IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 16, 2022, accepted May 6, 2022, date of publication May 16, 2022, date of current version May 24, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3175519

Security Issues of Novel RSA Variant

ABDERRAHMANE NITAJ[1], MUHAMMAD REZAL BIN KAMEL ARIFFIN[2], NURUL NUR HANISAH ADENAN[2], TERRY SHUE CHIEN LAU[2], AND JIAHUI CHEN[3], (Member, IEEE)

[1]LMNO, CNRS, University of Caen Normandy (UNICAEN), 14000 Caen, France
[2]Institute for Mathematical Research, Universiti Putra Malaysia, Serdang, Selangor 43400, Malaysia
[3]School of Computers, Guangdong University of Technology, Guangzhou 510006, China

Corresponding author: Muhammad Rezal Bin Kamel Ariffin (rezal@upm.edu.my)

This work was supported in part by the Guangzhou Basic and Applied Basic Research Foundation under Grant 202102020928.

ABSTRACT The RSA is one of the current default cryptosystems that provides security with applications such as encryptions and digital signatures. It is important to further study the weak characteristics of the RSA to ensure correct utilisation in order not to be susceptible to adversaries. In this paper, we give detailed analysis on security of the Murru-Saettone variant of the RSA cryptosystem that utilised a cubic Pell $ed - k\left(p^2+p+1\right)\left(q^2+q+1\right) = 1$ as key equation and $N = pq$ as RSA modulus. We propose some attacks on this variant when the prime difference $|p-q|$ is small. Our first approach is to utilise the continued fractions algorithm to determine the parameter d which enables us to determine the secret p and q. Our second approach considers the Coppersmith's method and lattice basis reduction to factor the modulus N. Our attacks improve recent cryptanalyses on the cubic Pell equation variant of RSA. Furthermore, our attacks prove that under small prime difference scenario, the number of susceptible private exponents for the cubic Pell equation variant of RSA is much larger than the standard RSA.

INDEX TERMS Continued fractions, Coppersmith's method, cubic Pell equation, factorization, RSA.

I. INTRODUCTION

The existence of cryptography becomes essential aligning to the demands of using the digital platform to transmit the data. Prior to the 70's, the data was relayed via symmetric cryptography. However, the designated cryptography was no longer effective as the number of users escalated significantly. The problem arose led to the development of asymmetric cryptography namely the RSA [15]. By employing different encryption key and decryption key, the RSA designed by Rivest, Shamir and Adleman publicised the key pair (N, e) purposely for encryption and at the same time ensure (N, d) private as they are needed to decrypt the data safely. To this day, RSA has been worldwidely implemented in various applications such as smart-cards, e-commerce, email and remote login session as it guarantees security of the user's information.

One main features of the RSA is the modulus $N = pq$ which p and q are large primes satisfying $q < p < 2q$. Let $\phi(N) = (p-1)(q-1)$ be the Euler totient function. Suppose that e and d are designated as public and private RSA parameters satisfying the equation $ed \equiv 1 \pmod{\phi(N)}$. An ingenious element of this cryptosystem is that the message is encrypted and decrypted using modular equation. That is, for encryption, the sender is required to compute $C \equiv M^e \pmod{N}$ where C is the ciphertext and M is the original message or plaintext. Since d is the multiplicative inverse of e, thus one simply requires to compute $M \equiv C^d \pmod{N}$. However, the task of decryption would not be possible if one does not have the value d. Futhermore, the values of $p, q, \phi(N)$ are also kept private. Hence, it makes the cryptosystem secure from attacks.

Since its invention, RSA has been widely used for encryption and has been intensively studied for vulnerabilities [5]. There are attempts on factoring the modulus $N = pq$ by studying its features and the methods that are applicable to factor it. In fact, the study in [7] showed that the 768-bit RSA modulus is insecure to be utilised as it can be factored by using number field sieve factoring method. Meanwhile, the work in [11] studied the method of semi-prime factorization and showed that their method managed to factor the RSA modulus from [7]. Other than that, the usage of small d may also lead to vulnerability although it helps to improve its efficiency. Wiener [19] presented a method, based on the

The associate editor coordinating the review of this manuscript and approving it for publication was Junggab Son.

continued fractions algorithm, to factor N when $d < \frac{1}{3}N^{\frac{1}{4}}$. By implementing the Coppersmith's technique [3] and lattice reduction methods [9], there is a more recent improvement of the bound to $d < N^{0.292}$ [2].

Application of variants of RSA is another endeavour made by the researchers to increase its efficiency. For instance, Takagi [17] utilised multi-power RSA $N = p^r q$ and proved that it can shorten the execution time for decryption process provided the Chinese Remainder Theorem and Hensel Lifting lemma are used. Note that, [17] only consider the case when r is small. Incited by the advantage of this new finding, few more studies have been made upon this matter. [10] and [16] managed to find the weakness of using this variant. They showed that this cryptosystem is vulnerable to attacks if certain conditions are satisfied. Their attacks are workable on large values of r. Later, Murru and Saettone [12] constructed a new RSA variant based on the cubic Pell equation $x^3+ry^3+r^2z^3-3rxyz = 1$ modulo an RSA modulus $N = pq$. Both e and d satisfy the following equation,

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

For the proposed scheme, its security is being examined in [12]. In [14], Nitaj *et al.* presented a cryptanalysis of the scheme by considering the continued fractions and the Coppersmith's method. In particular, an adversary can break the system if $d = N^{\delta}$ such that $\delta < \frac{7}{3} - \frac{2}{3}\sqrt{3\alpha+1}$ where $e = N^{\alpha}$. For $e \approx N^2$, that is $\alpha \approx 2$, the former bound reduces to $\delta < \frac{7}{3} - \frac{2}{3}\sqrt{7} \approx 0.569$. In [20], Zheng *et al.* presented another cryptanalysis of the scheme and gained a better bound for δ, namely $\delta < 2-\sqrt{2} \approx 0.585$. Hence, these recent works arose the following questions:

1) Based on Murru-Saettone scheme, is there any feature of the primes p and q that could lead to factorization?
2) What is the size of d that is safe from attack?

OUR CONTRIBUTION

In order to answer the questions above, we push further the cryptanalysis of the Murru-Saettone scheme by considering a specific RSA modulus $N = pq$, which p and q are two prime factors which have their most significant bits of the same structure. This implies the prime difference $|p-q|$ is much smaller than the ordinary case where $|p-q| \approx N^{\frac{1}{2}}$. By considering $e = N^{\alpha}$, $|p-q| = N^{\beta}$ and $d = N^{\delta}$, we show that one can extend the methods in [14] to improve the bounds on δ. Typically, using the continued fraction method, we show that the scheme is vulnerable if

$$\delta < \frac{7}{4} - \frac{1}{2}\alpha - \beta. \tag{2}$$

Similarly, we apply the Coppersmith's method and show that the scheme is vulnerable if

$$\delta < \frac{5}{3} + \frac{4}{3}\beta - \frac{2}{3}\sqrt{(4\beta-1)(3\alpha+4\beta-1)}. \tag{3}$$

For $\beta = \frac{1}{2}$, we get the bounds as in [14]. This shows that our new cryptanalysis is an extension of the method of [14] and gives better bounds.

This following is the organization for this paper. Section II gives the preliminaries required for subsequent sections. Various results are presented in Section III to ease the understanding of Sections IV and V. In Section IV, we detail our approach based on the continued fractions algorithm. In Section V, we describe our approach based on the Coppersmith's method and lattice reduction techniques. We conclude the paper in Section VI.

II. PRELIMINARIES

We give brief description on the continued fractions, lattices, Coppersmith's method and the Murru and Saettone scheme [12] in this section.

A. CONTINUED FRACTIONS

The expression of continued fractions expansion of $\xi \in \mathbb{R}$ can be written in these forms

$$\xi = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\cdots + \cfrac{1}{a_\mu}}}}} \tag{4}$$

which can also be written as $\xi = [a_0, a_1, \cdots, a_\mu, \cdots]$. If ξ is a rational number, then $\xi = [a_0, a_1, \cdots, a_\mu]$ and we can perform the continued fractions expansion algorithm in polynomial time. The convergents $\frac{r}{s}$ of ξ are the fractions denoted by $\frac{r}{s} = [a_0, a_1, \cdots, a_i]$ for $i \geq 0$. The following theorem is a useful result on continued fractions which is important in our attack.

Theorem 1: Let $\xi > 0$. Suppose that $\gcd(s, r) = 1$ and

$$\left|\xi - \frac{r}{s}\right| < \frac{1}{2s^2}. \tag{5}$$

Then $\frac{r}{s}$ is a convergent of the continued fractions expansion of ξ.

B. LATTICES

Let $\omega \leq n$ be an integer. Consider $l_1, \ldots, l_\omega \in \mathbb{R}^n$ such that they are linearly independent. We call the set of all integer linear combinations of the vectors v_i as the lattice $\mathcal{L}$ spanned by $\{l_1, \ldots, l_\omega\}$, i.e.

$$\mathcal{L} = \left\{ \sum_{i=1}^{\omega} x_i l_i,\ x_i \in \mathbb{Z} \right\}. \tag{6}$$

The set $\{l_1, \ldots, l_\omega\}$ is the basis of lattice $\mathcal{L}$ as it is used to generate $\mathcal{L}$. To find the lattice dimension, one simply needs to count the number of basis of $\mathcal{L}$. In our case, the lattice $\mathcal{L}$ has dimension $\dim(\mathcal{L}) = \omega$, and $\mathcal{L}$ is offull ranked when $\omega = n$. In 1982, Lenstra *et al.* [9] invented a very useful tool known as the LLL algorithm to determine the shortest basis vector that generates a lattice. The following theorem presents the results on LLL reduced basis vectors.

Theorem 2 (LLL [9]): Let $\{l_1, \ldots, l_\omega\}$ be a basis of a lattice $\mathcal{L}$. The LLL algorithm outputs a new basis $\{b_1, \ldots, b_\omega\}$ of L such that

$$\|b_1\| \leq \ldots \leq \|b_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\mathcal{L})^{\frac{1}{\omega+1-i}}, \tag{7}$$

for $1 \leq i \leq \omega$.

C. THE COPPERSMITH's METHOD

Suppose that we know how to factorize the modulus into its factors, then the solutions of a modular equation can be determined easily [4]. However, there are situations which we do not have any information on factorizing the modulus, thus finding the solutions can be difficult. Coppersmith [3] contributed on solving this problem by proposing a way to determine the small solutions of modular polynomial specifically for a univariate case and heuristically for a multivariate case. There are two important tools required in the Coppersmith's method: the LLL algorithm and the following result reformulated in [6].

Theorem 3 (Howgrave-Graham): *Let $h(x, y) = \sum a_{ij}x^i y^j$ be a polynomial over integers with at most ω monomials. The norm of $f(x, y)$ is defined by $\|h(x, y)\| = \sqrt{\sum a_{ij}^2}$. If $|x_0| < X$, $|y_0| < Y$, and*

$$h(x_0, y_0) \equiv 0 \pmod{e^m}, \quad \|h(xX, yY)\| < \frac{e^m}{\sqrt{\omega}}, \tag{8}$$

then $h(x_0, y_0) = 0$ is true over the integers.

D. THE MURRU-SAETTONE SCHEME

Murru and Saettone [12] designed a scheme using cubic Pell equation

$$x^3 + ry^3 + r^2z^3 - 3xyzr = 1, \tag{9}$$

where r is not a cube of an integer.

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

$$\begin{aligned}(x_1, y_1, z_1) \bullet (x_2, y_2, z_2) = (&x_1x_2 + (y_2z_1 + y_1z_2)r,\\ &x_2y_1 + x_1y_2 + rz_1z_2,\\ &y_1y_2 + x_2z_1 + x_1z_2).\end{aligned} \tag{10}$$

Next, consider the set

$$\mathcal{A} = \{(x, y, z) \in \mathbb{G}^3,\ x^3 + ry^3 + r^2z^3 - 3xyzr = 1\}. \tag{11}$$

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 $\boxplus$ defined by the following cases:

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

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

$$(m, n)^{\boxplus k} = (m, n) \boxplus (m, n) \boxplus \ldots (m, n), \quad (k \text{ times}). \tag{12}$$

Consequently, we can reduce B to

$$B = (\mathbb{G} \times \mathbb{G}) \cup (\mathbb{G} \times \{\alpha\}) \cup \{(\alpha, \alpha)\}. \tag{13}$$

Let p be a prime. If we take $\mathbb{G} = \mathbb{Z}/p\mathbb{Z}$, then one can choose $\alpha = \infty$. n 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 $(m, n)^{\boxplus p^2+p+1} = (\alpha, \alpha) \pmod{p}$ for all $(m, n) \in B$. The RSA cryptosystem variant presented in [12] is based on the former observations. Their construction of algorithms are presented as follows.

Algorithm 1 Key Generation

Input: n, the modulus N bit-size.
Output: A public key (e, N, r) and a private key (d, p, q).

1. Choose prime integers p and q.
2. Compute $N = pq$.
3. Choose an integer r such that it is not a cube integer and not a cubic modulo p, q, and N.
4. Choose an integer $e \in \mathbb{Z}$ satisfying
   $$\gcd(e, (p^2 + p + 1)(q^2 + q + 1)) = 1.$$
5. Compute the multiplicative inverse d satisfying:
   $$ed \equiv 1 \pmod{(p^2 + p + 1)(q^2 + q + 1)}.$$
6. Output the public key (e, N, r) and the private key (d, p, q).

Algorithm 2 Encryption

Input: A pair of messages $M_1, M_2 \in \mathbb{Z}_N$.
Output: The ciphertext (C_1, C_2).

1. Compute $(C_1, C_2) \equiv (M_1, M_2)^{\boxplus e} \pmod{N}$ using the addition operation $\boxplus$.
2. Output the ciphertext (C_1, C_2).

Algorithm 3 Decryption

Input: Ciphertext (C_1, C_2).
Output: Messages M_1, M_2.

1. Compute $(M_1, M_2) \equiv (C_1, C_2)^{\boxplus d} \pmod N$ using the addition operation $\boxplus$.
2. Output the messages (M_1, M_2).

III. USEFUL LEMMAS

Consider an RSA module $N = pq$ with $q < p < 2q$. Let $\Delta = |p - q|$. The next statement describes a relationship between p, q, N and Δ [18].

Lemma 1: If $N = pq$, then

$$0 < 4(p+q)\sqrt{N} - 8N < \Delta^2. \tag{14}$$

If $\Delta < 2N^{\frac{1}{4}}$, then $p+q = \left\lceil 2\sqrt{N} \right\rceil$. Since $N = pq$, we can substitute $N = pq$ into the previous statement and determine p and q. As a consequence, we make the assumption that $\Delta > 2N^{\frac{1}{4}}$ throughout this paper.

The following describes some bounds for p and q in relation to the term N (See [13]).

Lemma 2: Suppose that p and q are unknown integers satisfying $q < p < 2q$. Consider $N = pq$, then

$$2\sqrt{N} < p + q < 3\sqrt{N}. \tag{15}$$

By applying Lemma 2, we can estimate the value of $\psi(N)$, where $\psi(N) = \left(p^2 + p + 1\right)\left(q^2 + q + 1\right)$.

Proposition 1: Suppose that p and q are unknown integers satisfying $q < p < 2q$. Consider $N = pq > 230$ and $\psi_0(N) = \left(N + \sqrt{N} + 1\right)^2$. Then

$$|\psi(N) - \psi_0(N)| < \frac{1}{3}\Delta^2\sqrt{N}. \tag{16}$$

Proof: We have

$$\begin{aligned}\psi(N) &= \left(p^2 + p + 1\right)\left(q^2 + q + 1\right) \\ &= (p+q)^2 + (N+1)(p+q) + N^2 - N + 1,\end{aligned} \tag{17}$$

and

$$\begin{aligned}\psi_0(N) &= \left(N + \sqrt{N} + 1\right)^2 \\ &= \left(2\sqrt{N}\right)^2 + (N+1)2\sqrt{N} + N^2 - N + 1.\end{aligned} \tag{18}$$

Then,

$$\begin{aligned}&|\psi(N) - \psi_0(N)| \\ &\quad = \left(p + q - 2\sqrt{N}\right)\left(p + q + N + 2\sqrt{N} + 1\right) \\ &\quad = \frac{(p-q)^2}{p + q + 2\sqrt{N}}\left(p + q + N + 2\sqrt{N} + 1\right).\end{aligned} \tag{19}$$

Set $|p-q| = \Delta$. By Lemma 2, we have $2\sqrt{N} < p+q < 3\sqrt{N}$. Then,

$$|\psi(N) - \psi_0(N)| < \frac{\Delta^2}{4\sqrt{N}}\left(N + 5\sqrt{N} + 1\right). \tag{20}$$

For $N \geq 231$, we have $N + 5\sqrt{N} + 1 < \frac{4}{3}N$. This implies that

$$|\psi(N) - \psi_0(N)| < \frac{1}{3}\Delta^2\sqrt{N}, \tag{21}$$

which completes the proof. □

If $\psi(N)$ is known, we can perform factorization on the modulus $N = pq$ by the following result [14].

Proposition 2: Suppose that p and q are unknown integers satisfying $q < p$. Consider $N = pq$ and suppose that $\psi(N)$ is known. Then,

$$p = \frac{1}{2}\left(S + \sqrt{S^2 - 4N}\right), \quad q = \frac{1}{2}\left(S - \sqrt{S^2 - 4N}\right), \tag{22}$$

where

$$S = \frac{1}{2}\left(\sqrt{(N+1)^2 + 4\left(\psi(N) - \left(N^2 - N + 1\right)\right)} - (N+1)\right). \tag{23}$$

IV. APPLICATION OF CONTINUED FRACTIONS

We try to estimate the values for d, so that it could be determined via the continued fractions algorithm. Then, we can determine p and q from the modulus $N = pq$.

A. OUR ATTACK ON THE SCHEME

Theorem 4: Suppose that p and q are unknown integers satisfying $q < p < 2q$ and $|p - q| = N^\beta$. Consider $N = pq$. If $ed - k\psi(N) = 1$, where $e = N^\alpha$ and $d = N^\delta$. Then, for $\frac{1}{2} + 2\beta < \alpha < \frac{7}{2} - 2\beta$, one can determine d and factor N in polynomial time if

$$\delta < \frac{7}{4} - \frac{1}{2}\alpha - \beta. \tag{24}$$

Proof: Let $N = pq$ with satisfying the conditions in the hypothesis. If $ed - k\psi(N) = 1$, then

$$\begin{aligned}\left|\frac{k}{d} - \frac{e}{\psi_0(N)}\right| &= \frac{|ed - k\psi_0(N)|}{d\psi_0(N)} \\ &\leq \frac{|ed - k\psi(N)| + k|\psi(N) - \psi_0(N)|}{d\psi_0(N)},\end{aligned} \tag{25}$$

where $ed - k\psi(N) = 1$, and $\psi_0(N) = \left(N + \sqrt{N} + 1\right)^2$. By Proposition 1, we have $|\psi(N) - \psi_0(N)| < \frac{1}{3}\Delta^2\sqrt{N}$. This implies

$$\left|\frac{k}{d} - \frac{e}{\psi_0(N)}\right| < \frac{1 + \frac{1}{3}k\Delta^2\sqrt{N}}{d\left(N + \sqrt{N} + 1\right)^2} < \frac{k}{d}\frac{1 + \frac{1}{3}\Delta^2\sqrt{N}}{\left(N + \sqrt{N} + 1\right)^2}. \tag{26}$$

Therefore, $k\psi(N) = ed - 1 < ed$, and, since $\psi(N) > p^2q^2 = N^2$, we have

$$\frac{k}{d} < \frac{e}{\psi(N)} < \frac{N^\alpha}{N^2} = N^{\alpha-2}. \tag{27}$$

Also, we have

$$\frac{1+\frac{1}{3}\Delta^2\sqrt{N}}{\left(N+\sqrt{N}+1\right)^2} < \frac{\frac{1}{2}\Delta^2\sqrt{N}}{N^2} = \frac{1}{2}\Delta^2 N^{-\frac{3}{2}} = \frac{1}{2}N^{2\beta-\frac{3}{2}}. \tag{28}$$

This leads to

$$\left|\frac{k}{d}-\frac{e}{\psi_0(N)}\right| < \frac{1}{2}N^{\alpha-2}N^{2\beta-\frac{3}{2}} = \frac{1}{2}N^{\alpha+2\beta-\frac{7}{2}}. \tag{29}$$

If $\alpha+2\beta-\frac{7}{2} < -2\delta$, that is $\delta < \frac{7}{4}-\frac{1}{2}\alpha-\beta$, then

$$\left|\frac{k}{d}-\frac{e}{\psi_0(N)}\right| < \frac{1}{2d^2}. \tag{30}$$

As a consequence, $\frac{k}{d}$ is a convergent of $\frac{e}{\psi_0(N)}$. This can be determined by applying Theorem 1. Rearranging the term $ed-k\psi(N)=1$, we have $\psi(N)=\frac{ed-1}{k}$.

Applying Proposition 2, we can use $\psi(N)$ to determine the values of p and q.

Note that since $\delta > 0$ is required, we must have

$$\frac{7}{4}-\frac{1}{2}\alpha-\beta > 0 \Leftrightarrow \frac{7}{2}-2\beta > \alpha.$$

On the other hand, we require $\alpha+\delta \geq 2$, which implies that $\alpha > \frac{1}{2}+2\beta$. □

Observe that, if $e \approx N^2$, then the method will succeed $\delta < \frac{3}{4}-\beta$. This is the same condition obtained in [18] by extending the attack of Wiener on RSA to the case with small prime difference.

B. A SMALL NUMERICAL EXAMPLE

Consider the following small public parameters

$$\begin{aligned} N &= 455814364710887971906175204247759142820681933\backslash 460576277, \quad (31)\\ &= 893186606831920047789772708237990350854341374\backslash 068031165835567391404209503553636190032305700\backslash 06480613996041199. \quad (32)\end{aligned}$$

Then $e=N^{\alpha}$ with $\alpha \approx 1.993$.

Let $\psi_0(N) = \left(N+\sqrt{N}+1\right)^2$. When applying the continued fractions algorithm to $\frac{e}{\psi_0(N)}$, we get the first 40 partial quotients

$$[0, 2, 3, 15, 11, 6, 1, 1, 1, 2, 1, 3, 4, 58, 1, 3, 4, 9, 1, 12, 1, 1, 1, 5, 2, 1, 7, 3, 45, 1, 1, 27, 1, 29, 1, 2, 7, 1, 1, 57, \ldots] \tag{33}$$

Each convergent $\frac{a}{b}$ of $\frac{e}{\psi_0(N)}$ is a candidate for the solution $\frac{k}{d}$. We only need the convergents which satisfy the condition where $\psi = \frac{eb-1}{a} \in \mathbb{Z}$. Note that the 2nd, 3rd, and 33th convergents satisfy this condition.

Next, we need the convergents so that there exists solution for the equations $\left(p^2+p+1\right)\left(q^2+q+1\right)=\psi$, $pq=N$. This can be computed by Proposition 2. Upon verification, we check that the 33th convergent $\frac{a}{b} = \frac{282741560637038515}{657693369725239904}$ fulfils the conditions. We take

$$\begin{aligned} k &= 282741560637038515,\\ d &= 657693369725239904, \end{aligned} \tag{34}$$

which gives

$$\begin{aligned} \psi(N) &= \frac{ed-1}{k}\\ &= 207766735076790394084687946009877064094115\backslash 253294447231879276540186176131855583281749\backslash 788903115749862628168293. \end{aligned} \tag{35}$$

Then, by Proposition 2, we solve the equations $pq=N$ and $\left(p^2+p+1\right)\left(q^2+q+1\right)=\psi$. We obtain

$$p = 675147604133696055740471063, \tag{36}$$

$$q = 675132907115560710964512179. \tag{37}$$

Observing that $d=N^{\delta}$ where $\delta \approx 0.332$, and $|p-q|=N^{\beta}$ where $\beta \approx 0.413$. This makes all the conditions of Theorem 4 fulfilled.

In [14], the method based on the continued fractions algorithm works when the bound $\delta < \frac{5}{4}-\frac{\alpha}{2}$ is satisfied. In our example, we have $\alpha \approx 1.993$, $\delta \approx 0.332$, and $\frac{5}{4}-\frac{\alpha}{2} \approx 0.253$. As a consequence, the bound $\delta < \frac{5}{4}-\frac{\alpha}{2}$ is not satisfied, and the method in [14] will not succeed to factor N.

C. COMPARISON WITH FORMER ATTACKS ON STANDARD RSA UNDER SAME ASSUMPTION

In this section we provide a comparison with a former attack upon the standard RSA under the same assumption that is the modulus $N=pq$ contains primes that share MSB's and that the strategy to conduct the attack is via continued fractions. As provided in Table 1, it is visible that the bound for insecure private exponent d derived from the cubic Pell equation variant of RSA is much larger than the standard version. This implies the cubic Pell equation variant of RSA has much more insecure private exponents than the standard RSA under the sharing MSB's assumption and continued fractions analysis strategy. Thus, one needs to choose the parameters carefully so that the cryptosystem is insusceptible through the communication networks.

V. APPLICATION OF THE COPPERSMITH's METHOD

Consider e and d in the Murru-Saettone scheme which satisfies the equation $ed-k\left(p^2+p+1\right)\left(q^2+q+1\right)=1$. We can transform this equation into a modular equation of the form $x(y^2+ay+b)+1 \pmod{e}$, where a and b are constants. We can apply the Coppersmith's method to determine its small solutions, and then determine the factors p and q of N. The method described here is a generalization of the method described in [14].

A. THE SMALL INVERSE PROBLEM

Theorem 5: Suppose that p and q are unknown integers satisfying $q < p < 2q$. Consider $N=pq$ and $a, b \in \mathbb{Z}^+$.

TABLE 1. The values of δ for $\alpha = \log_N e = 1$ and $\beta = 0.25, 0.33, 0.50$.

Attack	General bound for d	β	δ
Ariffin et. al [1] attack on standard RSA	$d < \frac{\sqrt{3}}{\sqrt{2}} N^{\delta}$, $\delta < \frac{3}{4} - \beta$, $\lvert b^2 p - a^2 q \rvert < N^{\beta}$; $a, b = 1$	0.25	0.500
		0.33	0.417
		0.50	0.250
Our attack on cubic Pell equation variant of RSA	$\delta < \frac{7}{4} - \frac{1}{2}\alpha - \beta$, $e = N^{\alpha}, \alpha \approx 2$, $\lvert p - q \rvert = N^{\beta}$	0.25	1.000
		0.33	0.920
		0.50	0.750

Let

$$f(x, y) = x(y^2 + ay + b) + 1. \tag{38}$$

If $f(x, y) \equiv 0 \pmod{e}$ *where* $e = N^{\alpha}$, $y < N^{\beta}$, *and* $x < N^{\gamma}$. *Then, we can determine* x *and* y *in polynomial time if* $\alpha > 2\beta$ *and*

$$3\gamma < 3\alpha - 2\sqrt{6\alpha\beta + 4\beta^2} + 2\beta. \tag{39}$$

Proof: Let $m \in \mathbb{Z}^+$. For $0 \le k \le m$, define the polynomials (see [14], Theorem 5),

$$g_{k,i,j}(x, y) = x^{i-k} y^{j-2k} f(x, y)^k e^{m-k},$$

for $2k \le j \le 2k + 1$, $k \le i \le m$; or $2k + 2 \le j \le 2i + t$, $i = k$.

Note that if $f(x, y) \equiv 0 \pmod{e}$, then $g_{k,i,j}(x, y) \equiv 0 \pmod{e^m}$. Define $\mathcal{L}$ as the lattice spanned by the coefficient vectors of the polynomials

$$\{g_{k,i,j}(xX, yY) : X, Y \in \mathbb{Z}^+.\}$$

The rows of the matrix of the lattice are formed by the polynomials $g_{k,i,j}(xX, yY, zZ)$. The rows are ordered according to the order of (i, j, k). Note that the monomials $x^i y^j$ are arranged according to the order of (i, j). This leads to a triangular matrix which has determinant

$$\det(\mathcal{L}) = X^{n_X} Y^{n_Y} e^{n_e}. \tag{40}$$

Consider $\tau \ge 0$ which we will compute the optimal value later. Let $t = \tau m$. We give some approximations for the parameters n_X, n_Y, n_e and $\omega = \dim(\mathcal{L})$ (see [14], Theorem 5),

$$\begin{aligned} n_X &= \frac{1}{6}(3\tau + 4)m^3 + o(m^3), \\ n_Y &= \frac{1}{6}\left(3\tau^2 + 6\tau + 4\right)m^3 + o(m^3), \\ n_e &= \frac{1}{6}(3\tau + 4)m^3 + o(m^3), \\ \omega &= (\tau + 1)m^2 + o(m^2). \end{aligned} \tag{41}$$

Assume that

$$2^{\frac{\omega}{4}} \det(\mathcal{L})^{\frac{1}{\omega - 1}} < \frac{e^m}{\sqrt{\omega}}, \tag{42}$$

we have

$$\det(\mathcal{L}) < \frac{2^{-\frac{\omega(\omega-1)}{4}}}{\left(\sqrt{\omega}\right)^{\omega-1}} e^{m(\omega-1)}. \tag{43}$$

Then, using (40), we get

$$e^{n_e - m\omega} X^{n_X} Y^{n_Y} < \frac{2^{-\frac{\omega(\omega-1)}{4}}}{\left(\sqrt{\omega}\right)^{\omega-1}} e^{-m}. \tag{44}$$

Assume that $x < X = N^{\gamma}$, $y < Y = N^{\beta}$, and $e = N^{\alpha}$. Substituting (41) into (44), we get

$$6\beta\tau^2 + 6(2\beta + \gamma - \alpha)\tau + 4(2\beta + 2\gamma - \alpha) < -\varepsilon_1, \tag{45}$$

where $\varepsilon_1 > 0$ is a small value depending on m and N.

On the left side, the optimal value is $\tau = \frac{\alpha - 2\beta - \gamma}{2\beta}$. We have

$$-3\gamma^2 + 2(3\alpha + 2\beta)\gamma - 3\alpha^2 + 4\alpha\beta + 4\beta^2 < -\varepsilon_2, \tag{46}$$

where $\varepsilon_2 = 2\beta\varepsilon_1$. Solving the equation, we get the condition

$$\gamma < \alpha + \frac{1}{3}\left(2\beta - 2\sqrt{6\alpha\beta + 4\beta^2}\right).$$

Also, the optimal value τ should be positive, that is $\gamma \le \alpha - 2\beta$. Then, for $\alpha > 2\beta$, we get

$$\begin{aligned} \gamma &< \min\left(\alpha - 2\beta, \alpha + \frac{2}{3}\beta - \frac{2}{3}\sqrt{6\alpha\beta + 4\beta^2}\right) \\ &\Rightarrow 3\gamma < 3\alpha - 2\sqrt{6\alpha\beta + 4\beta^2} + 2\beta. \end{aligned} \tag{47}$$

From the reduced basis, we consider two polynomials $h_1(x, y)$ and $h_2(x, y)$ which satisfy

$$h_1(x, y) = h_2(x, y) = 0. \tag{48}$$

If both $h_1(x, y)$ and $h_2(x, y)$ are independent algebraically, then we can consider the Gröbner basis method to solve for (x, y). □

B. THE ATTACK WITH SMALL PRIME DIFFERENCE AND SMALL d

In this section, we consider the attack on the Murru-Saettone variant of the RSA in [12]. For $N = pq$, we assume that the value of $|p - q|$ is small.

Theorem 6: Suppose that p *and* q *are unknown integers satisfying* $q < p < 2q$ *and* $|p - q| = N^{\beta}$. *Consider* $N = pq$. *Suppose that* $ed - k\psi(N) = 1$ *with* $e = N^{\alpha}$ *and* $d = N^{\delta}$. *Then, we can determine* d *and compute* p *and* q *in polynomial time if* $\alpha > 2\beta$, *and*

$$\delta < \frac{1}{3}\left(5 + 4\beta - 2\sqrt{(4\beta - 1)(3\alpha + 4\beta - 1)}\right). \tag{49}$$

Proof: Let e be a public parameter of the RSA variant satisfying $ed - k\psi(N) = 1$. Let $M = \left\lfloor \sqrt{N} \right\rfloor$. A straightforward calculation shows that

$$\begin{aligned} \psi(N) = (p + q - 2M)^2 + (N + 4M + 1)(p + q - 2M) \\ + N^2 + 4M^2 + 2MN + 2M - N + 1. \end{aligned} \tag{50}$$

We set $x_0 = k$, $y_0 = p + q - 2M$, $a = N + 4M + 1$, and $b = N^2 + 4M^2 + 2MN + 2M - N + 1$.

We can now rewrite $ed - k\psi(N) = 1$ as a modular equation,

$$x_0(y_0^2 + ay_0 + b) + 1 \equiv 0 \pmod{e}.$$

Now, considering the polynomial $f(x, y)$ as in (38) . Then $f(x_0, y_0) \equiv 0 \pmod{e}$, and the small solutions can be computed by applying Theorem 5.

Assume that $|p - q| = N^\beta$, $e = N^\alpha$, and $d < N^\delta$. By Lemma 1, we have $y_0 = p + q - 2M < N^{2\beta - \frac{1}{2}}$. We set $Y = N^{2\beta - \frac{1}{2}}$. On the other hand, since $\psi(N) > p^2q^2 = N^2$, we obtain

$$x_0 = k = \frac{ed - 1}{\psi(N)} < N^{\alpha + \delta - 2}. \tag{51}$$

We set $X = N^{\alpha+\delta-2}$. Then, by Theorem 5, the condition to find the small solutions is

$$\gamma < \alpha + \frac{2}{3}\left(2\beta - \frac{1}{2}\right) - \frac{2}{3}\sqrt{6\alpha\left(2\beta - \frac{1}{2}\right) + 4\left(2\beta - \frac{1}{2}\right)^2}, \tag{52}$$

where $\gamma = \alpha + \delta - 2$. This implies

$$\delta < \frac{5}{3} + \frac{4}{3}\beta - \frac{2}{3}\sqrt{(4\beta - 1)(3\alpha + 4\beta - 1)}, \tag{53}$$

and thus completes the proof. □

Suppose that e is an exponent of full size, then $e \approx N^2$, and δ satisfies the following bound

$$\delta < \frac{5}{3} + \frac{4}{3}\beta - \frac{2}{3}\sqrt{(4\beta - 1)(5 + 4\beta)}.$$

In fact, this is twice the bound obtained by de Weger [18] for the attack on RSA with small prime difference.

C. EXPERIMENTAL RESULT

We experimented the method of Theorem 6 in Windows 10 on a 1.8 GHz Intel (R) CoreTM i7-8550U processor. In particular, we generated p and q of different sizes up to 1024 bits randomly, where p and q are prime satisfying $q < p < 2q$, and $|p - q| = N^\beta$ for various sizes of β where $N = pq$. Furthermore, we generated various integers d satisfying $\gcd(d, \psi(N)) = 1$, and $d = N^\delta$ with $\delta < 0.76$. Finally, we computed the inverse e of d with $ed \equiv 1 \pmod{\psi(N)}$, and applied Theorem 6 to determine the solution for equation $x(y^2 + ay + b) + 1 \equiv 0 \pmod{e}$ with $a = N + 4M + 1$, and $b = N^2 + 4M^2 + 2MN + 2M - N + 1$ where $M = \left\lfloor \sqrt{N} \right\rfloor$. If any, the solution should be $x_0 = k$, $y_0 = p + q - 2M$. We also used the parameters

$$X = \left\lfloor N^{\alpha+\delta-2} \right\rfloor, \quad Y = \left\lfloor N^{2\beta - \frac{1}{2}} \right\rfloor. \tag{54}$$

The run time of the method is essentially dominated by executing the LLL algorithm to reduce the basis of the lattice. We present the result when the size of primes are 512 bits. Let

$N = 152739894849024639833377530422598617226800715046348781131979618529844771257038220294004628607605816776256220779292169197545897392610901759\42379000777483548138152161583757801998290690049222213458914981352079809496493795852806156475\47597821863263598812175611409479287047008122656747472751057876560406156530033909,$ (55)

and

$e = 8244376305746274359300173489874081528855956848246566748417381154250098999880949569616868015780\65694334536224406441814157757530121822796439617\08833315651627819247540376705139622053100606198\66751754200183789552975377115083444272305558809\36479830988018702655448889460615818702745223761\18956404855286080772320251009493573118971757375\61727255154652961409337124180076907441094886778\63414619798977193873652948719174578749740209352\7922362779970663438301233823558996329666161278344141325951037134585598518127327974987518601436\59786626755538337749948071191808413784280125588\26681679536597528506806244992958049790680437328\99345.$ (56)

When $m = 4$, $t = 3$, $\omega = 40$, $X = \lfloor N^{0.7} \rfloor$, $Y = \lfloor N^{0.5} \rfloor$, we get

$y_0 = 308969956922417296530000444546889040710402409\37159141529057433020805178997386350204865151\60145439397721308864.$ (57)

Using $p + q = 2\left\lfloor \sqrt{N} \right\rfloor + y_0$ and $pq = N$, we get

$p = 123587982768966918611993998419617167938230363\66250313910481119990252931090005579893904921\60149448115395532869242417139370694457716386897\82937357157548266937,$ (58)

$q = 123587982768966918611981639621340271246369164\26266117738801737686661630605861453178190589\63083548059596593820026402194559154904429462\65657979864630905505577.$ (59)

Then, one can observe that $|p - q| = N^\beta$ with $\beta \approx 0.428$, $d = N^\delta$ with $\delta \approx 0.615$, and $e = N^\alpha$ with $\alpha \approx 1.998$. The bound on δ in Theorem 6 is then $\delta < 0.780$. We believe that by increasing m and t, our method will succeed to solve the problem for bounds on δ approaching the optimal value 0.780.

TABLE 2. The values of δ for $\alpha = \log_N e = 2$ and $\beta = 0.5$.

Attack	General bound for d	Bound for d
Kühnel [8] attack on standard RSA	$\delta < \frac{1}{6}(4\beta+5) - \frac{1}{3}\sqrt{(4\beta+5)(4\beta-1)}$ $\lvert p-q\rvert = N^\beta$	$\delta = 0.292$
Weger [18] attack on standard RSA	$\delta \leq 1 - \sqrt{2\beta - \frac{1}{2}}$ $\lvert p-q\rvert = N^\beta$	$\delta = 0.292$
Our attack on cubic Pell equation variant of RSA	$\delta < \frac{5}{3} + \frac{4}{3}\beta - \frac{2}{3}\sqrt{(4\beta-1)(3\alpha+4\beta-1)}$ $e = N^\alpha, \alpha \approx 2$ $\lvert p-q\rvert = N^\beta$	$\delta = 0.65$

D. COMPARISON WITH FORMER ATTACKS ON STANDARD RSA UNDER SAME ASSUMPTION

In this section we provide a comparison with a former attack upon the standard RSA under the same assumption that is the modulus $N = pq$ contains primes that share MSB's and that the strategy to conduct the attack is via Coppersmith's method. As provided in Table 2, it is visible that the bound for insecure private exponent d derived from the Murru-Saettone RSA variant is much larger than the standard version. This implies that, the cubic Pell equation variant of RSA has much more insecure private exponents than the standard RSA under the sharing MSB's assumption and Coppersmith's method analysis strategy. Thus, one needs to choose the parameters carefully so that the cryptosystem is insusceptible through the communication networks.

VI. CONCLUSION

In this paper, we present two novel attacks on the variant of the RSA crytosystem designed in [12]. This variant uses an RSA modulus of the form $N = pq$, a public parameter $e = N^\alpha$, and a private parameter $d = N^\delta$. Our new results extend the former results in [14]. Our work focuses on the conditions that a potential user of the cryptosystem being analyzed must avoid at all costs. The disadvantage for the user who is not careful enough when generating the keys, would result in a total break of the cryptosystem. As such, our work provides important inputs for the user in order not to be at a disadvantage when utilizing the cryptosytem that we have analyzed.

For the first approach, we utilised the continued fractions algorithm, and proved that the variant of the RSA crytosystem is vulnerable whenever $\delta < \frac{7}{4} - \frac{1}{2}\alpha - \beta$ whereas for the second attack, we applied Coppersmith's method and showed that when $d < N^\delta$ for $\delta < \frac{5}{3} + \frac{4}{3}\beta - \frac{2}{3}\sqrt{(4\beta-1)(3\alpha+4\beta-1)}$, then the private p and q can be solved in polynomial time.

Finally, as shown in Table 1 and 2, the cubic Pell equation variant of RSA which utilizes primes that share MSB's has a larger set of weak private keys when compared with the standard RSA algorithm when analyzed under the assumption that $|p-q| = N^\beta$ is sufficiently small.

Ultimately, if a user of the cryptosystem being analyzed adheres to our analysis, our attack would not be fruitful. Specifically, the user needs to ensure that the decryption exponent and the difference between both the primes are larger than our bound.

ACKNOWLEDGMENT

The authors would like to thank an anonymous reviewer and an editor for their valuable comments to improve this paper.

REFERENCES

[1] M. Ariffin, S. Abubakar, F. Yunos, and M. Asbullah, "New cryptanalytic attack on RSA modulus $N = pq$ using small prime difference method," *Cryptography*, vol. 3, no. 1, p. 2, Dec. 2018.

[2] D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$," in *Advances in Cryptology—EUROCRYPT'99*. Berlin, Germany: Springer, 1999, pp. 1–11.

[3] D. Coppersmith, "Small solutions to polynomial equations, and low exponent RSA vulnerabilities," *J. Cryptol.*, vol. 10, no. 4, pp. 233–260, Sep. 1997.

[4] S. D. Galbraith, *Mathematics of Public Key Cryptography*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[5] M. Hinek, *Cryptanalysis of RSA and Its Variants*. Boca Raton, FL, USA: CRC Press, 2009.

[6] N. Howgrave-Graham, "Finding small roots of univariate modular equations revisited," in *Proc. IMA Int. Conf. Cryptogr. Coding*. Berlin, Germany: Springer, 1997, pp. 131–142.

[7] T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. T. Riele, A. Timofeev, and P. Zimmermann, "Factorization of a 768-bit RSA modulus," in *Proc. 30th Annu. Cryptol. Conf.* Santa Barbara, CA, USA, 2010, pp. 333–350.

[8] M. Kühnel, "RSA vulnerabilities with small prime difference," in *Research in Cryptology*. Berlin, Germany: Springer, 2012, pp. 122–136.

[9] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, pp. 513–534, Dec. 1982.

[10] Y. Lu, R. Zhang, L. Peng, and D. Lin, "Solving linear equations modulo unknown divisors: Revisited," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2015, pp. 189–213.

[11] A. Overmars and S. Venkatraman, "Mathematical attack of RSA by extending the sum of squares of primes to factorize a semi-prime," *Math. Comput. Appl.*, vol. 25, no. 4, p. 63, Sep. 2020.

[12] N. Murru and F. M. Saettone, "A novel RSA-like cryptosystem based on a generalization of the Rédei rational functions," in *Number-Theoretic Methods in Cryptology*. Cham, Switzerland: Springer, 2018, pp. 91–103.

[13] A. Nitaj, "Another generalization of Wiener's attack on RSA," in *Progress in Cryptology—AFRICACRYPT 2008*. Berlin, Germany: Springer, 2008, pp. 174–190.

[14] A. Nitaj, M. R. K. Arrifin, N. N. H. Adenan, and A. Abu, "Classical attacks on a variant of the RSA cryptosystem," in *Progress in Cryptology—LATINCRYPT 2021*. Cham, Switzerland: Springer, 2021, pp. 151–167.

[15] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[16] S. Sarkar, "Small secret exponent attack on RSA variant with modulus $N = p^{rq}$," *Des., Codes Cryptogr.*, vol. 73, no. 2, pp. 383–392, 2014.

[17] T. Takagi, "A fast RSA-type public-key primitive modulo p^{kq} using Hensel lifting," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. 87, no. 1, pp. 94–101, 2004.

[18] B. de Weger, "Cryptanalysis of RSA with small prime difference," *Applicable Algebra Eng., Commun. Comput.*, vol. 13, no. 1, pp. 17–28, Apr. 2002.

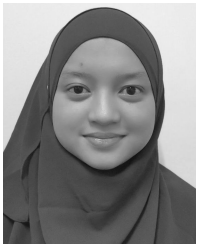
[19] M. J. Wiener, "Cryptanalysis of short RSA secret exponents," *IEEE Trans. Inf. Theory*, vol. 36, no. 3, pp. 553–558, May 1990.

[20] M. Zheng, N. Kunihiro, and Y. Yao, "Cryptanalysis of the RSA variant based on cubic Pell equation," *Theor. Comput. Sci.*, vol. 889, pp. 135–144, Oct. 2021.

[21] W. N. A. Ruzai, M. R. K. Ariffin, M. A. Asbullah, Z. Mahad, and A. Nawawi, "On the improvement attack upon some variants of RSA cryptosystem via the continued fractions method," *IEEE Access*, vol. 8, pp. 80997–81006, 2020.
[22] C. Luo, Y. Fei, and D. Kaeli, "Side-channel timing attack of RSA on a GPU," *ACM Trans. Archit. Code Optim.*, vol. 16, no. 3, pp. 1–18, Sep. 2019.

ABDERRAHMANE NITAJ received the Ph.D. degree in mathematics and the Habilitation degree in cryptography. He is currently a Professor of mathematics and a Researcher with the Laboratory of Mathematics Nicolas Oresme, University of Caen Normandy, France. He is involved in the organization of several international workshops and conferences, such as AfricaCrypt and C2SI. His research interests include cryptography and algorithmic number theory.

MUHAMMAD REZAL BIN KAMEL ARIFFIN received the B.S. and M.S. degrees in mathematics from Universiti Putra Malaysia (UPM), Malaysia, in 1999 and 2002, respectively, and the Ph.D. degree in mathematics from Universiti Kebangsaan Malaysia (UKM), Malaysia, in 2009. He is currently the Director of the Institute for Mathematical Research, UPM, and a Professor with the Department of Mathematics and Statistics, Faculty of Science, UPM. He is also the President of the Malaysian Society for Cryptology Research (MSCR). His research interests include cryptography, specifically designing and analysing number theoretic based cryptosystems and post-quantum cryptography and chaos dynamical systems. He is the General Chair of the Bi-Annual International Cryptology and Information Security Conference (CRYPTOLOGY) Series, in 2008, 2010, 2012, 2014, 2016, 2018, and 2020. He will also the chair for 2022. He is on the Scientific Committee for AfricaCrypt for the years 2016, 2017, 2019, and 2020.



NURUL NUR HANISAH ADENAN received the B.S. degree in mathematics and the M.S. degree in mathematical cryptography from Universiti Putra Malaysia, Malaysia, in 2016 and 2021, respectively. She is currently pursuing the Ph.D. degree in mathematical cryptography with the Institute for Mathematical Research, Universiti Putra Malaysia. Her current research interests include encompass algebraic cryptanalysis and post-quantum cryptography, specifically in code-based cryptography. She is a member of the Malaysian Society of Cryptology Research (MSCR).

TERRY SHUE CHIEN LAU received the B.S. degree in applied mathematics and the M.S. degree in mathematics from the National University of Singapore, Singapore, in 2011 and 2013, respectively, and the Ph.D. degree in mathematics from the University of Malaya, Malaysia, in 2016. He joined the Temasek Laboratories, National University of Singapore, as a Research Scientist, from March 2017 to July 2021. He is currently a Postdoctoral Researcher with the Institute for Mathematical Research, Universiti Putra Malaysia. His research interests include public key cryptography, post-quantum cryptography, code-based cryptography, algebraic combinatorics, and algebraic graph theory.

JIAHUI CHEN (Member, IEEE) received the B.S. degree from South China Normal University, China, in 2009, and the M.S. and Ph.D. degrees from the South China University of Technology, China, in 2012 and 2016, respectively. He joined the Temasek Laboratories, National University of Singapore, as a Research Scientist, from March 2017 to May 2018. He is currently an Associate Professor with the School of Computer and Technology, Guangdong University of Technology. His research interests include public key cryptography, post-quantum cryptography, and information security.