sqrt{(N+1)^2 + 4 \left( 9N + 3\sqrt{N}N + 3\sqrt{N} \right)} - (N+1) \right)
\]

\[
= \frac{1}{2} \left( \sqrt{N^2 + 2N + 1 + 36N + 12\sqrt{N}N + 12\sqrt{N} - (N+1)} \right)
\]

\[
= \frac{1}{2} \left( \sqrt{N^2 + 38N + 12\sqrt{N}N + 12\sqrt{N} + 1} - (N+1) \right)
\]

\[
= \frac{1}{2} \left( \sqrt{(N+1 + 6\sqrt{N})^2} - (N+1) \right)
\]

\[
= \frac{1}{2} \left( 6\sqrt{N} \right)
\]

\[
= 3\sqrt{N}.
\]
From Theorem 3, given \((N, e)\), a thorough user can utilize the following algorithm to determine the security of the provided key pair, whether it was generated via Algorithm 1 or not. In fact, the following algorithm will factor the modulus \(N = pq\). Algorithm 2 is as follows:

**Algorithm 2** Factoring weak Murru–Saettone cryptosystem moduli for adversary

**Input:** \(e\) and \(N = pq\)

**Output:** \(p, q\)

1. Run the continued fraction method on input \(\left( \frac{e}{A} - \frac{N^{1/4}}{2A} \right)\) to obtain the list of convergents \(\frac{x_1}{y_1}, \frac{x_2}{y_2}, \ldots, \frac{x_i}{y_i}\).
2. for \(1 \leq j \leq i\) do
3. Compute \(\zeta = ex_j - Ay_j + \psi_L\)
4. Computing \(S = \frac{1}{2} \left( \sqrt{(N + 1)^2 + 4(\zeta - (N^2 - N + 1))} - (N + 1) \right)\).
5. Find the two roots \(\hat{p}\) and \(\hat{q}\) by computing \(\hat{p} = \frac{1}{2} \left( S + \sqrt{S^2 - 4N} \right), \hat{q} = \frac{1}{2} \left( S - \sqrt{S^2 - 4N} \right)\).
6. if \(\frac{N}{\hat{p}}\) and \(\frac{N}{\hat{q}}\) is true then
7. return \((p = \hat{p}, q = \hat{q})\)
8. end if
9. end for
10. return \(\bot\)

The following is an example to illustrate Algorithm 2 for the case \(|Z - \psi| < \frac{p-q}{p+q}N^{1/4}\).

**Example 1.** We use 512-bits for modulus, \(N\) in this example. Specifically, an adversary is given

\[
N = 10474822604491897001733857277814570107822699106377787693425264554973361 \\
584584775463402422003323750703377331670427702899085519959211457360525 \\
1725921749487
\]

and

\[
e = 10769431345193232115549076564111889013279606438307747171785365502043223 \\
36983784754825450826076878953980291147535145118648508441400064293496014 \\
28037987577469755126079846620517207129565398016054178944122529342040600 \\
7995190210412777884589008136819196598990016792544117030228778670332199 \\
66688065360189864914067
\]

Then the adversary can compute the following parameters

\[
\psi_L = \left( \frac{N + \sqrt{N} + 1}{2} \right)^2 = 1097219085955744084144523347183869176710441989204148244265443157694326 \\
55090566006849331271968597124151449472369065606717076270695558973543340 \\
16399157992733129579088656285475377267416478695792386746053861066215 \\
1400535769028419218726002600785194693106806210105341266365825588084065 \\
487680210438025701139156;
\]
\[ \psi_U = \left( N + \frac{3}{4} \sqrt{2N} + 1 \right)^2 + \frac{3}{8}N \]
\[ = 1097219085955744084814452334718386917617044198204148242265443157694326 \\
55090597307478970371992316073205293629546536981622305227485167239321394 \\
389875116576799498313944890616229320981978881109107670226375226298967 \\
3856721732181434233548331851018257283060212388804238053825134923510675 \\
244601422078279861895276; \]
\[ A = \psi_L + \psi_U \]
\[ = 21944381719114881696289046694367783852340883978408296488530886315388653 \\
1018119331432830164396091319735674310187260258833931498107261264734 \\
55386669650413062789303354690169830936561253598048869089302429087365182 \\
52572575012098326420824334451803451976167018598909579320190960511594740 \\
7320403526458536873214822. \]

Using values of e, N and A, the adversary obtains the continued fraction expansion of \( \left( \frac{\xi}{A} - \frac{N^{1/4}}{2A} \right) \) which are
\[ \left[ 0, 1 \frac{1}{203}, 1 \frac{1}{204}, 4 \frac{1}{2649}, 13 \frac{17}{3464}, 64 \frac{81}{16505}, \cdots, 990529 \frac{201835601}{990529}, \cdots \right]. \]

Our algorithm stops at the 13th convergent \( \frac{\xi}{A} = \frac{990529}{201835601} \). Taking \( \frac{\xi}{A} = \frac{990529}{201835601} \), the adversary computes
\[ \zeta = e\xi_{13} - Ay_{13} + \psi_L \]
\[ = 557460807135244165547799143626693721783133782656715404009612529043 \\
939490085347880762347196536169393312904395683940461765091274051490 \\
4922129571135704857702475014481507126817419400466534386062373124882 \\
4598157616580496588587832162854352674873234776657314273075277460 \\
6903898920349753769291344577179649895178. \]

Using value of \( \zeta \), the adversary solves the Equations (5) and (4) to get S, p and q respectively.
\[ S = 2049497836294941654108617224665940730419279999375266179741638258140388 \\
0052072; \]
\[ p = 10760137676568779991090044679907911735120737664989630437784142392233347 \\
8553733; \]

and
\[ q = 97348406863086356499961275667514955690720623287630313596322401259070401 \\
498339. \]

5. Generating Weak Murru–Saettone Cryptosystem Public Keys by RCA: Case \( |Z - \psi| < N \)

In this section, we show that the condition \( |Z - \psi| < \frac{e - q}{p + q} N^{1/4} \) in the previous section can be extended to \( |Z - \psi| < N \).
Lemma 3. Let $N = pq$ with $q < p < 2q$. Let $e$ satisfies the equation $eX - AY = Z - \psi_L$ where $X$ and $Y$ are positive integers. If

$$1 \leq Y < X < \frac{A}{2(\psi - \psi_L)}$$

and $|Z - \psi| < N$ then $\frac{X}{Y}$ is a convergent function of $e - \frac{N}{2A}$.

Proof. Consider the following equation

$$eX - AY = Z - \psi_L. \tag{8}$$

Let $|Z - \psi| < N$. Then, divide (8) by $AX$, we obtain

$$\left| \frac{e}{A} \right| < \left| \frac{Z - \psi_L}{AX} \right| \leq \frac{N + \psi - \psi_L}{AX} \leq \frac{AX}{2} + \frac{\psi - \psi_L}{AX} \leq \frac{N}{2A} + \frac{\psi - \psi_L}{AX} \tag{9}$$

since $p - q < 2\sqrt{N}$, $p + q > 2\sqrt{N}$ and $X > 1$. If $X < \left| \frac{A}{2(\psi - \psi_L)} \right|$, then $\frac{1}{2X} > \left| \frac{2(\psi - \psi_L)}{A} \right|$. As $AX$ will always be a positive value, rearranging (9), we obtain

$$\left| \left( \frac{e}{A} - \frac{N}{2A} \right) - \frac{Y}{X} \right| < \left| \frac{\psi - \psi_L}{AX} \right| \leq \frac{1}{2X^2}$$

which satisfies Theorem 1. This terminates the proof. \hfill \Box

Theorem 3. Let $N = pq$ with $q < p < 2q$. Let $e$ satisfies the equation $eX - AY = Z - \psi_L$ where $X$, $Y$ are positive integers. If

- $1 \leq Y < X < \left| \frac{A}{2(\psi - \psi_L)} \right|
- \psi + N < N^2 + 8N + 3\sqrt{NN} + 3\sqrt{N} + 1
- |Z - \psi| < N$

then $N$ can be factored in polynomial time.

Proof. Suppose $e$ satisfies an equation $eX - AY = Z - \psi_L$. Let $X$, $Y$ and $Z$ satisfy the conditions in Lemma 3, then we can find the values of $X$ and $Y$ by computing $\frac{X}{Y} - \frac{N}{2A}$. From the values of $X$ and $Y$, we can have the value of $Z$ by computing $Z = eX - AY + \psi_L$. From the values of $Z$, we define Equation (5) as

$$S = \frac{1}{2} \left( \sqrt{(N + 1)^2 + 4(Z - (N^2 - N + 1))} - (N + 1) \right).$$
Since, $\psi + N < N^2 + 8N + 3\sqrt{NN} + 3\sqrt{N} + 1$ then
\[
S = \frac{1}{2} \left( \sqrt{(N + 1)^2 + 4(Z - (N^2 - N + 1))} - (N + 1) \right)
\leq \frac{1}{2} \left( \sqrt{(N + 1)^2 + 4\left( (N^2 + 8N + 3\sqrt{NN} + 3\sqrt{N} + 1) - (N^2 - N + 1) \right)} - (N + 1) \right)
\leq \frac{1}{2} \left( \sqrt{N^2 + 2N + 1 + 36N + 12\sqrt{NN} + 12\sqrt{N} - (N + 1)} \right)
\leq \frac{1}{2} \left( \sqrt{(N + 1 + 6\sqrt{N})^2} - (N + 1) \right)
\leq \frac{1}{2} \left( (N + 1) + 6\sqrt{N} - (N + 1) \right)
\leq \frac{1}{2} \left( 6\sqrt{N} \right)
= 3\sqrt{N}.
\]

Based on Proposition 1, we can factor $N$ in polynomial time. \qed

**Remark 2.** A RCA can build an algorithm that produces such weak public keys by using Algorithm 1 by changing step 6 and 7 instead of

\[
Z_L = \left\lfloor \psi - \frac{p - q}{p + q} N^{1/4} \right\rfloor \quad \text{to be } \quad Z_L = \psi - N
\]

and

\[
Z_U = \left\lceil \psi + \frac{p - q}{p + q} N^{1/4} \right\rceil \quad \text{to be } \quad Z_U = \psi + N
\]

respectively.

The following is an example to illustrate Algorithm 2 for the case $|Z - \psi| < N$.

**Example 2.** We use 512-bits for modulus, $N$ in this example. Specifically, an adversary is given
\[
N = 9099889189985602168085367893162619329958419488034971810965711742895590
7774100415809039409348571858260497344724878561601849467626260439789077
252741730547
\]
and
\[
e = 15387369231796195738270992845728344585898863892978423209867961015301962
4647224858360385843285862859500857363812725002682339828686015519248969
636801841704352829289484001700028279134662306718807531327694445559522168
84664833658348512658325929687042827403376132263722135766423596683016053
1518452792490127534307
\]
Then the adversary can compute the following parameters

\[
\psi_L = (N + \sqrt{N} + 1)^2 = 82807978338112784826780485020381417521129159135920594979482820416390407 \\
235134246315679287447583303676417359380920320842844589622981261601877 \\
6172314455763876929997101097916884883032041278367854644800805874441479 \\
18688097702791322474704887700856055822473759466601003234855838299076770 \\
683825614980799914083673;
\]

\[
\psi_U = (N + \frac{3}{4} \sqrt{2N} + 1)^2 + \frac{3}{8} N = 82807978338112784826780485020381417521129159135920594979482820416390407 \\
23513435164597038913347127453285470152597341975735352828212397829422636 \\
39341490139659551164180227994657123576942524448711206060944024048587573 \\
3170304535879273992579527103381777720156105924631432140051008685419014 \\
861113526695021736842632;
\]

\[
A = \psi_L + \psi_U = 165615956676225569653560907040762835042258381287184118995896546083278081 \\
447026859797753831878782570578209272706906893740600198117904221045102451 \\
401064364697298320464151238978325972470265657270796070489520823092095 \\
2503911430615840624005001048042378335426298653912351263749068498449578 \\
554493914167582165092696.
\]

Using values of e, N and A, the adversary obtain the continued fraction expansion of \(\frac{A - N}{A^2}\) which are

\[
[0, 1076, 3229, 13992, 17221, 31213, 48434, 181685, \ldots, 149512, 160921419, \ldots]
\]

Our algorithm stops at the 15th convergent \(\frac{\xi_{15}}{\eta_{15}} = 149512 \div 160921419\). Taking \(\frac{\xi_{15}}{\eta_{15}} = 149512 \div 160921419\), the adversary computes

\[
\zeta = e \xi_{15} - A \eta_{15} + \psi_L = 82807978338112784826780485020381417521129159135920594979482820416390407 \\
4072351342563599343952356385582480725166846394319581596275257230 \\
3632018218353221404022231036420777232659973150835293152204280391789 \\
57249458966734366000113779068154844089550989060700323801509035475 \\
8989840453283514219334557078991720354078.
\]

Using value of \(\zeta\), the adversary solve the Equations (5) and (4) to get \(S, p\) and \(q\) respectively.

\[
S = 19188870757973671053726455398280471509352628848967903121245052936330134 \\
1353108;
\]

\[
p = 106212270090504332401071865550320491034358692446050781657596777445866056 \\
0181091;
\]

and

\[
q = 856764374892323781361926884324842240591675960436282495548275490460781 \\
172017.
\]
Remark 3. The above examples uses two random prime numbers with \(|p - q| \approx N^{0.49}\) and \(e \approx N^2\). By using the values of \(p\) and \(q\) in the examples, the adversary can easily compute the private exponent \(d \approx N^2\). Therefore, based on the examples, it is difficult for the user to identify that the rogue digital certificate because all the public and private parameters generated satisfy the conditions imposed during the key generation process.

6. Conclusions

We have constructed novel strategies to identify whether the Murru–Saettone RSA variant cryptosystem key pair was generated by a potential RCA. Based on our findings, if the following condition of \(|Z - \psi| < \frac{p - q}{p + q} N^{1/4}\) or \(|Z - \psi| < N\) where \(Z\) is an approximation of \(\psi\) satisfies, then Murru–Saettone RSA variant cryptosystem is vulnerable to an attack. An adversary will be able to successfully execute an attack in polynomial time by using continued fractions algorithm to factor the modulus \(N\) without having any information of the private keys upon the public key pair. Furthermore, by factoring modulus \(N\), an adversary will be able to compute the value of \(\psi = (p^2 + p + 1)(q^2 + q + 1)\) and, finally, acquire the private key, \(d \equiv e^{-1} \mod \psi\).

Author Contributions: Conceptualization, Z.M. and M.R.K.A.; formal analysis, Z.M.; funding acquisition, Z.M.; investigation, Z.M.; methodology, Z.M. and M.R.K.A.; software, Z.M.; supervision, M.R.K.A. and A.H.A.G.; validation, Z.M., M.R.K.A., A.H.A.G. and N.R.S.; writing—original draft, Z.M.; writing—review & editing, Z.M., M.R.K.A., A.H.A.G. and N.R.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Universiti Putra Malaysia under Putra Grant with project number GP-IPM/2021/9699900.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Rivest, R.L.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Commun. ACM 1978, 21, 120–126. [CrossRef]
2. Wiener, M. Cryptanalysis of Short RSA Secret Exponents. IEEE Trans. Inf. Theory 1990, 36, 553–558. [CrossRef]
3. Bunder, M.; Tonien, J. A new improved attack on RSA. In Proceedings of the 5th International Cryptology and Information Security Conference 2016, pp. 101–110.
4. Susilo, W.; Tonien, J.; Yang, G. A generalised bound for the Wiener attack on RSA. J. Inf. Secur. Appl. 2020, 53, 102531. [CrossRef]
5. Boneh, D.; Durfee, G. Cryptanalysis of RSA with private key \(d\) less than \(N^{0.292}\). IEEE Trans. Inf. Theory 2000, 46, 1339–1349. [CrossRef]
6. Herrmann, M.; May, A. Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA. In Proceedings of the Public Key Cryptography—PKC 2010, Paris, France, 26–28 May 2010; Eds.; Springer: Berlin/Heidelberg, Germany, 2010; pp. 53–69.
7. Takagi, T. Fast RSA-type cryptosystem modulo \(pq\). In Proceedings of the Advances in Cryptology—CRYPTO’98, Santa Barbara, CA, USA, 23–27 August 1998; Krawczyk, H., Ed.; Springer: Berlin/Heidelberg, Germany, 1998; pp. 318–326.
8. Quisquater, J.J.; Couvreur, C. Fast decipherment algorithm for RSA public-key cryptosystem. Electron. Lett. 1982, 18, 905–907. [CrossRef]
9. Ashullah, M.A.; Kamel Ariffin, M.R.; Mahad, Z.; Daud, M.A. (In)security of the cryptosystem for transmitting large data. In Proceedings of the ICSCA’19: The 2019 8th International Conference on Software and Computer Applications, Penang, Malaysia, 19–21 February 2019; Volume Part F147956, pp. 91–94. [CrossRef]
10. Mahad, Z.; Ashullah, M.; Ariffin, M. Efficient methods to overcome rabin cryptosystem decryption failure. Malays. J. Math. Sci. 2017, 11, 9–20.
11. Ariffin, M.; Ashullah, M.; Abu, N.; Mahad, Z. A new efficient asymmetric cryptosystem based on the integer factorization problem of \(N = pq\). Malays. J. Math. Sci. 2013, 7, 19–37.
12. Elkamchouchi, H.; Elshenawy, K.; Shaban, H. Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers. In Proceedings of the The 8th International Conference on Communication Systems, Singapore, 28 November 2002; pp. 91–95. [CrossRef]
13. Dong, Z.; Kane, K.; Camp, L.J. Detection of Rogue Certificates from Trusted Certificate Authorities Using Deep Neural Networks. ACM Trans. Priv. Secur. 2016, 19, 1–31. [CrossRef]

14. Murru, N.; Saettone, F.M. A Novel RSA-Like Cryptosystem Based on a Generalization of the Rédei Rational Functions. In Proceedings of the Number-Theoretic Methods in Cryptology, Warsaw, Poland, 11–13 September 2018; Kaczorowski, J., Pieprzyk, J., Pomykała, J., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 91–103.

15. Nitaj, A. Another Generalization of Wiener’s Attack on RSA. In Proceedings of the Progress in Cryptology—AFRICACRYPT 2008, Casablanca, Morocco, 11–14 June 2008; Vaudenay, S., Ed.; Springer: Berlin/Heidelberg, Germany, 2008; pp. 174–190.

16. Nitaj, A.; Ariffin, M.R.B.K.; Adenan, N.N.H.; Abu, N.A. Classical Attacks on a Variant of the RSA Cryptosystem. In Proceedings of the Progress in Cryptology—LATINCRYPT 2021, Bogotá, Colombia, 6–8 October 2021; Longa, P., Ràfols, C., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 151–167.