A New Public Key Cryptosystem Based on the Cubic Pell Curve

Michel Seck[1] and Abderrahmane Nitaj[2(✉)]

[1] Ecole Polytechnique de Thies, LTISI, Senegal
mseck@ept.sn
[2] Normandie Univ, UNICAEN, CNRS, LMNO, 14000 Caen, France
abderrahmane.nitaj@unicaen.fr

Abstract. Since its invention in 1978 by Rivest, Shamir and Adleman, the public key cryptosystem RSA has become a widely popular and a widely useful scheme in cryptography. Its security is related to the difficulty of factoring large integers which are the product of two large prime numbers. For various reasons, several variants of RSA have been proposed, and some have different arithmetics such as elliptic and singular cubic curves. In 2018, Murru and Saettone proposed another variant of RSA based on the cubic Pell curve with a modulus of the form $N = pq$. In this paper, we present a new public key cryptosystem based on the arithmetic of the cubic Pell curve with a modulus of the form $N = p^r q^s$. Its security is based on the hardness of factoring composite integers, and on Rabin's trapdoor one way function. In the new scheme, the arithmetic operations are performed on a cubic Pell curve which is known only to the sender and the recipient of a plaintext.

Keywords: Public Key Cryptography, Cubic Pell curve, RSA, KMOV, Rabin's trapdoor

1 Introduction

The RSA cryptosystem is one of the earliest and most popular public key encryption schemes. It was proposed by Rivest, Shamir, and Adleman in 1978 [RSA78] after the introduction of the concept of a trapdoor one-way function by Diffie and Hellman in 1976 [DH76]. In RSA, to generate a public key $\mathcal{PK}$ and a private key $\mathcal{SK}$, the following steps are taken. First, two prime numbers, p and q, are generated, and the modulus N is computed as $N = pq$. An element e in $\mathbb{Z}/N\mathbb{Z}$ is then chosen such that it is coprime with $\phi(N) = (p-1)(q-1)$, where ϕ is the Euler function. Next, the private exponent $d = e^{-1} \pmod{\phi(N)}$ is computed. The public key is $\mathcal{PK} = (N, e)$, and the private key is $\mathcal{SK} = (N, d)$. To encrypt a message $m \in \mathbb{Z}/N\mathbb{Z}$ with the public key $\mathcal{PK} = (N, e)$, the ciphertext $c \equiv m^e \pmod{N}$ is computed. To decrypt the ciphertext c using the private key $\mathcal{SK} = (N, d)$, the original message is obtained as $m \equiv c^d \pmod{N}$.

In 1979 Rabin [Rab79,Wil85] published a public-key encryption scheme similar to RSA whose security is also related to factoring composite integers. It is

known that breaking the Rabin scheme is equivalent to factoring N while for RSA this equivalence is not proven. For Rabin encryption scheme, to generate a public key $\mathcal{PK}$ and a private key $\mathcal{SK}$, one first generates two primes p and q such that $p, q \equiv 3 \pmod 4$, and computes the modulus $N = pq$. The public key is $\mathcal{PK} = N$ and the private key is $\mathcal{SK} = (p, q)$. To encrypt a message m, one computes $C \equiv m^2 \pmod N$. For the decryption of C, one proceeds as follows. First, solve the equation $X^2 = C \pmod p$ and $X^2 = C \pmod q$. By the Chinese Remainder Theorem, this leads to four solutions which include the plaintext.

Certain vulnerabilities of RSA are know for particular choices of the prime factors p, q, the public exponent e, and the private exponent d [Wie90,Nit08,Bon99], [BDF98,BDHG99,BD99,Cop97,dW02,TC23]. For example, when $p < q < 2p$, and d is too small with respect to N such as $d < \frac{1}{3}N^{0.25}$, one can use Wiener's attack [Wie90,Nit08] to efficiently recover the secrete d. It is shown that RSA with a low public exponent e, e.g. $e = 3$, is vulnerable to Håstad's broadcast attack[Hås86,Bon99]. When $d < N^{0.292}$, the RSA modulus N can be factored in polynomial time [BD99] using Coppersmith's method [Cop97] which is based on lattice reduction techniques, especially the by the LLL algorithm [LLL82].

Some RSA-like cryptosystems have been also proposed over non-singular and singular curves when certain groups or rings can be defined. In 1991, Koyama, Maurer, Okamoto, and Vanstone [KMOV91] proposed a variant of RSA based on elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ when $N = pq$ is the product of two primes with $p, q \equiv 2 \pmod 3$. This variant is known as KMOV. In KMOV, to generate a public key $\mathcal{PK}$ and a private key $\mathcal{SK}$, one first generates two primes p and q such that $p, q \equiv 2 \pmod 3$, and computes the modulus $N = pq$ as in RSA. Then, one chooses an exponent e that is invertible modulo $\psi(N) = \text{lcm}(p + 1, q + 1)$ and computes $d = e^{-1} \pmod{\psi(N)}$. The public key is $\mathcal{PK} = (N, e)$, and the private key is $\mathcal{SK} = (N, d)$. To encrypt a message $m = (x_m, y_m) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ with the public key $\mathcal{PK}$, one first computes $b \equiv y_m^2 - x_m^3 \pmod N$, and then the ciphertext $c = e(x_m, y_m)$ on the elliptic curve $E_b : y^2 = x^3 + b$ over the ring $\mathbb{Z}/N\mathbb{Z}$. To decrypt the ciphertext $c = (x_c, y_c)$ with the private key $\mathcal{SK}$, one computes $b \equiv y_c^2 - x_c^3 \pmod N$, and then $m = d(x_c, y_c)$ on the elliptic curve $E_b : y^2 = x^3 + b$. Note that the condition $p, q \equiv 2 \pmod 3$ ensures that the supersingular elliptic curve $E_b : y^2 = x^3 + b$ has order $p + 1$ modulo p and order $q + 1$ modulo q. This guarantee the correctness of the decryption phase in KMOV.

Another RSA variant over elliptic curves was proposed by Demytko [Dem94] in 1993. Since then, several variants of KMOV and Demytko constructions have been proposed in the last decades with an RSA modulus $N = pq$. One was proposed by Koyama [Koy95] based on the singular cubic curve $y^2 + axy = x^3 \pmod N$, a second one was proposed in 1995 by Kuwakado, Koyama, and Tsuruoka [KKT95] based on the singular cubic curve $y^2 \equiv x^3 + bx^2 \pmod N$, and a third one was proposed in 2018 by Murru and Saettone [MS18] using the cubic Pell curve $C_r : x^3 + ry^3 + r^2z^3 - 3rxyz \equiv 1 \pmod N$.

Several variants of the RSA cryptosystem have been proposed where the modulus is of a different shape. A first variant was proposed by Takagi in

1998 with a modulus of the form $N = p^k q$. In 1998, Okamoto, Uchiyama, and Fujisaki [OU98] proposed EPOC and ESIGN Algorithms [OUF98], where the modulus is of the form $N = p^2 q$. The same modulus was used by Schmidt-Samoa [SS06] in 2005 to design a trapdoor one-way permutation. In 2000, Lim, Kim, Yie and Lee [LKYL00] proposed a variant of RSA where the modulus is a multi-prime power integer of the form $N = p^r q^s$ with $r, s \geq 1$. Two more variants based on elliptic curves and Edwards curves were proposed by Boudabra and Nitaj [BN17,BN19] with a multi-power modulus $N = p^r q^s$.

Contributions : In this paper, we study the arithmetic of cubic Pell curves $\mathcal{PC}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz = 1$ over $\mathbb{Z}/N\mathbb{Z}$ where $N = p^r q^s$ is a multi-prime power integer, and propose a new scheme. We summarize our contributions as follows.

- We present a detailed study of the cubic Pell curves with the equation $\mathcal{PC}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz = 1$, specifically regarding the number of solutions modulo p^r, q^s, and $N = p^r q^s$.
- We propose a new scheme using the arithmetic of the cubic Pell curve $\mathcal{PC}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz = 1$ over $\mathbb{Z}/N\mathbb{Z}$ where $N = p^r q^s$, and study its security.

  The new scheme works as follows.

  1. The public parameters in the new scheme are a prime power modulus $N = p^r q^s$, and a public exponent e.
  2. To encrypt a message M with the new scheme, one represents it as $(x_M, y_M, 0)$, and then computes $a \equiv \frac{1-x_M^3}{y_M^3} \pmod N$, and $(x_C, y_C, z_C) = e \otimes (x_M, y_M, 0)$ on the cubic Pell curve $\mathcal{PC}_a(N) : x^3+ay^3+a^2z^3-3axyz = 1$ over $\mathbb{Z}/N\mathbb{Z}$.
  3. To decrypt a ciphertext $(x_C, y_C, z_C) \in \mathcal{PC}_a(N)$, one first find a solution a of the quadratic equation $x_C^3 + ay_C^3 + a^2z_C^3 - 3ax_Cy_Cz_C - 1 \equiv 0 \pmod N$. Then, one computes $d = e^{-1} \pmod{|\mathcal{PC}_a(N)|}$, and $(x_D, y_D, z_D) = d \otimes (x_C, y_C, z_C)$ on the cubic Pell curve $\mathcal{PC}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz = 1$ over $\mathbb{Z}/N\mathbb{Z}$. Then, one of the values a leads to the plaintext $(x_D, y_D, z_D) = (x_M, y_M, 0)$.

     Since the modular equation $x_C^3 + ay_C^3 + a^2z_C^3 - 3ax_Cy_Cz_C - 1 \equiv 0 \pmod N$ has four solutions a_i, $i = 1, 2, 3, 4$, then there are four decryption exponents d_i, $i = 1, 2, 3, 4$, and four potential plaintexts $(x_i, y_i, z_i) = d_i \otimes (x_C, y_C, z_C)$. One of these plaintexts is the original one $(x_M, y_M, 0)$. For the other plaintexts, we do not know if $z_i = 0$ for one of them. We show that this scenario has negligible probability. We have extensively experimented our scheme. In all cases, the decryption performed correctly and uniquely.

  Any attack should start by trying to find the solutions of the quadratic equation $x_C^3 + ay_C^3 + a^2z_C^3 - 3ax_Cy_Cz_C - 1 \equiv 0 \pmod N$. This is known to be equivalent to factoring as in Rabin's scheme [Rab79]. To our knowledge, the new scheme is the first KMOV-like public key encryption scheme that has

this additional property. A proof of concept implementation of our scheme with SimulaMath [Sim23] and SageMath [Sag23] is provided in [Sec23]. We note that the decryption protocol in our scheme has negligible failure.

Paper Organization : The rest of this paper is organized as follows. In Section 2, we review essential concepts related to curves over finite fields and the ring $\mathbb{Z}/N\mathbb{Z}$, focusing on the cubic Pell curves. In Section 3, we investigate the properties of the cubic Pell curve over $\mathbb{Z}/N\mathbb{Z}$ where $N = p^r q^s$ is a product of two distinct prime powers. Our public key encryption scheme is presented in Section 4. In Section 5, we provide a security analysis of our scheme by examining different attacks. We conclude the paper in Section 6.

2 Preliminaries

In this section, we begin by revisiting some useful definitions and properties associated with quadratic residues modulo a prime p and cubic residues modulo an integer n. Additionally, we recapitulate key properties concerning the arithmetic of the cubic Pell curve, which serves as a generalization of the traditional Pell curve in the cubic setting. And finally, we recall the Chinese remainder theorem, the Hensel lemma and some properties related to the number of solution of multivariate polynomial functions overs the set of integers modulo prime power.

2.1 Quadratic and cubic residue modulo prime powers

Definition 1 (quadratic residue). *Let p be a prime number and r a positive integer. An integer a is a quadratic residue modulo p^r if the equation $x^2 \equiv a \pmod{p^r}$ has at least one solution, otherwise, a is a quadratic non-residue modulo p^r.*

Definition 2 (cubic residue). *Let p be a prime number. An integer a is a cubic residue modulo p if the equation $x^3 \equiv a \pmod{p}$ has at least one solution, otherwise, a is a cubic non-residue modulo p.*

Notice that when $p \equiv 1 \pmod 3$, there are $(p-1)/3$ non-zero cubic residues modulo p, and when $p \not\equiv 1 \pmod 3$, every element in $\mathbb{Z}/p\mathbb{Z}$ is a cubic residue modulo p.

Theorem 1 ([Ros93]). *The equation $x^k \equiv a \pmod{p}$ has a solution if and only if $a^{(p-1)/d} \equiv 1 \pmod{p}$, where $d = \gcd(k, p-1)$. If the congruence has a solution, then it has d incongruent solutions modulo p.*

Corollary 1. *Let $p \geq 3$ be a prime number.*

1. *An integer a is a quadratic residue modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.*
2. *An integer a is a cubic residue modulo p if and only if $a^{(p-1)/\gcd(3,p-1)} \equiv 1 \pmod{p}$.*

The Euler totient function ϕ is defined by $\phi(p^r) = p^{r-1}(p-1)$ if p is a prime number, and satisfies $\phi(mn) = \phi(m)\phi(n)$ if $\gcd(m,n) = 1$.

Theorem 2 ([Ros93]). *Let n be a positive integer with a primitive root. If k is a positive integer and a is an integer relatively prime to n, then the congruence $x^k \equiv a \pmod{n}$ has a solution if and only if*

$$a^{\phi(n)/d} \equiv 1 \pmod{n}$$

where $d = \gcd(k, \phi(n))$. If the congruence has a solution, then it has d incongruent solutions modulo n.

2.2 The cubic Pell curve over a field

Let $\mathbb{F}$ be a field and let $a \in \mathbb{F}$. Define the quotient ring $R_a = \mathbb{F}[t]/\left(t^3 - a\right)$. Note that R_a is a field if a is a cube non-residue in $\mathbb{F}$. An element $w \in R_a$ can be written as $w = x + yt + zt^2$ for some $(x, y, z) \in \mathbb{F}^3$. Let $w_1 = x_1 + y_1 t + z_1 t^2$ and $w_2 = x_2 + y_2 t + z_2 t^2$ be two elements of R_a. The product $w_1 \cdot w_2$ is defined by

$$w_1 \cdot w_2 = [x_1x_2 + a(y_2z_1 + y_1z_2)] + [x_2y_1 + x_1y_2 + az_1z_2]t + [y_1y_2 + x_2z_1 + x_1z_2]t^2.$$

The norm of $w = x + yt + zt^2$ is given by $N_a(w) = x^3 + ay^3 + a^2z^3 - 3axyz$ (see [Bar03]). Consider the set $\mathcal{U}_a$ of unitary elements defined as

$$\mathcal{U}_a = \left\{x + yt + zt^2 \in R_a : x^3 + ay^3 + a^2z^3 - 3axyz = 1\right\},$$

and consider the cubic Pell curve over $\mathbb{F}$

$$P_a^3 = \left\{(x, y, z) \in \mathbb{F}^3 : x^3 + ay^3 + a^2z^3 - 3axyz = 1\right\}.$$

The natural product on $\mathcal{U}_a$ induces the generalized Brahmagupta product $\oplus$ defined as follows.

$$w_1 \oplus w_2 = (x_1x_2 + a(y_2z_1 + y_1z_2), x_2y_1 + x_1y_2 + az_1z_2, y_1y_2 + x_2z_1 + x_1z_2),$$

where $w_1 = (x_1, y_1, z_1) \in P_a^3$ and $w_2 = (x_2, y_2, z_2) \in P_a^3$. Notice that $(P_a^3, \oplus)$ is a group with neutral element $(1, 0, 0)$, and the inverse of $w = (x, y, z)$ is given by $w^{-1} = (x^2 - ayz, az^2 - xy, y^2 - xz)$.

2.3 Curves over the ring $\mathbb{Z}/N\mathbb{Z}$

Definition 3. *Let $F(x_1, x_2, \ldots, x_k)$ be a polynomial in k variables with integer coefficients, and N a positive integer. A solution $(a_1, a_2, \ldots, a_k)$ of the modular equation $F(x_1, x_2, \ldots, x_k) \equiv 0 \pmod{N}$ is said to be singular modulo N if it satisfies*

$$\frac{\partial F}{\partial x_1}(a_1, a_2, \ldots, a_k) = 0, \ \ldots, \ \frac{\partial F}{\partial x_k}(a_1, a_2, \ldots, a_k) = 0.$$

If the equation $F(x_1, x_2, \ldots, x_k) \equiv 0 \pmod N$ has only non-singular solutions, the curve is non-singular. We denote by c_N the number of solutions of the equation $F(x_1, x_2, \ldots, x_k) \equiv 0 \pmod N$, and by s_N the number of singular solutions. The number of non-singular or regular solutions is $R_N = c_N - s_N$.

The following result is useful to count the number of solutions of the equation $F(x_1, x_2, \ldots, x_k) \equiv 0 \pmod N$.

Theorem 3 ([BN17]). *Let $F(t_1, \ldots, t_k) \in \mathbb{Z}[t_1, \ldots, t_k]$ be a polynomial. Consider the curve*

$$F(t_1, \ldots, t_k) \equiv 0 \pmod{p^r},$$

Then $R_{p^r} = p^{(k-1)(r-1)} R_p$. Moreover, if the curve $F(t_1, \ldots, t_k)$ is non-singular, then $c_{p^r} = p^{(k-1)(r-1)} c_p$.

Theorem 4 ([BN17]). *Let p^r and q^s be two prime power integers with $\gcd(p, q) = 1$. Then*

$$c_{p^r \cdot q^s} = c_{p^r} \cdot c_{q^s}$$

2.4 Chinese Remainder Theorem and Hensel Lemma

The Chinese Remainder Theorem is often used to solve systems of equations modulo a composite number with known factorisation.

Theorem 5 (Chinese Remainder Theorem [DPS96]). *Let n_i, $i = 1, 2, \ldots, m$ be m pairwise relatively prime numbers. For any set of integers a_i, $i = 1, 2, \ldots, m$, the system of congruences*

$$x \equiv a_i \pmod{n_i}, \quad i = 1, 2, \ldots, m, \tag{1}$$

has exactly one solution modulo $N = \prod_{i=1}^{m} n_i$.

The following algorithm gives the details in the Chinese Remainder Algorithm to determine the unique solution of the Equation (1) modulo $N = \prod_{i=1}^{m} n_i$.

Algorithm 1 Chinese Remainder Algorithm

Input: m, a_i, n_i for $i = 1, 2, \ldots, m$.
Output: The unique solution X modulo $N = \prod_{i=1}^{m} n_i$ of Equation (1).

1: Compute $N_k = \prod_{i=1, i \neq k}^{m} n_i$ for $k = 1, 2, \ldots, m$.
2: Compute $X_i = N_i^{-1} \pmod{n_i}$ for $i = 1, 2, \ldots, m$.
3: Compute $X = \sum_{i=1}^{m} a_i X_i N_i \pmod N$.
4: Return X.

The following result is a simple application of Theorem 5.

Corollary 2. *Let p^r and q^s be two prime powers with $p \neq q$, and $N = p^r q^s$. Let a_p and a_q be integers. The unique solution to the system*

$$x = a_p \pmod{p^r}, \quad x = a_q \pmod{q^s},$$

is given by

$$X = a_p \times q^s \times [(q^s)^{-1} \bmod p^r] + a_q \times p^r \times [(p^r)^{-1} \bmod q^s] \pmod{N}.$$

Hensel's Lemma is useful to find a solution of a polynomial equation modulo a prime power p^r when a solution modulo p is known.

Lemma 1 (Hensel's lemma, [Gal12]). *Let p be a prime number. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial and $f'(x)$ its derivative. If there exists an integer $r_1 \in \mathbb{Z}/p\mathbb{Z}$ such that $f(r_1) \equiv 0 \pmod{p}$ and $f'(r_1) \not\equiv 0 \pmod{p}$, then there exists a unique sequence $(r_n)_{n\geq 1}$ of integers satisfying for all $n \geq 1$*

- $r_n \equiv r_1 \pmod{p}$,
- $f(r_n) \equiv 0 \pmod{p^n}$

Moreover, for $n \geq 2$, r_n is given by

$$r_n = r_{n-1} - \frac{f(r_{n-1})}{f'(r_{n-1})} \pmod{p^n},$$

A possible application of Hensel's lemma is the following result which concerns the solutions of the quadratic equation $ax^2 + bx + c \equiv 0 \pmod{p}$.

Corollary 3 (Quadratic equation). *Let a, b, c be integers et p an odd prime numbers. Suppose that $\gcd(a, p) = 1$ and $\Delta = b^2 - 4ac \neq 0 \pmod{p}$. If Δ is a quadratic residue modulo p, then, for $n \geq 1$, the equation $ax^2 + bx + c \equiv 0 \pmod{p^n}$ has two roots y_n and z_n, recursively defined by*

$$\begin{aligned}
y_1 &= \frac{-b + \sqrt{\Delta}}{2a} \pmod{p}, \\
z_1 &= \frac{-b - \sqrt{\Delta}}{2a} \pmod{p}, \\
y_{n+1} &= y_n - \frac{ay_n^2 + by_n + c}{2ay_n + b} \pmod{p^{n+1}}, \\
z_{n+1} &= z_n - \frac{az_n^2 + bz_n + c}{2az_n + b} \pmod{p^{n+1}}.
\end{aligned}$$

Notice that if $p \equiv 3 \pmod{4}$ and Δ is a quadratic residue modulo p, then

$$\sqrt{\Delta} \equiv \pm \Delta^{\frac{p+1}{4}} \pmod{p}.$$

In the case of $p \equiv 1 \pmod{4}$, one can use the Tonelli-Shank algorithm [Zeu19] to compute the square roots of Δ modulo p.

3 The Cubic Pell Curve over the Ring $\mathbb{Z}/N\mathbb{Z}$ with $N = p^r q^s$

Let $N = p^r q^s$ where p and q are two different prime numbers, and r and s are positive integers. Let $a \in Z/NZ\backslash\{0\}$. In this section, we study the properties of the cubic Pell curve with the equation

$$x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod{N}.$$

The generalized Brahmagupta product $\oplus$ defined in Section 2.2 works perfectly for two solutions of the cubic Pell curve modulo N. Moreover, for a positive integer n, we define the scalar multiplication of a solution (x, y, z) by n as follows

$$n \otimes (x, y, z) = (x, y, z) \oplus \cdots \oplus (x, y, z) \quad (n \text{ times}).$$

Proposition 1. *Let $N > 3$ be an integer, and $a \in \mathbb{Z}/N\mathbb{Z}$. The cubic Pell curve*

$$\mathcal{PC}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod{N},$$

is nonsingular.

Proof. Let $F(x, y, z) = x^3 + ay^3 + a^2z^3 - 3axyz - 1$. Consider the system of equations modulo N,

$$F(x, y, z) \equiv 0,\ \frac{\partial F}{\partial x}(x, y, z) \equiv 0,\ \frac{\partial F}{\partial y}(x, y, z) \equiv 0,\ \frac{\partial F}{\partial z}(x, y, z) \equiv 0, \tag{2}$$

that is

$$\begin{cases} x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod{N} \\ 3x^2 - 3ayz \equiv 0 \pmod{N}, \\ 3ay^2 - 3axz \equiv 0 \pmod{N}, \\ 3a^2z^2 - 3axy \equiv 0 \pmod{N}, \end{cases}$$

This implies that

$$\begin{cases} 3x^3 - 3axyz \equiv 0 \pmod{N}, \\ 3ay^3 - 3axyz \equiv 0 \pmod{N}, \\ 3a^2z^3 - 3axyz \equiv 0 \pmod{N}, \end{cases}$$

Summing the three sides, we get

$$3\left(x^3 + ay^3 + a^2z^3 - 3axyz\right) \equiv 0 \pmod{N}.$$

Since $x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod{N}$, then $3 \equiv 0 \pmod{N}$, which is impossible. Hence the system (2) has no solution and the cubic Pell curve is nonsingular. □

For a prime power p^r and $a \in \mathbb{Z}/p^r\mathbb{Z}$, let $\mathcal{PC}_a(p^r)$ be the set of the solutions of the cubic Pell curve

$$x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod{p^r}.$$

The proof of the following result can found in [DM22].

Lemma 2. *Let p be a prime number with $p \equiv 1 \pmod 3$. Let a be an integer with $\gcd(a,p)=1$. The cardinality of $\mathcal{PC}_a(p)$ is*

$$|\mathcal{PC}_a(p)| = \begin{cases} p^2+p+1 & \text{if } a \text{ is a cube non-residue modulo } p, \\ (p-1)^2 & \text{if } a \text{ is a non-zero cube residue modulo } p. \end{cases}$$

When $r \geq 2$, we have the following result.

Lemma 3. *Let p^r be a prime power with $p \equiv 1 \pmod 3$, and $r \geq 1$. Let $a \in \mathbb{Z}/p^r\mathbb{Z}$ with $\gcd(a,p)=1$. The cardinality of $\mathcal{PC}_a(p^r)$ is*

$$|\mathcal{PC}_a(p^r)| = \begin{cases} p^{2(r-1)}\left(p^2+p+1\right) & \text{if } a \text{ is a cubic non residue modulo } p, \\ p^{2(r-1)}(p-1)^2 & \text{if } a \text{ is a cubic residue modulo } p. \end{cases}$$

Proof. Suppose that p is a prime number such that $p \equiv 1 \pmod 3$ and let a be an integer with $\gcd(a,p)=1$. By Proposition 1, the curve $x^3+ay^3+a^2z^3-3axyz \equiv 1 \pmod{p^r}$ is non-singular. Therefore, by applying Lemma 3 with $k=3$, we get

$$|\mathcal{PC}_a(p^r)| = p^{(3-1)(r-1)}|\mathcal{PC}_a(p)| = p^{2(r-1)}|\mathcal{PC}_a(p)|.$$

Combining with Lemma 2, we get

$$|\mathcal{PC}_a(p^r)| = \begin{cases} p^{2(r-1)}\left(p^2+p+1\right) & \text{if } a \text{ is a cubic non residue modulo } p, \\ p^{2(r-1)}(p-1)^2 & \text{if } a \text{ is a cubic residue modulo } p. \end{cases}$$

This terminates the proof. □

For $N=p^rq^s$ and $a \in \mathbb{Z}/N\mathbb{Z}$, let $\mathcal{PC}_a(N)$ be the set of the solutions of the cubic Pell curve

$$x^3+ay^3+a^2z^3-3axyz \equiv 1 \pmod N.$$

The following result is an easy consequence of Lemma 3.

Corollary 4. *Let $N=p^rq^s$ be a prime power modulus with $p,q \equiv 1 \pmod 3$. The number of solutions of the cubic Pell curve $x^3+ay^3+a^2z^3-3axyz \equiv 1 \pmod N$ is given by*

$$|\mathcal{PC}_a(N)| = |\mathcal{PC}_a(p^r)|\,|\mathcal{PC}_a(q^s)|,$$

where $\mathcal{PC}_a(p^r)$ and $\mathcal{PC}_a(q^s)$ are the sets of the solutions of the cubic Pell equation $x^3+ay^3+a^2z^3-3axyz \equiv 1$ modulo p^r and modulo q^s respectively.

Proof. Let $N=p^rq^s$ with $p,q \equiv 1 \pmod 3$. Let $a \in \mathbb{Z}/N\mathbb{Z}$ with $a \neq 0$. By the Chinese Remainder Theorem, there is a bijection between $\mathbb{Z}/N\mathbb{Z}$ and $\mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/q^s\mathbb{Z}$. This induces a bijection between the solutions (x_N, y_N, z_N) of the cubic Pell curve $x^3+ay^3+a^2z^3-3axyz \equiv 1 \pmod N$, and the solutions $((x_{p^r}, y_{p^r}, z_{p^r}), (x_{q^s}, y_{q^s}, z_{q^s}))$ formed by a solution of the cubic Pell curve

$x^3+ay^3+a^2z^3-3axyz \equiv 1$ modulo p^r and a solution of the same curve modulo p^r. Moreover, this implies that

$$|\mathcal{PC}_a(N)| = |\mathcal{PC}_a(p^r)|\,|\mathcal{PC}_a(q^s)|,$$

where $\mathcal{PC}_a(p^r)$ and $\mathcal{PC}_a(p^r)$ are the sets of the solutions of the cubic Pell equation $x^3+ay^3+a^2z^3-3axyz \equiv 1$ modulo p^r and modulo q^s respectively. □

The properties of the cubic Pell curve modulo a prime power modulus $N=p^rq^s$ with $p,q \equiv 1 \pmod 3$ can be summarized as follows.

1. For a prime power modulus $N=p^rq^s$, let $\mathcal{R}^3(N)$ be the set of the cubic residues a modulo p with $(\gcd(a,N)=1$. Its cardinality is
$$\left|\mathcal{R}^3(N)\right| = \frac{p^{r-1}q^{s-1}(p-1)(q-1)}{9}.$$
2. Define the values
$$\begin{aligned}
\psi_1(N) &= p^{2(r-1)}q^{2(s-1)}\left(p^2+p+1\right)\left(q^2+q+1\right),\\
\psi_2(N) &= p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2,\\
\psi_3(N) &= p^{2(r-1)}q^{2(s-1)}\left(p^2+p+1\right)(q-1)^2,\\
\psi_4(N) &= p^{2(r-1)}q^{2(s-1)}(p-1)^2\left(q^2+q+1\right).
\end{aligned} \tag{3}$$
For $a \in \mathbb{Z}/N\mathbb{Z}$ with $\gcd(a,N)=1$, the number of solutions of the equation $x^3+ay^3+a^2z^3-3axyz \equiv 1 \pmod N$ is then
$$|\mathcal{PC}_a(N)| = \begin{cases}
\psi_1(N) & \text{if } a \notin \mathcal{R}^3(p) \text{ and } a \notin \mathcal{R}^3(q),\\
\psi_2(N) & \text{if } a \in \mathcal{R}^3(p) \text{ and } a \in \mathcal{R}^3(q),\\
\psi_3(N) & \text{if } a \notin \mathcal{R}^3(p) \text{ and } a \in \mathcal{R}^3(q),\\
\psi_4(N) & \text{if } a \in \mathcal{R}^3(p) \text{ and } a \notin \mathcal{R}^3(q).
\end{cases}$$
where $\mathcal{R}^3(p)$ is the set of the cubic residues modulo p, and $\mathcal{R}^3(q)$ is the set of the cubic residues modulo q.
3. Let $\mathcal{PC}_a(N)$ be the set of the solutions of the cubic Pell curve $x^3+ay^3+a^2z^3-3axyz \equiv 1 \pmod N$ in $(\mathbb{Z}/N\mathbb{Z})^3$. Then $(\mathcal{PC}_a(N),\oplus)$ is an abelian group with order $|\mathcal{PC}_a(N)|$.
4. The neutral element of $\mathcal{PC}_a(N)$ is $(1,0,0)$.
5. The inverse of a solution $(x,y,z) \in \mathcal{PC}_a(N)$ is $\left(x^2-ayz, az^2-xy, y^2-xz\right) \pmod N$.
6. The sum of two solutions $(x_1,y_1,z_1),(x_2,y_2,z_2) \in \mathcal{PC}_a(N)$ is (x_3,y_3,z_3) with
$$(x_3,y_3,z_3) = (x_1x_2+a(y_2z_1+y_1z_2), x_2y_1+x_1y_2+az_1z_2, y_1y_2+x_2z_1+x_1z_2).$$
7. The scalar product of a solution $(x,y,z) \in \mathcal{PC}_a(N)$ by an integer n is
$$n \otimes (x,y,z) = (x,y,z) \oplus \cdots \oplus (x,y,z) \quad (n \text{ times}).$$

8. For any positive integer k, and any solution $(x, y, z) \in \mathcal{PC}_a(N)$,

$$(1 + k|\mathcal{PC}_a(N)|) \otimes (x, y, z) = (x, y, z).$$

In $\mathcal{PC}_a(N)$, the addition $\oplus$, the doubling, and the scalar multiplication by an integer are summarized in the following algorithms.

Algorithm 2 Addition in $\mathcal{PC}_a(N)$

Input: $N = p^r q^s$, $a \in \mathbb{Z}/N\mathbb{Z}\backslash\{0\}$, and $(x_1, y_1, z_1), (x_2, y_2, z_2) \in \mathcal{PC}_a(N)$.
Output: $(x_3, y_3, z_3) = (x_1, y_1, z_1) \oplus (x_2, y_2, z_2) \in \mathcal{PC}_a(N)$.
1: $x_3 \equiv x_1x_2 + a(y_2z_1 + y_1z_2) \pmod N$.
2: $y_3 \equiv x_2y_1 + x_1y_2 + az_1z_2 \pmod N$.
3: $z_3 \equiv y_1y_2 + x_2z_1 + x_1z_2 \pmod N$.
4: Return (x_3, y_3, z_3).

Algorithm 3 Doubling in $\mathcal{PC}_a(N)$

Input: $N = p^r q^s$, $a \in \mathbb{Z}/N\mathbb{Z}\backslash\{0\}$, and $(x_1, y_1, z_1) \in \mathcal{PC}_a(N)$.
Output: $(x_3, y_3, z_3) = 2 \otimes (x_1, y_1, z_1) \in \mathcal{PC}_a(N)$.
1: $x_3 \equiv x_1^2 + 2ay_1z_1 \pmod N$.
2: $y_3 \equiv 2x_1y_1 + az_1^2 \pmod N$.
3: $z_3 \equiv y_1^2 + 2x_1z_1 \pmod N$.
4: Return (x_3, y_3, z_3).

Algorithm 4 Left-to-right scalar multiplication in $\mathcal{PC}_a(N)$

Input: $N = p^r q^s$, $a \in \mathbb{Z}/N\mathbb{Z}\backslash\{0\}$, $(x_1, y_1, z_1) \in \mathcal{PC}_a(N)$, and an integer $n \geq 2$.
Output: $(x_2, y_2, z_2) = n \otimes (x_1, y_1, z_1) \in \mathcal{PC}_a(N)$.
1: Expand n in base 2, that is $n = (n_{k-1}n_{k-2} \dots n_1n_0)_2$.
2: $(x_2, y_2, z_2) = (1, 0, 0)$.
3: **For** i from $k - 1$ **downto** 0 **do**
4: $\quad (x_2, y_2, z_2) = 2 \otimes (x_2, y_2, z_2)$.
5: $\quad$ **If** $n_i = 1$ **then**
6: $\quad\quad (x_2, y_2, z_2) = (x_2, y_2, z_2) \oplus (x_1, y_1, z_1)$.
7: $\quad$ **End If**
8: **End For**
9: Return (x_2, y_2, z_2).

4 Our construction

In this section, we present a new scheme based on the cubic Pell curve. It is a variant of both RSA and KMOV. We also provide a numerical example for our scheme.

4.1 The new public key encryption scheme

In the following algorithms, we give the algorithms of the new public key encryption scheme, namely, the key generation, the encryption, and the decryption algorithm.

Algorithm 5 Key Generation

Input: A security parameter λ, and two small positive integers r and s.
Output: A public key $\mathcal{PK}$ and a private key $\mathcal{SK}$.

1: Choose a prime number p of λ bit size with $p \equiv 1 \pmod 3$.
2: Choose a prime number q of λ bit size with $q \equiv 1 \pmod 3$.
3: Compute $N = p^r q^s$.
4: For $i = 1, 2, 3, 4$, compute $\psi_i(N)$ using (3).
5: Choose an integer $e \in \mathbb{Z}/N\mathbb{Z}$ such that

$$\gcd\left(e, pq\left(p^2+p+1\right)\left(q^2+q+1\right)(p-1)(q-1)\right) = 1.$$

6: For $i = 1, 2, 3, 4$, compute $d_i \equiv e^{-1} \pmod{\psi_i(N)}$.
7: The public key is $\mathcal{PK} = (N, e)$.
8: The private key is $\mathcal{SK} = (p, q, N, d_1, d_2, d_3, d_4, r, s)$.
9: Return the keypair $(\mathcal{PK}, \mathcal{SK})$.

Algorithm 6 Encryption Process

Input: A message $M = (x_M, y_M) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ and a public key $\mathcal{PK} = (N, e)$.
Output: The ciphertext of M.

1: Represent the message M as $M = (x_M, y_M, 0)$.
2: Compute $a \equiv \frac{1-x_M^3}{y_M^3} \pmod N$. ▷ $(x_M, y_M, 0) \in \mathcal{PC}_a(N)$
3: Compute $(x_C, y_C, z_C) = e \otimes (x_M, y_M, 0)$ on the cubic Pell curve with the equation

$$\mathcal{PC}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod N.$$

4: Return the ciphertext (x_C, y_C, z_C).

Algorithm 7 Decryption Process

Input: A ciphertext (x_C, y_C, z_C), and a private key $\mathcal{SK} = (p, q, N, d_1, d_2, d_3, d_4, r, s)$.
Output: The decryption of (x_C, y_C, z_C).

1: Find the solutions $x = a_{p,1}$ and $x = a_{p,2}$ of the equation

$$x_C^3 + xy_C^3 + x^2 z_C^3 - 3xx_C y_C z_C \equiv 1 \pmod{p^r}.$$

2: Find the solutions $y = a_{q,1}$ and $y = a_{q,2}$ of the equation

$$x_C^3 + yy_C^3 + y^2 z_C^3 - 3yx_C y_C z_C \equiv 1 \pmod{q^s}.$$

3: Using the Chinese Remainder Theorem, compute $a_i \in \mathbb{Z}/N\mathbb{Z}$, $i = 1, 2, 3, 4$ such that

$$\begin{aligned} a_1 &\equiv a_{p,1} \pmod{p^r}, a_1 \equiv a_{q,1} \pmod{q^s}, \\ a_2 &\equiv a_{p,1} \pmod{p^r}, a_2 \equiv a_{q,2} \pmod{q^s}, \\ a_3 &\equiv a_{p,2} \pmod{p^r}, a_3 \equiv a_{q,1} \pmod{q^s}, \\ a_4 &\equiv a_{p,2} \pmod{p^r}, a_4 \equiv a_{q,2} \pmod{q^s}. \end{aligned}$$

4: **For** $i = 1, 2, 3, 4$ **do**
5: Set

$$D_i = \begin{cases} d_1 & \text{if } a_i \notin \mathcal{R}^3(p) \text{ and } a_i \notin \mathcal{R}^3(q), \\ d_2 & \text{if } a_i \in \mathcal{R}^3(p) \text{ and } a_i \in \mathcal{R}^3(q), \\ d_3 & \text{if } a_i \notin \mathcal{R}^3(p) \text{ and } a_i \in \mathcal{R}^3(q), \\ d_4 & \text{if } a_i \in \mathcal{R}^3(p) \text{ and } a_i \notin \mathcal{R}^3(q), \end{cases}$$

where $\mathcal{R}^3(p)$ and $\mathcal{R}^3(q)$ are the sets of the cubic residues in $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$ respectively.
6: Compute $M_i = (x_i, y_i, z_i) = D_i \otimes (x_C, y_C, z_C)$ on the cubic Pell curve

$$\mathcal{PC}_{a_i}(N) : x^3 + a_i y^3 + a_i^2 z^3 - 3a_i xyz \equiv 1 \pmod{N}.$$

7: **End For**
8: Return the plaintext (x_i, y_i, z_i) for which $z_i = 0$. ▷ M=$(x_i, y_i, 0)$ is the original message.

Notice that in Algorithm 7, Step 1 to Step 3 are devoted to the computation of the parameter a of the cubic Pell curve used in the encryption process given only the ciphertext (x_C, y_C, z_C) and the private parameters p, q, r, s. Since these steps require the computation of square roots modulo p and modulo q, one can choose p and q so that $p, q \equiv 7 \pmod{12}$, which implies $p, q \equiv 1 \pmod{3}$ and $p, q \equiv 3 \pmod{4}$. This allows to compute the square roots of a quadratic residue $\Delta \bmod p$ as $\pm\Delta^{(p+1)/4} \pmod{p}$.

4.2 The failure of the decryption algorithm

In several schemes such as LWE [Reg05], RLWE [LPR13], Ramstake [Sze17], New Hope [SAB+17], and several variants of CRYSTALS-Kyber [BDK+18], the de-

cryption protocol is probabilistic with a negligible probability of failure. Despite their possible failure, some of the former schemes are used in many cryptographic applications such as electronic voting, electronic auction, and digital signatures.

We do not know if our new scheme presents a possibility of decryption failure. We have extensively experienced it, and the decryption protocol was always successful and unique. The following result shows that the probability of a possible failure is negligible.

Lemma 4. *Let $N = p^r q^s$ be a prime power modulus, $x_M, y_M \in \mathbb{Z}/N\mathbb{Z}$, and $(x_C, y_C, z_C) = e(x_M, y_M, 0)$ be the ciphertext computed with the cubic Pell curve $\mathcal{PC}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod N$ with $a \equiv \frac{1-x_M^3}{y_M^3} \pmod N$. The failure probability of the decryption of the scheme lies in the interval $\left(\frac{1}{16N}, \frac{16}{N}\right)$, and is negligible.*

Proof. Let $(x_M, y_M, 0)$ be a plaintext, and (x_C, y_C, z_C) be the corresponding ciphertext over the cubic Pell curve $x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod N$ where $a \equiv \frac{1-x_M^3}{y_M^3}$. Suppose that another solution a_0 of the quadratic equation $x_C^3 + a_0y_C^3 + a_0^2z_C^3 - 3a_0x_Cy_Cz_C \equiv 1 \pmod N$ is such that $d(x_C, y_C, z_C) = (x_1, y_1, 0)$ for one decryption exponent $d \in \{d_1, d_2, d_3, d_4\}$, on the cubic Pell curve $\mathcal{PC}_{a_0}(N) : x^3+a_0y^3+a_0^2z^3-3a_0xyz \equiv 1 \pmod N$, and $(x_M, y_M, 0) \neq (x_1, y_1, 0)$. Then, $(x_1, y_1, 0) \in \mathcal{PC}_{a_0}^0(N)$ where $\mathcal{PC}_{a_0}^0(N)$ is the set of the solutions of the cubic equation

$$\mathcal{PC}_{a_0}^0(N) : x^3 + a_0y^3 \equiv 1 \pmod N.$$

This scenario happens with probability

$$\text{Prob}(z = 0) = \frac{|\mathcal{PC}_{a_0}^0(N)|}{|\mathcal{PC}_{a_0}(N)|}. \tag{4}$$

The curve $\mathcal{PC}_{a_0}^0(N)$ is a specific case of the cubic Pell equation. Hence, if $\mathcal{PC}_{a_0}^0(p)$ is the number of the solutions of $x^3 + ay^3 \equiv 1 \pmod p$, then, by Theorem 3, the number of the solutions of the equation $x^3 + ay^3 \equiv 1 \pmod{p^r}$ is

$$\left|\mathcal{PC}_{a_0}^0(p^r)\right| = p^{r-1}\left|\mathcal{PC}_{a_0}^0(p)\right|.$$

Using the Chinese Remainder Theorem, it follows that the number of solutions of the equation $x^3 + ay^3 \equiv 1 \pmod N$ is

$$\left|\mathcal{PC}_{a_0}^0(N)\right| = p^{r-1}p^{s-1}\left|\mathcal{PC}_{a_0}^0(p)\right|\left|\mathcal{PC}_{a_0}^0(q)\right|.$$

The curve $x^3 + ay^3 \equiv 1 \pmod p$ is a specific form of the Selmer curve. It is birationally equivalent to the elliptic curve

$$E_p : v^2 \equiv u^3 - 432a^2 \pmod p,$$

under the transformations

$$u = -\frac{12a_1y}{x-1}, \quad v = 36a_1\frac{x+1}{x-1},$$
$$x = \frac{v+36a_1}{v-36a_1}, \quad y = -\frac{6u}{v-36a_1}.$$

By Hasse Theorem [Gal12], the order of E_p satisfies

$$(\sqrt{p}-1)^2 \leq |E_p| \leq (\sqrt{p}+1)^2 .$$

Since $|E_p| = \left|\mathcal{PC}^0_{a_0}(p)\right|$, then using $\left(\sqrt{p}-1\right)^2 > \frac{1}{2}p$ and $\left(\sqrt{p}+1\right)^2 < 2p$, we get

$$\frac{1}{2}p < \left|\mathcal{PC}^0_{a_0}(p)\right| < 2p.$$

By Theorem 3 and the Chinese Remainder Theorem, this implies that $\left|\mathcal{PC}^0_{a_0}(N)\right|$ satisfies

$$\frac{1}{4}p^{r-1}p^{s-1}pq \leq \left|\mathcal{PC}^0_{a_0}(N)\right| \leq 4\frac{1}{4}p^{r-1}p^{s-1}pq,$$

that is

$$\frac{1}{4}N \leq \left|\mathcal{PC}^0_{a_0}(N)\right| \leq 4N. \tag{5}$$

On the other hand, the orders $\psi_i(N)$, $i = 1, 2, 3, 4$ as defined in 3 satisfy

$$p^{r-1}p^{s-1}(p-1)^2(q-1)^2 \leq \psi_i(N) \leq p^{r-1}p^{s-1}\left(p^2+p+1\right)\left(q^2+q+1\right).$$

Since $|\mathcal{PC}_{a_0}(N)| \in \{\psi_1(N), \psi_2(N), \psi_3(N), \psi_4(N)\}$, and since $(p-1)^2 > \frac{1}{2}p^2$, and $p^2+p+1 < 2p^2$ for $p > 4$, we get

$$\frac{1}{4}N^2 \leq |\mathcal{PC}_{a_0}(N)| \leq 4N^2.$$

Combining this with (5), the probability (4) satisfies

$$\frac{1}{16N} < \text{Prob}(z=0) < \frac{16}{N}.$$

This shows that the decryption failure is negligible. □

4.3 A numerical example for the scheme

Let us consider the following small example.

1. **Key Generation**
   - Let $p = 922039$, $q = 760531$, $r = 1$ and $s = 3$. Then

     $$N = 922039 \times 760531^3 = 405601968528411801552349.$$

   - Let $e = 190681261905711342654691$. The public key is

     $$(N, e) = (405601968528411801552349, 190681261905711342654691).$$

- The private exponents are

$$\begin{aligned}
d_1 &= e^{-1} \pmod{p^{2(r-1)}q^{2(s-1)}\left(p^2+p+1\right)\left(q^2+q+1\right)},\\
&= 11897277222328345101425117506949101141922308852 0,\\
d_2 &= e^{-1} \pmod{p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2},\\
&= 52673607813631318169063886466607845951930222411,\\
d_3 &= e^{-1} \pmod{p^{2(r-1)}q^{2(s-1)}\left(p^2+p+1\right)(q-1)^2},\\
&= 11056208697029256535518185134639459956701066871 1,\\
d_4 &= e^{-1} \pmod{p^{2(r-1)}q^{2(s-1)}(p-1)^2\left(q^2+q+1\right)},\\
&= 15506417996252072324528031405338008627364567039 5.
\end{aligned}$$

- The private key is $(p, q, N, d_1, d_2, d_3, d_4, r, s)$.

2. **The plaintext**
Consider the plaintext $(x_M, y_M, 0)$ with

$$\begin{aligned}
x_M &= 94727413669590175405397,\\
y_M &= 40042921671686898776823 0.
\end{aligned}$$

3. **Encryption :**
   - First we compute

$$a \equiv \frac{1-x_M^3}{y_M^3} \pmod{N} = 40212934565513209306735 1.$$

   - The cubic Pell curve is then

$$\mathcal{PC}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod{N}.$$

   - We compute $(x_C, y_C, z_C) = e \otimes (x_M, y_M, 0)$ on the cubic Pell curve $\mathcal{PC}_a(N)$ using the Algorithm 4. We get the ciphertext (x_C, y_C, z_C) with

$$\begin{aligned}
x_C &= 296657492079316956423913,\\
y_C &= 336170831341196089366817,\\
z_C &= 351828474470867029080629.
\end{aligned}$$

4. **Decryption :**
   - Solving the equation

$$x_C^3 + xy_C^3 + x^2z_C^3 - 3xx_Cy_Cz_C \equiv 1 \pmod{p},$$

   we get the solutions $x_1 = 124693$, and $x_2 = 29301$.
   - Apply Hensel's lemma with x_1 and x_2 to solve the equation

$$x_C^3 + xy_C^3 + x^2z_C^3 - 3xx_Cy_Cz_C \equiv 1 \pmod{p^r}.$$

   We get $x = a_{p,1} = 124693$ and $x = a_{p,2} = 29301$.

- Solve the equation

$$x_C^3 + yy_C^3 + y^2 z_C^3 - 3yx_C y_C z_C \equiv 1 \pmod{q}.$$

  We get the solutions $y_1 = 272543$, and $y_2 = 758118$.
- Apply Hensel's lemma with y_1 and y_2 to solve the equation

$$x_C^3 + yy_C^3 + y^2 z_C^3 - 3yx_C y_C z_C \equiv 1 \pmod{q^s}.$$

  We get $y = a_{q,1} = 362045505517707447$ and $y = a_{q,2} = 228874968160044609$.
- Using the Chinese theorem with $a_{p,1}$ and $a_{q,1}$, we get

$$a_1 = 402129345655132093067351 \pmod{N}.$$

- Using the Chinese theorem with $a_{p,2}$ and $a_{q,2}$, we get

$$a_2 = 261500816821281874691178 \pmod{N}.$$

- Using the Chinese theorem with $a_{p,1}$ and $a_{q,2}$, we get

$$a_3 = 170916396245462831245876 \pmod{N}.$$

- Using the Chinese theorem with $a_{p,2}$ and $a_{q,1}$, we get

$$a_4 = 87111797702539334960304 \pmod{N}.$$

- We can check that a_1 is a cubic residue modulo p and a cubic non-residue modulo q. So $D_1 = d_4$. We then compute $(x_1, y_1, z_1) = d_4 \otimes (x_C, y_C, z_C)$ on the cubic Pell curve $\mathcal{PC}_{a_1}(N)$ using Algorithm 4. We get

$$(x_1, y_1, z_1) = (94727413669590175405397, 40042921671686898776823 0, 0),$$

  which is the original plaintext.
- We can check that a_2 is a cubic non-residue modulo p and a cubic non-residue modulo q. So $D_2 = d_1$. We then compute $(x_2, y_2, z_2) = d_1 \otimes (x_C, y_C, z_C)$ on the cubic Pell curve $\mathcal{PC}_{a_1}(N)$ using Algorithm 4. We get a solution (x_2, y_2, z_2) with

$$\begin{aligned} x_2 &= 315084178973498538996923, \\ y_2 &= 334849906408238591863534, \\ z_2 &= 119465479892270850302989. \end{aligned}$$

  which is not the original plaintext.
- We can check that a_3 is a cubic residue modulo p and cubic non-residue modulo q. So $D_3 = d_4$. We then compute $(x_1, y_2, z_2) = d_4 \otimes (x_C, y_C, z_C)$ on the cubic Pell curve $\mathcal{PC}_{a_1}(N)$ using Algorithm 4. We get a solution (x_3, y_3, z_3) with

$$\begin{aligned} x_3 &= 348782910156330842695269, \\ y_3 &= 334241529189406423678081, \\ z_3 &= 147702892801927905973570. \end{aligned}$$

  which is not the original plaintext.

- We can check that a_4 is a cubic non-residue modulo p and a cubic non-residue modulo q. So $D_4 = d_1$. We then compute $(x_4, y_4, z_4) = d_1 \otimes (x_C, y_C, z_C)$ on the cubic Pell curve $\mathcal{PC}_{a_1}(N)$ using Algorithm 4. We get a solution (x_4, y_4, z_4) with

$$\begin{aligned} x_4 &= 61028682486757871707051, \\ y_4 &= 401037593935701155953683, \\ z_4 &= 377364555618754745881768. \end{aligned}$$

  which is not the original plaintext.

We notice that the decryption performs perfectly, and is unique.

5 Security Analysis

In this section, we study the security of the new scheme as described in Section 4.

5.1 Resistance against finding the cubic Pell curve

In the new scheme, the value of a in the Pell curve $x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod N$ is not public. Indeed, the public parameters are N and a solution $(x_C, y_C, z_C) \in \mathcal{PC}_a(N)$. To compute the parameter a, one should solve the modular equation

$$z_C^3 a^2 + \left(y_C^3 - 3x_C y_C z_C\right) a + x_C^3 - 1 \equiv 0 \pmod N,$$

which is quadratic in a. The discriminant of the equation is

$$\Delta = \left(y_C^3 - 3x_C y_C z_C\right)^2 - 4z_C^3 \left(x_C^3 - 1\right).$$

Then, finding a is equivalent to solving the quadratic equation

$$x^2 \equiv \Delta \pmod N,$$

where the factorization of N is unknown. This is known as the SQRT-MOD-N problem, and is equivalent to the integer factoring problem [Gal12].

5.2 Resistance against the small private exponent attacks

It is known that using a small private exponent is insecure in several schemes such as RSA [Cop97,Wie90,BD99], KMOV[Nit14], and others [NAAA21]. The main known techniques are based on the continued fraction algorithm [Wie90] or on Coppersmith's method [Cop97,BD99]. The attacks based on the continued fraction algorithm use the following well known result of Legendre (see Theorem 184 of [HW79]).

Theorem 6 (Legendre). *Let ξ be a positive number. Let a and b be integers such that* $\gcd(a,b)=1$ *and*

$$\left|\xi-\frac{a}{b}\right|<\frac{1}{2b^2}.$$

Then $\frac{a}{b}$ is one of the convergents of the continued fraction expansion of ξ.

In most cases, the RSA moduli and their variants are the product of large prime numbers of the same bit size. In our schemes, we also suppose that the prime numbers p and q in the modulus $N=p^rq^s$ are of the same bit size, and ordered so that $q<p<2q$. The following result gives effective bounds for p and q.

Proposition 2. *Let $N=p^rq^s$ be a prime power modulus with $q<p<2q$. Then*

$$2^{\frac{-1}{r+s}}N^{\frac{1}{r+s}}<q<N^{\frac{1}{r+s}}<p<2^{\frac{s}{r+s}}N^{\frac{1}{r+s}}.$$

Proof. Suppose that $q<p<2q$. Then $q^r<p^r<2^rq^r$ and $q^s<p^s<2^sq^s$. Multiplying the former inequalities, we get

$$q^{r+s}<N<2^{r+s}q^{r+s},$$

which implies that $q<N^{\frac{1}{r+s}}$ and $2^{\frac{-1}{r+s}}N^{\frac{1}{r+s}}<q$.
Multiplying $q^s<p^s<2^sq^s$ by p^r, we get

$$N<p^{r+s}<2^sN,$$

and $N^{\frac{1}{r+s}}<p<2^{\frac{s}{r+s}}N^{\frac{1}{r+s}}$. Summarizing all inequalities, we get

$$2^{\frac{-1}{r+s}}N^{\frac{1}{r+s}}<q<N^{\frac{1}{r+s}}<p<2^{\frac{s}{r+s}}N^{\frac{1}{r+s}}.$$

This terminates the proof. □

For $i=1,2,3,4$, and $\psi(N)\in\{\psi_1(N),\psi_2(N),\psi_3(N),\psi_4(N)\}$ as given in (3), the following result gives an approximation of $\psi_i(N)$ in terms of N.

Proposition 3. *Let $N=p^rq^s$ be a prime power modulus with $q<p<2q$. Let $\psi(N)\in\{\psi_1(N),\psi_2(N),\psi_3(N),\psi_4(N)\}$ as given in (3). Then N^2 is an approximation of $\psi(N)$ with*

$$\left|\psi(N)-N^2\right|<8N^{2-\frac{1}{r+s}}.$$

Proof. Let $\psi(N)\in\{\psi_1(N),\psi_2(N),\psi_3(N),\psi_4(N)\}$. Then

$$p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2\leq\psi(N)\leq p^{2(r-1)}q^{2(s-1)}\left(p^2+p+1\right)\left(q^2+p+1\right).$$

This can be rewritten as

$$N^2\left(1-\frac{2}{p}+\frac{1}{p^2}\right)\left(1-\frac{2}{q}+\frac{1}{q^2}\right)\leq\psi(N)\leq N^2\left(1+\frac{1}{p}+\frac{1}{p^2}\right)\left(1+\frac{1}{q}+\frac{1}{q^2}\right)$$

By Proposition 2, we have $N^{\frac{1}{r+s}}<p$. Then

$$1-\frac{2}{p}+\frac{1}{p^2}>1-\frac{2}{p}>1-2N^{\frac{-1}{r+s}}.$$

Similarly, by Proposition 2, we have $2^{\frac{-1}{r+s}}N^{\frac{1}{r+s}} < q$. Then

$$1 - \frac{2}{q} + \frac{1}{q^2} > 1 - \frac{2}{q} > 1 - 2^{1+\frac{1}{r+s}}N^{\frac{-1}{r+s}}.$$

Using the former inequalities, we get

$$\begin{aligned}\psi(N) &> N^2\left(1 - 2N^{\frac{-1}{r+s}}\right)\left(1 - 2^{1+\frac{1}{r+s}}N^{\frac{-1}{r+s}}\right)\\ &= N^2\left(1 - 2^{1+\frac{1}{r+s}}N^{\frac{-1}{r+s}} - 2N^{\frac{-1}{r+s}} + 2^{2+\frac{1}{r+s}}N^{\frac{-2}{r+s}}\right)\\ &> N^2\left(1 - 8N^{\frac{-1}{r+s}}\right).\end{aligned}$$

Using this, we get

$$\psi(N) - N^2 > -8N^{2-\frac{1}{r+s}}. \tag{6}$$

Also, by Proposition 2, we have $N^{\frac{1}{r+s}} < p$. Then

$$1 + \frac{1}{p} + \frac{1}{p^2} < 1 + \frac{2}{p} < 1 + 2N^{\frac{-1}{r+s}}.$$

Similarly, by Proposition 2, we have $2^{\frac{-1}{r+s}}N^{\frac{1}{r+s}} < q$. Then

$$1 + \frac{1}{q} + \frac{1}{q^2} < 1 + \frac{2}{q} < 1 + 2^{\frac{r+s+1}{r+s}}N^{\frac{-1}{r+s}}.$$

Plugging this in $\psi(N)$, we get

$$\begin{aligned}\psi(N) &< N^2\left(1 + 2N^{\frac{-1}{r+s}}\right)\left(1 + 2^{\frac{r+s+1}{r+s}}N^{\frac{-1}{r+s}}\right)\\ &= N^2\left(1 + 2^{\frac{r+s+1}{r+s}}N^{\frac{-1}{r+s}} + 2N^{\frac{-1}{r+s}} + 2^{1+\frac{r+s+1}{r+s}}N^{\frac{-2}{r+s}}\right)\\ &< N^2\left(1 + 8N^{\frac{-1}{r+s}}\right).\end{aligned}$$

Using this, we get

$$\psi(N) - N^2 < 8N^{2-\frac{1}{r+s}}. \tag{7}$$

Combining (6) and (7), we get

$$\left|\psi(N) - N^2\right| < 8N^{2-\frac{1}{r+s}}.$$

This completes the proof. □

The following result which is based on the continued fraction algorithm shows that using a small private exponent d is vulnerable.

Proposition 4. *Let $N = p^r q^s$ be a prime power modulus with $q < p < 2q$. Let e be a public exponent, and $d \equiv e^{-1} \pmod{\psi(N)}$ where $\psi(N)$ is one of the orders $\psi_1(N)$, $\psi_2(N)$, $\psi_3(N)$, or $\psi_4(N)$. If $e < \psi(N)$, and*

$$d < \frac{\sqrt{2}}{4} N^{\frac{1}{2(r+s)}},$$

then one can find d and factor N in polynomial time.

Proof. The relation $d \equiv e^{-1} \pmod{\psi(N)}$ can be rewritten as $ed - k\psi(N) = 1$ with a positive integer k. This can be rewritten as

$$\left| \frac{e}{\psi(N)} - \frac{k}{d} \right| = \frac{1}{d\psi(N)}.$$

Suppose $e < \psi(N)$. Using Proposition 3, we have $\left|\psi(N) - N^2\right| < 8N^{2-\frac{1}{r+s}}$. Then

$$\begin{aligned}
\left| \frac{e}{N^2} - \frac{k}{d} \right| &< \left| \frac{e}{N^2} - \frac{e}{\psi(N)} \right| + \left| \frac{e}{\psi(N)} - \frac{k}{d} \right| \\
&< \psi(N) \left| \frac{\psi(N) - N^2}{N^2 \psi(N)} \right| + \frac{1}{d\psi(N)} \\
&< \frac{8N^{2-\frac{1}{r+s}}}{N^2} + \frac{1}{d\psi(N)} \\
&< \frac{8}{N^{\frac{1}{r+s}}} + \frac{1}{N^2 d}.
\end{aligned}$$

Suppose that $d < \frac{\sqrt{2}}{8} N^{\frac{1}{2(r+s)}}$. Then $d < \frac{1}{4} N^2$, and

$$\left| \frac{e}{N^2} - \frac{k}{d} \right| < \frac{1}{4d^2} + \frac{1}{4d^2} = \frac{1}{2d^2}.$$

By Legendre's Theorem 6, this implies that $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{N^2}$, which can be found in polynomial time. Using k and d in the equation $ed - k\psi(N) = 1$, we get

$$\psi(N) = \frac{ed - 1}{k}.$$

Using $\psi(N)$, we get

$$g = \gcd\left(N^2, \psi(N)\right) = p^{2(r-1)} q^{2(s-1)}.$$

In turn, this gives

$$pq = \frac{N}{\sqrt{g}},$$

and, combining with $N = p^r q^s$, we finally get

$$p = \left(\frac{N^{s-1}}{g^{\frac{s}{2}}} \right)^{\frac{1}{s-r}}, q = \left(\frac{N^{r-1}}{g^{\frac{r}{2}}} \right)^{\frac{1}{r-s}}.$$

This completes the proof. □

6 Conclusion

In this paper, we proposed a new public key cryptosystem based on the cubic Pell curve modulo a prime power modulus of the form $N = p^r q^s$ to perform encryption and decryption. We studied its security and showed that it is based on two computationally hard problems, namely, the integer factorization problem, and the Rabin trapdoor. The advantage of the new scheme is that the arithmetic operations have to be performed on a cubic Pell curve which is known only to the sender and the recipient.

References

Bar03. E. J. Barbeau. Pell equation. In *Pell Equation*, chapter 7: The Cubic Analogue of Pell Equation. Springer, New York, 2003. 5

BD99. D. Boneh and G. Durfee. Cryptanalysis of RSA with private key d less than $n^{0.292}$. In *Advances in Cryptology - EUROCRYPT'99*, volume 1592 of *Lecture Notes in Computer Science*, pages 1–11. Springer-Verlag, 1999. 2, 18

BDF98. D. Boneh, G. Durfee, and Y. Frankel. An attack on RSA given a small fraction of the private key bits. In *ASIACRYPT 1998*, pages 25–34, 1998. 2

BDHG99. D. Boneh, G. Durfee, and N. Howgrave-Graham. Factoring $n = p^r q$ for large r. In *CRYPTO 1999*, pages 326–337, 1999. 2

BDK+18. J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanckk, P. Schwabe, G. Seiler, and D. Stehlé. CRYSTALS-Kyber: A CCA-secure module-latticebased KEM. In *2018 IEEE European Symposium on Security and Privacy (EuroSP)*, pages 353–367. IEEE, 2018. 13

BN17. M. Boudabra and A. Nitaj. A new generalization of the KMOV cryptosystem. *J. Appl. Math. Comput.*, 57(1–2):229–245, 2017. 3, 6

BN19. M. Boudabra and A. Nitaj. A new public key cryptosystem based on Edwards curves. *J. Appl. Math. Comput.*, 61:431–450, 2019. 3

Bon99. D. Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices Amer. Math. Soc.*, 46(2):203–213, 1999. 2

Cop97. D. Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology*, 10(4):233–260, 1997. 2, 18

Dem94. N. Demytko. A new elliptic curve based analogue of RSA. In T. Helleseth, editor, *EUROCRYPT 1993*, volume 765 of *Lecture Notes in Computer Science*, pages 40–49. Springer-Verlag, 1994. 2

DH76. W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theory*, 22(6):644–654, 1976. 1

DM22. Simone Dutto and Nadir Murru. On the cubic Pell equation over finite fields, 2022. arXiv:2203.05290. 8

DPS96. C. Ding, D. Pei, and A. Salomaa. *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography.* World Scientific, 1996. 6

dW02. B. de Weger. Cryptanalysis of RSA with small prime difference. *Appl. Algebra Eng. Commun. Comput.*, 13(1):17–28, 2002. 2

Gal12. S. Galbraith. *Mathematics of Public Key Cryptography.* Cambridge University Press, Cambridge, UK, 2012. 7, 15, 18

Hås86. J. Håstad. N using RSA with low exponent in a public key network. In *Advances in Cryptology - CRYPTO'85*, pages 403–408. Springer Berlin Heidelberg, 1986. 2

HW79. G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. The Clarendon Press Oxford University Press, New York, 5th edition, 1979. 18

KKT95. H. Kuwakado, K. Koyama, and Y. Tsuruoka. A new RSA-type scheme based on singular cubic curves $y^2 \equiv x^3 + bx^2 \pmod{n}$. *IEICE Trans. Fundam.*, E78-A:27–33, 1995. 2

KMOV91. K. Koyama, U. M. Maurer, T. Okamoto, and S. A. Vanstone. New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$. In *CRYPTO 1991*, volume 576 of *Lecture Notes in Computer Science*, pages 252–266, 1991. 2

Koy95. K. Koyama. Fast RSA type scheme based on singular cubic curve $y^2 + axy = x^3 \pmod{n}$. In *EUROCRYPT'95*, volume 921 of *Lecture Notes in Computer Science*, pages 329–339. Springer-Verlag, 1995. 2

LKYL00. S. Lim, S. Kim, I. Yie, and H. Lee. A generalized Takagi-cryptosystem with a modulus of the form $p^r q^s$. In *Indocrypt*, pages 283–294. Springer, 2000. 3

LLL82. A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:513–534, 1982. 2

LPR13. V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. *J. ACM*, 60(6):1–35, 2013. 13

MS18. N. Murru and F. M. Saettone. A novel RSA-like cryptosystem based on a generalization of the rédei rational functions. In J. Kaczorowski, J. Pieprzyk, and J. Pomykala, editors, *Number-Theoretic Methods in Cryptology*, volume 10737 of *Lecture Notes in Computer Science*, pages 174–190. Springer, Cham, 2018. 2

NAAA21. A. Nitaj, M. R. B. K. Ariffin, N. N. H. Adenan, and N. A. Abu. Classical attacks on a variant of the RSA cryptosystem. In P. Longa and C. Rafols, editors, *Progress in Cryptology - LATINCRYPT 2021*, volume 12912 of *Lecture Notes in Computer Science*. Springer, 2021. 18

Nit08. A. Nitaj. Another generalization of Wiener's attack on RSA. In S. Vaudenay, editor, *Africacrypt 2008*, volume 5023 of *Lecture Notes in Computer Science*, pages 174–190, Heidelberg, 2008. Springer. 2

Nit14. A. Nitaj. A new attack on the KMOV cryptosystem. *Bull. Korean Math. Soc.*, 51:1347–1356, 2014. 18

OU98. T. Okamoto and U. Uchiyama. A new public-key cryptosystem as secure as factoring. In *EUROCRYPT 1998*, volume 1403 of *Lecture Notes in Computer Science*, pages 308–318, Berlin, 1998. Springer. 3

OUF98. T. Okamoto, U. Uchiyama, and E. Fujisaki. EPOC: Efficient probabilistic public-key encryption. 1998. 3

Rab79. M. O. Rabin. Digitalized signatures and public key functions as intractable as factorization. Technical Report MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979. 1, 3

Reg05. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *STOC'05*, pages 84–93. ACM, 2005. 13

Ros93. K. H. Rosen. *Elementary Number Theory and Its Applications*. Addison-Wesley, Reading, 3rd edition, 1993. 4, 5

RSA78. R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978. 1

SAB+17. P. Schwabe, R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, G. Seiler, and D. Stehlé. Newhope. Technical report, National Institute of Standards and Technology, 2017. https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions. 13

Sag23. Sage Developers. SageMath, the Sage mathematics software system. https://www.sagemath.org, 2023. Version 10.1. 4

Sec23. M. Seck. Proof of concept implementation of the proposed encryption scheme. https://github.com/mseckept/schemesecknitaj.git, 2023. 4

Sim23. SimulaMath Developers. SimulaMath, a software for learning, teaching and research in mathematics. https://simulamath.org, 2023. Version 1.1. 4

SS06. K. Schmidt-Samoa. A new Rabin-type trapdoor permutation equivalent to factoring. *Electron. Notes Theor. Comput. Sci.*, 157(3):79–94, 2006. https://eprint.iacr.org/2005/278.pdf. 3

Sze17. A. Szepieniec. Ramstake. https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions, 2017. 13

TC23. George Teseleanu and Paul Cotan. Small private key attack against a family of RSA-like cryptosystems. https://eprint.iacr.org/2023/1356, 2023. Cryptology ePrint Archive, Paper 2023/1356. 2

Wie90. M. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Trans. Inf. Theory*, 36:553–558, 1990. 2, 18

Wil85. H. C. Williams. An M^3 public-key encryption scheme. In *CRYPTO 1985*, Lecture Notes in Computer Science, pages 358–368. Springer Berlin Heidelberg, 1985. 1

Zeu19. Thomas Zeugmann. Taking discrete roots in the field $\mathbb{Z}_p$ and in the ring $\mathbb{Z}_{p^e}$. Report series a, Division of Computer Science, 2019. 7