Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 45 (2024), No. 5, pp. 1263–1280
DOI : 10.47974/JIOS-1333

Cryptanalysis of a cubic Pell variant of RSA with primes sharing least significant bits

Nurul Nur Hanisah Adenan [§]
Institute for Mathematical Research
Universiti Putra Malaysia
43400 Serdang
Selangor
Malaysia

Abderrahmane Nitaj *
Department of Mathematics
Normandie Univ
UNICAEN, CNRS, LMNO
14000 Caen
France

Muhammad Rezal Kamel Ariffin [†]
Department of Mathematics and Statistics
Universiti Putra Malaysia
43400 Serdang
Selangor
Malaysia

and

Institute for Mathematical Research
Universiti Putra Malaysia
43400 Serdang
Selangor
Malaysia

* *E-mail:* **abderrahmane.nitaj@unicaen.fr (Corresponding Author)**

[§] *Orcid Id:* **0000-0002-5957-1524**
* *Orcid Id:* **0000-0002-0372-1757**
[†] *Orcid Id:* **0000-0001-5000-354X**

Nur Azman Abu ‡
Faculty of Information Technology and Communication
Universiti Teknikal Malaysia
Melaka
Malaysia

Abstract

In this paper, we push further the cryptanalysis of a cryptosystem of the RSA's variant which utilized a cubic Pell equation with the key equation $ed - k(p^2 + p + 1)(q^2 + q + 1) = 1$ where $N = pq$ is an RSA modulus, e, N are publicized, while d, p, q are kept private. We consider the case where the prime factors share an amount of their least significant bits (LSBs), that is p and q satisfy $p - q = 2^m u$ where m is known, and u is unknown. Through this work, we show that via Coppermith's method and lattice basis reduction, it is feasible to retrieve the secret key d and factor N for larger values of d.

Subject Classification: *11T71, 14G50.*

Keywords: *RSA, Factorization, Coppersmith's method, Lattice basis reduction, Cubic Pell equation.*

1. Introduction

The RSA encryption method [12] has been widely studied and implemented since it was introduced in 1978. Various modifications and improvements have been proposed for better efficiency and security. Any new variant of RSA from a different field will be evaluated in terms of its security vulnerabilities in comparison to the original RSA design.

The RSA construction algorithm consists of the public and private keys written as (N, e) and $(p, q, d, \phi(N))$ respectively. The integer $N = pq$ is an expression of the multiplication between two private prime numbers, p and q while $e \in \mathbb{Z}^+$ must be coprime with $\phi(N)$, where $\phi(N) = (p-1)(q-1)$. The computation of inverse modulo of $e \pmod{\phi(N)}$ yields the integer d. A standard RSA uses a small public exponent e for fast signature verification. The size of d affects greatly the efficiency of the decryption algorithm, thus leading to the favorable usage of small $d = N^{\delta}$.

Wiener [15] was the first that designed an attack upon the RSA. He proved that whenever $d < \frac{1}{3}N^{1/4}$, the method of continued fraction upon $\frac{e}{N}$ would yield $\frac{k}{d}$ as one of the convergents. Knowing these private keys is adequate to factor the modulus N. This result was later extended by [1] up to $\delta < 0.292$ for traditional RSA with a relatively small private exponent.

‡ *Orcid Id:* 0000-0003-4624-3123

A few years later, Coppersmith [2] proposed a lattice basis reduction technique to efficiently find small solutions of modular polynomial equations and roots of polynomials of a specific form. He applied this method to an RSA modulus $N = pq$ and demonstrated that knowing half of the bits of p or q is sufficient to factorize N.

Meanwhile, the works from [13,14,9] presented RSA variants in which primes share a certain number of LSBs, and found that the bound on the private exponent d for which RSA is vulnerable can be improved based on the parameter t.

In the year 2018, a cubic Pell RSA variant was designed by [7] with the aim to have better security compared to the original RSA for broadcast applications. In this variant, they modified the key equation into $ed - 1 \equiv 0 (\mathrm{mod}\, \psi(N))$, where $\psi(N) = (p^2 + p + 1)(q^2 + q + 1)$. They claimed that their scheme was not vulnerable to the attack designed by [15], as the secret exponent d was as large as the modulus N. However, Nitaj et al. showed that the method in [15] and [1] can still be used to attack their scheme. The cubic Pell RSA variant is particularly vulnerable to Coppersmith's method on a small private exponent $d < N^{0.569}$, and even more so to the lattice-based method when $d < N^{0.585}$. These bounds are much higher than the current bound of $N^{0.292}$ by Boneh and Durfee and the conjectured bound of $d < N^{0.5}$ for standard RSA.

In a previous work [11], the authors investigated investigated the vulnerability of the cubic Pell RSA variant $N = pq$ when the difference between the primes is small, which occurs whenever some amount of their most significant bits (MSBs) is shared. They found that using Coppersmith's method on a small private exponent $d = N^{\delta}$, the insecure bound can be extended up to $\delta < \frac{5}{3} + \frac{4}{3}\beta - \frac{2}{3}\sqrt{(4\beta-1)(3\alpha+4\beta-1)}$, where $p - q = N^{\beta}$ and $e = N^{\alpha}$.

The work in this paper explores the vulnerability of the cubic Pell RSA variant when the primes share a number of their LSBs, specifically when $p - q = 2^m u$ where m is either known or unknown. This scenario has been studied in the literature for the original RSA (see [13,14,9]). For the cubic Pell RSA variant, we set $e = N^{\alpha}$, $d = N^{\delta}$, and $p - q = 2^m u$ with $2^m = N^{\beta}$, and transform the key equation into a polynomial

$$x(y^2 + ax + b) + c \equiv 0 \pmod{e},$$

where a, b, and c are known integer coefficients. We then use Coppersmith's method and lattice reduction to show that the cubic Pell RSA variant is vulnerable if

$$\delta < \frac{7}{3} - \frac{4}{3}\beta - \frac{2}{3}\sqrt{(1-4\beta)(3\alpha+1-4\beta)}.$$

In a typical scenario where $p, q \approx 2^{1024}$, $N \approx 2^{2048}$, e being roughly N^2 and $p-q$ around $2^{40}u$, we can estimate α to be about 2 and β to be approximately 0.02. If we take $d = N^{\delta}$ where δ is less than 0.624, then the cubic Pell RSA variant is vulnerable. Notably, this bound is significantly surpassed the bound of 0.569 in [10] and 0.585 in [16].

The rest of this paper is covered by six crucial sections. Section 2 describes the cubic Pell RSA variant of Murru and Saettone, and presents Coppersmith's method. Meanwhile, two useful lemmas from the literature are presented in Section 3. The next two sections present our main work that includes the theorem and proof and an improved bound for the cryptanalysis of the cubic Pell RSA variant respectively. The numerical example of a large and concrete value is presented in the next section and the conclusion is in the last section.

2. Preliminaries

This section presents briefly Murru and Saettone's scheme and the method of Coppersmith to solve for the small solutions given a single modular multivariate polynomial.

2.1 *Murru and Saettone Scheme*

An RSA-like scheme has been constructed by Murru and Saettone [11] which is intended to have better security compared to the RSA in broadcast applications that work on a cubic field relating to the cubic Pell equation

$$x^3 + ry^3 + r^2z^3 - 3rxyz = 1,$$

where r is a given non-cubic integer and x, y, z are unknown numbers. Let $(G, +, \times)$ be a field. Take a quotient field $A = G[t]/(t^3 - r)$ as the set of elements of the form $x + ty + t^2z$ with $(x, y, z) \in G^3$. Then, a product $\bullet$ between two such elements can be computed as follows:

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

Next, consider the set

$$A = \{(x, y, z) \in G^3 : x^3 + ry^3 + r^2z^3 - 3rxyz = 1\}.$$

Then, $(A, \bullet)$ is a commutative group with the identity $e = (1, 0, 0,)$ and the inverse of (x, y, z) in A is $(x, y, z)^{-1} = (x^2 - ryz, rz^2 - xy, y^2 - xz)$.

Next, let a quotient group $B = F^* / G^*$ composed with elements of the forms $a + bt + t^2$, or $a + t$, or 1 only. Consequently, the group B reduces to

$$B = \{G \times G\} \cup \{G \times \{\mu\}\} \cup \{(\mu, \mu)\},$$

where (μ, μ) denotes a point at infinity. A commutative addition operation $\oplus$ in B can be defined as follows:

1. $(a, \mu) \oplus (p, \mu) = (ap, a + p)$.
2. $(a, b) \oplus (p, \mu) = (\mu, \mu)$ when $b + p = 0$ and $a - b^2 = 0$.
3. $(a, b) \oplus (p, \mu) = (\frac{ap+r}{a-b^2}, \mu)$ when $b + p = 0$ and $a - b^2 \neq 0$.
4. $(a, b) \oplus (p, \mu) = \left(\frac{ap+r}{b+p}, \frac{a+bp}{b+p}\right)$ when $b + p \neq 0$.
5. $(a, b) \oplus (p, q) = (\mu, \mu)$ when $a + p + bq = 0$ and $bp + aq + r = 0$.
6. $(a, b) \oplus (p, q) = \left(\frac{ap+(b+q)r}{bp+aq+r}, \mu\right)$ when $a + p + bq = 0$ and $bp + aq + r \neq 0$.
7. $(a, b) \oplus (p, q) = \left(\frac{ap+(b+q)r}{a+p+bq}, \frac{bp+aq+r}{a+p+bq}\right)$ when $a + p + bq \neq 0$.

In addition, an exponentiation operation to a power of a positive integer k is defined as

$$(a, b)^{\oplus k} = (a, b) \oplus (a, b) \oplus \ldots \oplus (a, b), \; k \text{ times}.$$

Taking $G = \mathbb{F}_p$ as a prime field and $\mu = \infty$, we get that $A = G^3$ is a Galois field with p^3 elements. Then B is a cyclic group of order $\frac{p^3-1}{p-1} = p^2 + p + 1$. Therefore, we always have $(a, b)^{\oplus(p^2+p+1)} = (\mu, \mu) \bmod p$ for every $(a, b) \in B$.

A scheme of RSA variant was proposed by [7] based on the group B. Suppose $N = pq$, take the ring $G = \mathbb{Z} / \mathbb{Z}_N$ and $\mu = \infty$. Then the corresponding set B is a cyclic group of order $\psi(N) = (p^2 + p + 1)(q^2 + q + 1)$. Therefore, for any $(a, b) \in B$, we have

$$(a, b)^{\oplus \psi(N)} = (\mu, \mu) \; (\text{mod } N).$$

Having all group properties above, an RSA variant on the quotient group B provides a valid cryptosystem. Three algorithms on this scheme are presented as follows.

1. **Key Generation**

   Input: The modulus of n bit-size.

   Output: A public key (N, e, r) and a private key (N, d, r).

- Select two prime numbers p and q.
- Compute $N = pq$ and $\psi(N) = (p^2 + p + 1)(q^2 + q + 1)$.
- Select $r \in \mathbb{Z}$ which is non-cubic modulo p, q, and N.
- Select $e \in \mathbb{Z}$ such that e and $\psi(N)$ are coprime.
- Compute $d \equiv \frac{1}{e} (\mathrm{mod}\, \psi(N))$.
- Return (N, e, r) and (N, d, r).

2. **Encryption**

Input: A pair of messages $m_1, m_2 \in \mathbb{Z}_N$, and public key (N, e, r).

Output: The ciphertext (c_1, c_2).

- Compute $(c_1, c_2) \equiv (m_1, m_2)^{\oplus e}$ using the addition operation $\oplus$ on the curve with the equation $x^3 + ry^3 + r^2z^3 - 3rxyz \equiv 1 \pmod N$.
- Return (c_1, c_2).

3. **Decryption**

Input: The ciphertext (c_1, c_2), and private key (N, d, r).

Output: Messages m_1, m_2.

- Compute $(m_1, m_2) \equiv (c_1, c_2)^{\oplus d}$ using the addition operation $\oplus$ on the curve with the equation $x^3 + ry^3 + r^2z^3 - 3rxyz \equiv 1 \pmod N$.
- Return (m_1, m_2).

2.2 *Coppersmith's method*

A useful tool was invented by [2] to solve an integer bivariate equation $F(x, y) = 0$, and a modular equation of one variable $G(x) \equiv 0 \pmod N$, where both polynomials consisting of integer coefficients. Since then, the method of Coppersmith has been generalized in several forms. This method uses lattice reduction algorithms to find the roots of the intended polynomial[5]. The following result is useful to our attack on the cubic Pell variant of RSA (see [6]).

Theorem 1 (LLL): *Let a basis* $(u_1, \ldots, u_\omega)$ *spanned a lattice* $\mathcal{L}$. *The LLL algorithm yields a new basis* $(b_1, \ldots, b_\omega)$ *of L that satisfies*

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

for $i = 1, 2, \ldots, \omega$.

Let $H(x_1, x_2) = \sum a_{i_1 i_2} x_1^{i_1} x_2^{i_2}$ be a polynomial where the coefficients are integer. Define the norm of $H(x_1, x_2)$ as $\| F(x_1, x_2) \| = \sqrt{\sum a_{i_1 i_2}^2}$. The result below is a foundation of Coppersmith's method.

Theorem 2 [Howgrave-Graham] [3]: *Let* $H(x_1, x_2) = \sum a_{i_1 i_2} x_1^{i_1} x_2^{i_2}$ *be a polynomial with integer coefficients with at most* ω *monomials. If*

$$| x_1^{(0)} | < X_1, \quad | x_2^{(0)} | < X_2, \quad h(x_1^{(0)}, x_2^{(0)}) \equiv 0 \pmod{e^m}, \quad \| H(x_1 X_1, x_2 X_2) \| < \frac{e^m}{\sqrt{\omega}},$$

then $H(x_1^{(0)}, x_2^{(0)}) = 0$ *holds over the integers.*

The first step to find small solutions $(x_1^{(0)}, x_2^{(0)})$ of $F(x_1, x_2) \equiv 0 \pmod{N}$ with $| x_1^{(0)} | < X_1$, $| x_2^{(0)} | < X_2$ is by collecting ω polynomials $F_i(x_1, x_2)$ satisfying $F_i(x_1^{(0)}, x_2^{(0)}) \equiv 0 \pmod{N}$. A lattice is then constructed by collecting the coefficients of the polynomials $F_i(X_1 x_1, X_2 x_2)$ to form its basis. Then, reducing the basis gives rise to ω polynomials $H_i(x, y)$ satisfying $H_i(x_1^{(0)}, x_2^{(0)}) \equiv 0 \pmod{N}$. Combining Theorem 1, Theorem 2, and under some specific conditions on X_1 and X_2, at least two polynomials $H_1(x_1, x_2)$ and $H_2(x_1, x_2)$ share the small root $(x_1^{(0)}, x_2^{(0)})$ over the integers, that is $H_1(x_1^{(0)}, x_2^{(0)}) = H_2(x_1^{(0)}, x_2^{(0)}) = 0$. By resultant techniques or Gröbner basis calculation, it is possible to find $(x_1^{(0)}, x_2^{(0)})$ assuming that $H_1(x_1, x_2)$ and $H_2(x_1, x_2)$ are coprime.

3. Useful Lemmas

The work in [8] provides the results for the bounds for p, and q in terms of N. Let $N = pq$ be the product of two unknown and balanced primes. Then

$$N^{1/2} < p + q < 3N^{1/2}.$$

The following result concerns the case when there exists a number of LSBs shared between the primes p and q of the modulus N. (see [13, 9]).

Lemma 2: *Let* $N = pq$ *be an RSA modulus with* $q < p < 2q$. *Suppose that* $p - q = 2^m u$ *where* m *is known. Then* $p = 2^m p_1 + u_0$, $q = 2^m q_1 + u_0$, *and* $p + q = 2^{2m} v + v_0$ *where* u_0 *is a solution of the equation* $z^2 \equiv N \pmod{2^m}$ *and*

$$v_0 \equiv 2u_0 + (N - u_0^2) u_0^{-1} \pmod{2^{2m}}.$$

4. The Small Solutions of the Generalized Key Equation

In this section, we apply Coppersmith's method to find the small solutions of the generalized key equation $x_1(x_2^2 + ax_2 + b) + c \equiv 0 \pmod{e}$.

Theorem 3: *Let e and* $N \in \mathbb{Z}^+$ *with* $e = N^\alpha$. *Let* $a < e$, $b < e$, $c < e$ *be positive integers. Suppose that* $x_1(x_2^2 + ax_2 + b) + c \equiv 0 \pmod{e}$ *with* $x_1 = N^{\delta_1}$, $x_2 = N^{\delta_2}$, *and* $\delta_2 < \frac{1}{2}\alpha$. *Then one can retrieve* x_1 *and* x_2 *if*

$$\delta_1 < \alpha + \frac{2}{3}\delta_2 - \frac{2}{3}\sqrt{2\delta_2(2\delta_2 + 3\alpha)}.$$

Proof: Let $N, e \in \mathbb{Z}^+$ and $e = N^\alpha$. Suppose that e fulfilled the condition such that

$$x_1(x_2^2 + ax_2 + b) + c \equiv 0 \pmod{e},$$

where $a, b, c \in \mathbb{Z}^+$ are smaller than e. Set

$$f(x_1, x_2) = x_1(x_2^2 + ax_2 + b) + c \equiv 0 \pmod{e},$$

where $x_1 \le N^{\delta_1}$ and $x_2 \le N^{\delta_2}$ are the small solutions that needed to be solved via Coppersmith's method. We consider the following strategy, inspired by [4]. Suppose $m, t \in \mathbb{Z}^+$. The set is defined as

$$M_l = \bigcup_{0 \le k \le t} \{x_1^{i_1} x_2^{i_2+k} \mid x_1^{i_1} x_2^{i_2} \text{ is a monomial of } f^m(x_1, x_2) \text{ and } \frac{x_1^{i_1} x_2^{i_2}}{(x_1 x_2^2)^l} \text{ is a monomial of } f^{m-l}(x_1, x_2)\}$$

for $l = 0, \ldots, m$. The monomials of the set M_l can be characterized by $x_1^{i_1} x_2^{i_2} \in M_l$ if

$$i = l, \ldots, m,\ j = 2l, \ldots, 2i + t.$$

For $l = 0, \ldots, m$, the polynomial is defined as

$$G_{l,i,j}(x, y) = \frac{x_1^{i_1} x_2^{i_2}}{(x_1 x_2^2)^l} f(x_1, x_2)^l e^{m-l} \quad \text{with} \quad x_1^{i_1} x_2^{i_2} \in M_l \setminus M_{l+1}.$$

From M_l, we deduce M_{l+1} as $x_1^{i_1} x_2^{i_2} \in M_{l+1}$ if

$$i_1 = l + 1, \ldots, m,\ i_2 = 2l + 2, \ldots, 2i + t.$$

The set $M_l \setminus M_{l+1}$ is characterized by $x_1^{i_1} x_2^{i_2} \in M_l \setminus M_{l+1}$ if

$$\begin{cases} i_1 = l, \ldots, m, \\ i_2 = 2l, 2l + 1. \end{cases} \quad \text{or} \quad \begin{cases} i_1 = l, \\ i_2 = 2l + 2, \ldots, 2i + t. \end{cases}$$

Then $G_{l,i_1,i_2}(x_1,x_2)$ reduces to one of the following polynomials

$$G_{l,i_1,i_2}(x_1,x_2)=x_1^{i_1-l}x_2^{i_2-2l}f(x_1,x_2)^l e^{m-l},$$

for

$$\begin{cases} l=0,\dots m, \\ i_1=l,\dots,m, \\ i_2=2l,2l+1, \end{cases} \quad \text{or} \quad \begin{cases} l=0,\dots m, \\ i_1=l, \\ i_2=2l+2,\dots,2i_1+t. \end{cases}$$

A lattice $\mathcal{L}$ is defined to be spanned by the coefficient vectors of the polynomials $G_{l,i_1,i_2}(x_1X_1,x_2X_2)$ where $X_1,X_2\in\mathbb{Z}^+$ satisfying

$$X_1=[N^{\delta_1}],X_2=[N^{\delta_2}].$$

The matrix of the lattice contains the rows that denoted as G_{l,i_1,i_2} and ordered by the rule G_{l,i_1,i_2} is prior to $G_{l',i_{1'},i_{2'}}$ if

$$\{i_1<i_{1'}\} \text{ or } \{i_1=i_{1'},i_2<i_{2'}\} \text{ or } \{i_1=i_{1'},i_2=i_{2'},l<l'\}.$$

The monomials $x_1^{i_1}x_2^{i_2}$ are ordered by the rule $x_1^{i_1}x_2^{i_2}$ is prior to $x_1^{i_{1'}}x_2^{i_{2'}}$ if

$$\{i_1<i_{1'}\} \text{ or } \{i_1=i_{1'},i_2<i_{2'}\}.$$

Table 1 presents the structure of the lattice $\mathcal{L}$ as follows.

Table 1

The matrix of the lattice for $m=2$ and $t=2$.

$G_{l,i_1,2}$	1	x_2	x_2^2	x_1	x_1x_2	$x_1x_2^2$	$x_1x_2^3$	$x_1x_2^4$	x_1^2	$x_1^2x_2$	$x_1^2x_2^2$	$x_1^2x_2^3$	$x_1^2x_2^4$	$x_1^2x_2^5$	$x_1^2x_2^6$
$G_{0,0,0}$	e^2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,0,1}$	0	X_2e^2	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,0,2}$	0	0	$X_2^2e^2$	0	0	0	0	0	0	0	0	0	0	0	0
$g_{0,1,0}$	0	0	0	X_1e^2	0	0	0	0	0	0	0	0	0	0	0
$G_{0,1,1}$	0	0	0	0	$X_1X_2e^2$	0	0	0	0	0	0	0	0	0	0
$G_{1,1,2}$	⊛	0	0	⊛	⊛	$X_1X_2^2e$	0	0	0	0	0	0	0	0	0
$G_{1,1,3}$	0	⊛	0	0	⊛	⊛	$X_1X_2^3e$	0	0	0	0	0	0	0	0
$G_{1,1,4}$	0	0	⊛	0	0	⊛	⊛	$X_1X_2^4e$	0	0	0	0	0	0	0
$G_{0,2,0}$	0	0	0	0	0	0	0	0	$X_1^2e^2$	0	0	0	0	0	0
$G_{0,2,1}$	0	0	0	0	0	0	0	0	0	$X_1^2X_2e^2$	0	0	0	0	0
$G_{1,2,2}$	0	0	0	⊛	0	0	0	0	⊛	⊛	$X_1^2X_2^2e$	0	0	0	0
$G_{1,2,3}$	0	0	0	0	⊛	0	0	0	0	⊛	⊛	$X_1^2X_2^3e$	0	0	0
$G_{2,2,4}$	⊛	0	0	⊛	⊛	⊛	0	0	⊛	⊛	⊛	⊛	$X_1^2X_2^4$	0	0
$G_{2,2,5}$	0	⊛	0	0	⊛	⊛	⊛	0	0	⊛	⊛	⊛	⊛	$X_1^2X_2^5$	0
$G_{2,2,6}$	0	0	⊛	0	0	⊛	⊛	⊛	0	0	⊛	⊛	⊛	⊛	$X_1^2X_2^6$

Note that the symbols $\circledast$ are non-zero entries and they only fill up the lower triangle of the square matrix. Thus, its determinant can be computed by taking the product of the elements diagonally which are written as follows,

$$\det(\mathcal{L}) = X_1^{n_{X_1}} X_2^{n_{X_2}} e^{n_e}. \tag{1}$$

We define the function S by

$$S(z) = \sum_{l=0}^{m} \sum_{i_1=l}^{m} \sum_{i_2=2l}^{2l+1} z + \sum_{l=0}^{m} \sum_{i_1=l}^{l} \sum_{i_2=2l+2}^{2i_1+t} z,$$

and set $t = m\tau$ for a certain value τ to be optimized later. Note that ω is symbolized as the dimension of the lattice. Then, n_{X_1}, n_{X_2}, n_e, and ω satisfy

$$\begin{aligned}
n_{X_1} &= S(i_1) = \frac{1}{6} m(m+1)(4m+3\tau m+5) \\
&= \frac{1}{6}(3\tau+4)m^3 + o(m^3) \\
n_{X_2} &= S(i_2) = \frac{1}{6} m(m+1)(3\tau^2 m+6\tau m+3\tau+4m+5) \\
&= \frac{1}{6}(3\tau^2+6\tau+4)m^3 + o(m^3) \\
n_e &= S(m-l) = \frac{1}{6} m(m+1)(4m+3\tau m+5) \\
&= \frac{1}{6}(3\tau+4)m^3 + o(m^3) \\
\omega &= S(1) = (m+1)(m+\tau m+1) \\
&= (\tau+1)m^2 + o(m^2).
\end{aligned} \tag{2}$$

Next, we combine Theorem 2 and Theorem 1 for $i_1 = 2$ by the condition

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

or equivalently

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

Using $\det(\mathcal{L}) = X_1^{n_{X_1}} X_2^{n_{X_2}} e^{n_e}$, we get

$$e^{n_e - m\omega} X_1^{n_{X_1}} X_2^{n_{X_2}} < \frac{2^{-\frac{\omega(\omega-1)}{4}}}{(\sqrt{\omega})^{\omega-1}} e^{-m}. \tag{3}$$

We use the approximations n_{X_1}, n_{X_2}, n_e, ω from (2), and $X_1 = N^{\delta_1}$, $X_2 = N_2^{\delta}$, $e = N^{\alpha}$ in (3), we get after taking logarithms, and dividing by $\log(N)$,

$$3\delta_2\tau^2 + 3(\delta_1 + 2\delta_2 - \alpha)\tau + 2(2\delta_1 + 2\delta_2 - \alpha) < -\varepsilon_1,$$

where $\varepsilon_1 \in \mathbb{Z}^+$ is negligible. In the left side, the optimal value for τ is $\tau_0 = \frac{\alpha - \delta_1 - 2\delta_2}{2\delta_2}$, for which the inequality reduces to

$$-3\delta_1^2 + 2(3\alpha + 2\delta_2)\delta_1 + 4\delta_2^2 + 4\alpha\delta_2 - 3\alpha^2 < -\varepsilon_2,$$

for a $\varepsilon_2 \in \mathbb{Z}^+$ where the value is small. The former inequality is fulfilled if

$$\delta_1 < \alpha + \frac{2}{3}\delta_2 - \frac{2}{3}\sqrt{2\delta_2(2\delta_2 + 3\alpha)}.$$

There are some extra conditions to be satisfied. First, τ_0 should be positive. Hence $\alpha - \delta_1 - 2\delta_2 \geq 0$, that is $\delta_1 \leq \alpha - 2\delta_2$. Next, we must have $\alpha - 2\delta_2 \geq 0$, that is $\delta_2 \leq \frac{1}{2}\alpha$. Then, we have $\alpha \geq 2\delta_2$, and

$$\begin{aligned}
\alpha + \frac{2}{3}\delta_2 - \frac{2}{3}\sqrt{2\delta_2(2\delta_2 + 3\alpha)} &= \frac{\left(\alpha + \frac{2}{3}\delta_2\right)^2 - \frac{4}{9}\times 2\delta_2(2\delta_2 + 3\alpha)}{\alpha + \frac{2}{3}\delta_2 + \frac{2}{3}\sqrt{2\delta_2(2\delta_2 + 3\alpha)}} \\
&= \frac{\frac{1}{3}(3\alpha + 2\delta_2)(\alpha - 2\delta_2)}{\alpha + \frac{2}{3}\delta_2 + \frac{2}{3}\sqrt{2\delta_2(2\delta_2 + 3\alpha)}} \\
&\geq 0,
\end{aligned}$$

which shows that the bound on δ_1 is valid. Combining both conditions on δ_1, a straightforward computation shows that for $\alpha \geq 2\delta_2$, we have

$$\delta_1 < \min\left(\alpha + \frac{2}{3}\delta_2 - \frac{2}{3}\sqrt{2\delta_2(2\delta_2 + 3\alpha)}, \alpha - 2\delta_2\right) = \alpha + \frac{2}{3}\delta_2 - \frac{2}{3}\sqrt{2\delta_2(2\delta_2 + 3\alpha)}.$$

Performing LLL, we then extract two polynomials $h_1(x_1, x_2)$ and $h_2(x_1, x_2)$ satisfying $h_1(x_1^{(0)}, x_2^{(0)}) = h_2(x_1^{(0)}, x_2^{(0)}) = 0$. If the polynomials are coprime, then resultant techniques or Gröbner basis are the suitable approaches used to find all solutions $(x_1^{(0)}, x_2^{(0)})$ with $|x_1^{(0)}| < X_1$, and $|x_1^{(0)}| < X_2$. This terminates the proof.

5. Cryptanalysis of the RSA Variant Based on Cubic Pell Equation

In this section, we present our attack on the scheme of Murru and Saettone using the key equation $ed - k(p^2 + p + 1)(q^2 + q + 1) = 1$ when p and q share an amount of their least significant bits.

Theorem 4: *Let* $N = pq$ *such that* $q < p < 2q$ *be the product of two large unknown primes and* $p - q = 2^m u$ *where m is known. Suppose that* $2^m = N^\beta$ *and* $e = N^\alpha$ *is an odd integer that satisfies* $ed \equiv 1 (\mathrm{mod}\, \psi(N))$ *with* $\psi(N) = (p^2 + p + 1)(q^2 + q + 1)$, *and* $d = N^\delta$. *Then, d could be retrieved which leads to the factorization of N if* $\alpha > 2\beta$, *and*

$$\delta < \frac{7}{3} - \frac{4}{3}\beta - \frac{2}{3}\sqrt{(1-4\beta)(3\alpha + 1 - 4\beta)}.$$

Proof: Suppose that e is an odd public key that satisfies the key equation $ed - k\psi(N) = 1$ with $\psi(N) = (p^2 + p + 1)(q^2 + q + 1)$, and $p - q = 2^m u$ where $2^m = N^\beta$ is known. We have

$$\psi(N) = (p^2 + p + 1)(q^2 + q + 1) = (p + q)^2 + (N + 1)(p + q) + N^2 - N + 1.$$

Let $v_0 \equiv 2u_0 + (N - u_0^2)u_0^{-1} \pmod{2^{2m}}$, where u_0 is a solution of the equation $z^2 \equiv N \pmod{2^m}$. Using Lemma 2, we rewrite $\psi(N)$ as follows,

$$\begin{aligned} \psi(N) &= (2^{2m}v + v_0)^2 + (N + 1)(2^{2m}v + v_0) + N^2 - N + 1 \\ &= 2^{4m}v^2 + 2^{2m}(N + 2v_0 + 1)v + v_0^2 + (N + 1)v_0 + N^2 - N + 1. \end{aligned} \tag{4}$$

Transforming $ed - k\psi(N) = 1$ into the modular equation $k\psi(N) + 1 \equiv 0 \pmod{e}$ and substituting the value of $\psi(N)$ from (4),

$$k(2^{4m}v^2 + 2^{2m}(N + 2v_0 + 1)v + v_0^2 + (N + 1)v_0 + N^2 - N + 1) + 1 \equiv 0 \pmod{e}. \tag{5}$$

Since e is odd, (5) can be rewritten as

$$k\left(v^2 + \frac{N + 2v_0 + 1}{2^{2m}}v + \frac{v_0^2 + (N+1)v_0 + N^2 - N + 1}{2^{4m}}\right) + \frac{1}{2^{4m}} \equiv 0 \pmod{e}. \tag{6}$$

We reconstruct (6) into $f(x_1, x_2) = x_1(x_2^2 + ax_2 + b) + c$ where

$$\begin{aligned} a &\equiv \frac{N + 2v_0 + 1}{2^{2m}} \pmod{e}, \\ b &\equiv \frac{v_0^2 + (N+1)v_0 + N^2 - N + 1}{2^{4m}} \pmod{e}, \\ c &\equiv \frac{1}{2^{4m}} \pmod{e}, \end{aligned}$$

Then $(x_1, x_2) = (k, v)$ is a solution of the polynomial modular equation $f(x_1, x_2) \equiv 0 \pmod{e}$. We then apply Theorem 3 to solve for the roots x_1 and x_2. Let $e = N^\alpha$, $d = N^\delta$. Since $\psi(N) > p^2q^2 = N^2$, then

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

Next, let $2^m = N^\beta$. We have $p+q = 2^{2m}v + v_0$ with $v_0 < 2^{2m}$ and $2N^{\frac{1}{2}} < p+q < 3N^{\frac{1}{2}}$ by Lemma 2 and Lemma 1 respectively . Then

$$v = \frac{p+q-v_0}{2^{2m}} < 3N^{\frac{1}{2}-2\beta}.$$

We set

$$X_1 = [N^{\alpha+\delta-2}], X_2 = [3N^{\frac{1}{2}-2\beta}].$$

We apply Theorem 3 with $\delta_1 = \alpha+\delta-2$ and $\delta_2 = \frac{1}{2}-2\beta$. First, the optimal value for τ_0 becomes

$$\tau_0 = \frac{1+4\beta-\delta}{1-4\beta}.$$

Second, from the condition of Theorem 3, we get

$$\delta < \frac{7}{3} - \frac{4}{3}\beta - \frac{2}{3}\sqrt{(1-4\beta)(3\alpha+1-4\beta)}.$$

Then, under this condition, we will find the solution (k,v). These values are then used to compute $p+q = 2^{2m}v + v_0$. Combining it with $pq = N$, we retrieve p, q, and factor the RSA modulus. Observe that, since $p+q < 3N^{\frac{1}{2}}$, then $2^{2m}v + v_0 < 3N^{\frac{1}{2}}$, and, since $2^{2m} = N^{2\beta}$, we get $2\beta < \frac{1}{2}$, that is $\beta < \frac{1}{4}$. This shows that the bound on δ is valid for all β.

Notice that in a random situation, if the primes of the modulus $N = pq$ share only a small number of LSBs, we have $p+q = 2^{2m}v + u_0$ with $2^m = N^\beta$ and $\beta \approx 0$. Then the condition on δ in Theorem 4 becomes $\delta < \frac{7}{3} - \frac{2}{3}\sqrt{3\alpha+1}$. This retrieves the bound in [11].

6. Numerical Analysis

This section describes our experiments to check the validity of our new attack on the cubic Pell RSA variant. The steps of the experiments are as follows.

- An integer n is chose up to 512.
- An integer $n_0 \leq \frac{n}{5}$ is chose and an odd random number u_0 of n_0 bits is generated.
- An integer $m_0 \leq \frac{n}{7}$ is chose, and a random prime number p of the form $p = 2^{m_0}p_1 + u_0$ having n bits is generated.
- A random prime number q of the form $q = 2^{m_0}q_1 + u_0$ having n bits is generated.

- The modulus $N = pq$ and $\psi(N) = (p^2 + p + 1)(q^2 + q + 1)$ are computed. This implies the following estimations
$$N \approx 2^{2n}, 2^{m_0} \approx N^{\beta}, \beta = \frac{m_0}{2n}.$$
- A random integer $d \approx N^{\delta}$ is chose satisfying $\gcd(d, \psi(N)$ where δ satisfies the condition of Theorem 4 with $\alpha \approx 2,$ that is
$$\delta < \frac{7}{3} - \frac{4}{3}\beta - \frac{2}{3}\sqrt{(1-4\beta)(7-4\beta)}.$$
- The public key $e \equiv \frac{1}{d} (\mathrm{mod}\, \psi(N))$ is computed. If e is even, the value of d will be increased in the former step.
- The methods described in Theorem 4 is applied to find p and q.

The following numerical example is generated using large numbers and the steps are shown in detail.

$n = 512, n_0 = \left\lfloor \frac{n}{6} \right\rfloor = 85, m_0 = \left\lfloor \frac{n}{7} \right\rfloor = 73,$

$u_0 = 313606196852762878431267 91,$

$N = 80146987079285381126059233088741332009003020030762492883$
$041188350336305183708963224367744964556613213893580339 82$
$056661841130360569104030734444756430498508397429209412 17$
$679754038032381419526208878559797929560614125982119077 70$
$031084286196467856396222631205578377178236348519226191 51$
$024541416166404560330596459 3,$

$e = 220469490790040135741786080407220592352543411154123084 36$
$627015212973221267287093965373975629948822150703858125 61$
$087974411602037395969808609626450532367867926665028497 32$
$145064751950539301530551312480000889922652984489745046 91$
$958178481532844551777685690737608230770021850745529781 98$
$025826539152400608111028876261870293163285672459620087 13$
$533798112470032147713783802462448858735517748009771195 76$
$911996976626705632139395915606952028682001880086100671 71$
$616988392224194674919183343178811563013774542836637054 12$
$325120476654362834154139560400360901886585792564050532 80$
$599413060031763832447266419293228146476067686882039603 29,$

$$
\begin{aligned}
v_0 &\equiv 2u_0 + (N - u_0^2)u_0^{-1} (\mathrm{mod}\, 2^{2m_0}) \\
&= 80222982022227665022322349812196897896438798, \\
\delta &= 0.611273, \alpha = 1.99849, \beta = 0.07137, m = 5, t = 4, \omega = 60,
\end{aligned}
$$

$$
\begin{aligned}
X &= \left\lfloor N^{\alpha+\delta-2} \right\rfloor \\
&= 56027077752546643521638030535718188939172145873082777950 \\
&\quad 70174334818935985459289761436866210307181819006705036408 \\
&\quad 90770419263722211580683747548508711327313525150866795120 \\
&\quad 95454336785713684510, \\
Y &= 3\left\lfloor N^{\frac{1}{2}-2\beta} \right\rfloor \\
&= 30107816035492760215294704195259837167730439318993619276 \\
&\quad 58139567913250510994334729522762079338809465243894567 10.
\end{aligned}
$$

The next step is to apply the method described in Theorem 4 to the polynomial modular equation $x_1(x_2^2 + ax_2 + b)c \equiv 0 \pmod{e}$ which yield

$$
\begin{aligned}
x_1 = k = {} & 56092776617213969149376278097471666290790435416688826 \\
& 71844290645995413302576529276196714105009513106450251 \\
& 50345680449384923629295695290302264152271836046276357 \\
& 25260840458255389858497686701, \\
x_2 = v = {} & 20366195036763489658896318021555281201393584283637525 \\
& 73950790650094111225767483169019797568576285322419471 \\
& 96224.
\end{aligned}
$$

The values of p and q are obtained by generating then solving the quadratic equation using the knowledge of $p + q = 2^{2m_0} v + v_0$, and $N = pq$,

$$
\begin{aligned}
p = {} & 10621574422685639932609108809772202578944908243791912 08 \\
& 78618989023019218745596041371909599288546898461536722 91 \\
& 00963705389413508646499221830782963379229850 3, \\
q = {} & 75456786244520240619465439214885554467883265367155703 21 \\
& 90928812375540104321393174664239375826172301253475599 93 \\
& 87034901642460373177429524579742701916737031.
\end{aligned}
$$

Then, the exponent d can be retrieved by using e, and $\psi(N)$,

$$\begin{aligned} d &\equiv \frac{1}{e} (\mathrm{mod}\, \psi(N)) \\ &= 163430398963312031868937683466744955952743951178563660480741469097219166989216776945895101506090648761552026061204868579259382336367709628894624074381484883245574461441067694208638956306990. \end{aligned}$$

The running time for the reduction of the basis of the lattice by the the LLL algorithm took 163582 seconds, and the Gröbner basis method took 2.266 seconds. Observe that the method of [16] can retrieve p and q only if $\delta < 2 - \sqrt{\alpha}$ where $d = N^{\delta}$, and $e = N^{\alpha}$. In our example, we have $\delta = 0.611273$, and $\alpha = 1.99849$. Then $2 - \sqrt{\alpha} \approx 0.58632$, and δ is much larger than $2 - \sqrt{\alpha}$. This shows that the method of [16] can not retrieve p and q in this example.

7. Conclusion

An RSA variant scheme has been constructed by Murru and Saettone based on the arithmetic generated by a cubic Pell equation, with the hope that it is going to be more secure in comparison to a original RSA in any applications that require data transmission. The authors of this cubic Pell RSA variant thought that common attacks on a standard RSA will not be applicable. Unfortunately, this cubic Pell RSA variant has been shown to hardly spar better on a larger order at the expense of higher computing requirement. A smaller exponent may be opted to gain a faster power modulo operations. This option has been shown to weaken the security level of the cubic Pell RSA variant worse than expected under common attacks on standard RSA. Moreover, sharing some LSBs between prime factors is another practical option. In this paper, we showed that this option, coupled with an efficient small private exponent will only further extend an insecure bound much higher on a private exponent d from previous bounds.

References

[1] Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$, Advances in Cryptology-Eurocrypt'99, Lecture Notes in Computer Science 1592, pp. 1-11, Springer, Berlin, Heidelberg, (1999). 10.1007/3-540-48910-X_1

[2] Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology*, 10(4), 233-260, (1997)

[3] Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited, In: IMA International Conference on Cryptography and Coding, LNCS 1355, pp. 131-142, Springer, Berlin, Heidelberg (1997). 10.1007/BFb0024458.

[4] Jochemsz, E., May, A.: A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants, In: ASIACRYPT 2006, LNCS 4284, pp. 267-282, Springer-Verlag (2006). 10.1007/11935230_18.

[5] Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients, *Mathematische Annalen*, 261, pp. 513-534, (1982).

[6] May, A.: New RSA Vulnerabilities Using Lattice Reduction Methods. PhD thesis, University of Paderborn, Germany (2003).

[7] Murru N., Saettone F.M.: A novel rsa-like cryptosystem based on a generalization of the rédei rational functions. In: Kaczorowski J., Pieprzyk J., Pomykala J. (eds) Number-Theoretic Methods in Cryptology. NuTMiC 2017. Lecture Notes in Computer Science, 10737 pp. 91-103, Springer, Cham, (2018) . 10.1007/978-3-319-76620-1_6.

[8] Nitaj, A.: Another generalization of Wiener's attack on RSA, In: Vaudenay, S. (Ed.) Africacrypt 2008. LNCS, 5023, pp. 174-190. Springer, Heidelberg (2008). 10.1007/978-3-540-68164-9_12.

[9] Nitaj, A., Arrifin, M.R.K., D.I. Nassr, Bahig, H.M.: New attacks on the RSA cryptosystem, in D. Pointcheval and D. Vergnaud (Eds.): AFRICACRYPT 2014, LNCS 8469, pp. 178-198, Springer (2014).

[10] Nitaj, A., Arrifin, M.R.K., Adenan, N.N.H., Abu, N.A.: Classical attacks on a variant of the RSA cryptosystem, LATINCRYPT 2021, pp.151-167, Springer (2021).

[11] Nitaj, A., Arrifin, M.R.K., Adenan, N.N.H., Lau, T.S.C., Chen, J.: Security issues of novel RSA variant, IEEE Access, 10, 53788-53796, (2002).

[12] Rivest, R., Shamir, A., Adleman, L.: A Method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM,21(2), 120-126 (1978).

[13] Steinfeld, R., Zheng, Y.: On the security of RSA with primes sharing least-significant bits. Appl. Algebra Eng. Commun. Comput. 15(3-4), 179-200 (2004).

[14] Sun, H.M., Wu, M.E., Steinfeld, R., Guo, J., Wang, H.: Cryptanalysis of short exponent RSA with primes sharing least significant bits. in MK Franklin, LCK Hui & DS Wong (eds), Cryptology and Network Security - 7th International Conference, CANS 2008, Proceedings. vol. 5339 LNCS, Lecture Notes in Computer Science (2008).

[15] Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory,36(3), 553-558 (1990).

[16] Zheng, M., Kunihiro, N., Yao, Y: Cryptanalysis of the RSA variant based on cubic Pell equation, Theoretical Computer Science, 889, 135-144, (2021).

Received June, 2022