Moroccan Journal of Algebra and Geometry with Applications
Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco
Volume 4, Issue 1 (2025), pp 89-107
ISSN: 2820-7114

Title :

A New Public Key Encryption Scheme Based on the Cubic Pell Curve Using Encoding Functions

Author(s):

Abderrahmane Nitaj and Michel Seck

Moroccan Journal of Algebra and Geometry with Applications
Vol. 4(1) (2025), 89–107
Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco **ISSN: 2820-7114**

A New Public Key Encryption Scheme Based on the Cubic Pell Curve Using Encoding Functions

Abderrahmane Nitaj[1] and Michel Seck[2]

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

Communicated by Najib Mahdou
(Received 20 October 2024, Revised 30 November 2024, Accepted 19 December 2024)

Abstract. RSA is a public key encryption scheme introduced by Rivest, Shamir, and Adleman in 1978. Its security relies on the difficulty of factoring an integer $N = pq$ which is the product of two large prime numbers p and q. In 2018, Murru and Saettone proposed a variant of RSA, based on the cubic Pell curve with a modulus of the same form. Recently, Seck and Nitaj extended the scheme of Murru and Saettone to a prime power modulus of the form $N = p^r q^s$ where the ciphertexts C are represented as elements of $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, with a size of $3\log_2(N)$. In addition to the difficulty of factoring composite integers, the security of the scheme of Seck and Nitaj is based on Rabin's trapdoor one-way function. In this paper, we propose a new variant of the scheme of Seck and Nitaj where the ciphertext size is reduced to a size $2\log_2(N)$ instead of $3\log_2(N)$ for a fixed modulus N. This achievement is made possible through the incorporation of encoding and compression functions.

Key Words: Public Key Cryptography, cubic Pell curve, RSA variants, Encoding functions.
2020 MSC: Primary 94A60.

Dedicated to our Professor David E. Dobbs for his 80th Birthday.

1 Introduction

In 1976, Diffie and Hellman introduced the notion of a trapdoor one-way function, which allows two different entities to share the same secret key via a non-secure channel [14]. In 1978, the RSA cryptosystem was published by Rivest, Shamir, and Adleman [33]. RSA is suitable for both encryption and digital signature. In RSA, the public key is represented as $pk = (N, e)$, and the private key as $sk = (N, d)$, where $N = pq$ is the product of two prime numbers p and q. The public exponent $e \geq 3$ and the private exponent d are chosen so that $ed \equiv 1 \pmod{(p-1)(q-1)}$. To encrypt a message $m \in \mathbb{Z}/N\mathbb{Z}$ with the public key $pk = (N, e)$ or to decrypt a ciphertext c using the private key $sk = (N, d)$, the function $f_s(y) = y^s \pmod{N}$ is applied, where $(s, y) = (e, m)$ for encryption and $(s, y) = (d, c)$ for decryption.

The security of RSA is based on the difficulty of factoring large composite integers of the form $N = pq$. Certain vulnerabilities of RSA are known for specific forms of the prime factors p and q, or for the public exponent e and the secret exponent d [45, 29, 5, 7, 8, 9, 12, 44, 43]. For example, one can use Wiener's attack [45] to efficiently recover the private exponent d when $q < p < 2q$ and

$d < \frac{1}{3}N^{1/4}$. Using Coppersmith's method [12], Boneh and Durfee [9] have improved the bound up to $d < N^{0.292}$. On the other hand, RSA is vulnerable to Håstad's broadcast attack [18, 5] when e is small.

To design more efficient, and more resistant schemes than the standard RSA, numerous variants have been proposed. For instance, Takagi [42] proposed a variant of RSA with the modulus $N = p^k q$ to achieve a faster decryption process than RSA. This construction was later generalized by Lim, Kim, and Lee [25] with the modulus $N = p^r q^s$. Other variants of RSA have been proposed over non-singular or singular curves when a certain ring can be defined. Koyama, Maurer, Okamoto, and Vanstone [22] proposed three RSA-like cryptosystems, called KMOV, based on supersingular elliptic curves $E_b : y^2 = x^3 + b$ over $\mathbb{Z}/N\mathbb{Z}$ with $N = pq$ and $p \equiv q \equiv 2 \pmod 3$. In 1993, Demytko [13] proposed an RSA variant over elliptic curves in Weierstrass form $E_{a,b} : y^2 = x^3 + ax + b$ where only the x coordinates instead of the full points are used in the computations. A fast RSA type scheme based on the singular cubic curve $y^2 + axy = x^3 \pmod N$ was proposed by Koyama [21] in 1995. In the same year, Kuwakado, Koyama, and Tsuruoka [23] proposed another RSA-type scheme based on singular cubic curves $y^2 \equiv x^3 + bx^2 \pmod N$. Later on, Boudabra and Nitaj [10, 11] have proposed two variants with a multi-power modulus $N = p^r q^s$, the first one is based on supersingular elliptic curves $E_b : y^2 = x^3 + b$ and the second one on Edwards curves $E_d : -dx^2 + y^2 = 1 + dx^2y^2$. In 2018, Murru and Saettone [28] proposed an RSA-like cryptosystem over the cubic Pell curve $C_r : x^3 + ry^3 + r^2z^3 - 3rxyz \equiv 1 \pmod N$ with a modulus $N = pq$. Their scheme was recently generalized by Seck and Nitaj [39] over the cubic Pell curve with a prime power modulus $N = p^r q^s$. In the scheme of Seck and Nitaj, the ciphertext has size $3\log_2(N)$, and its security is based on the difficulty of factoring composite integers, and on Rabin's trapdoor one way function [31].

Our Contributions : In this paper, we propose a new RSA-like cryptosystem using the arithmetic of the cubic Pell curve $\mathcal{C}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod N$ where $N = p^r q^s$. The advantage of the new scheme over the scheme of Seck and Nitaj is that the bit-size of the ciphertext is minimized from $3\log_2(N)$ to $2\log_2(N)$. This bit-size reduction is possible by using encoding functions. Notice that, for several applications and design of cryptographic primitives, various encoding functions over finite fields have been proposed in the last decade for both elliptic and hyperelliptic curves [6, 20, 16, 4, 37, 38].

We summarize our contributions as follows.

- First encoding functions : For a modulus $N = \prod_{i=1}^{l} p_i$ where, for $i = 1, 2, \ldots, l$, p_i is a prime number, $p_i \neq p_j$ if $i \neq j$, and $p_i \equiv 2 \pmod 3$, we construct an injective and invertible encoding from $\mathbb{Z}/N\mathbb{Z}$ into the cubic Pell curve $\mathcal{C}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz = 1$ over $\mathbb{Z}/N\mathbb{Z}$. To this end, we adapt the cube-root encoding technique of Boneh and Franklin [6] as well as the technique of Icart[20] for elliptic curves to the cubic Pell curve.

- Second encoding functions : For the modulus $N = p^r q^s$ with $r, s \geq 1$, and $p \equiv q \equiv 1 \pmod 3$, we construct an efficient injective and invertible encoding that sends an element $(m_x, m_y) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ into a point $(x, y, z) \in \mathcal{C}_a(N)$ using the isomorphism constructed by Dutto and Murru [15] for the cubic Pell curve. This encoding function is used in our new scheme, especially in the reduction of the ciphertext.

- A new cryptosystem : We propose a new public key encryption scheme which is a generalization of the scheme of Murru and Saettone [28]. In the new scheme, we use a modulus of the form $N = p^r q^s$. The main advantages of our construction over the scheme of Seck and Nitaj [39] are two folds. (i) For a fixed modulus N, the ciphertexts of our scheme are of size $2\log_2(N)$ while they are of size $3\log_2(N)$ in the scheme of Seck and Nitaj. This improvement is possible by using injective and invertible encoding functions into the cubic Pell curve. (ii) Our scheme

can be used as a digital signature scheme while no such transformation is known for Seck and Nitaj cryptosystem.

- Security analysis : We analyze the security of the new scheme, specifically by studying its resistance to algebraic attacks based on the continued fraction algorithm and Coppersmith's technique. We also discuss how to get the CCA security using the OAEP transformation [3, 17, 40].

A proof of concept implementation of our scheme with SimulaMath [41] and SageMath [35] is provided in [36].

Paper Organization : The rest of this paper is organized as follows.
In Section 2, we recall some properties related to cubic residue modulo a prime, encoding functions and the arithmetic of the cubic Pell curve, especially over the ring $\mathbb{Z}/n\mathbb{Z}$. In Section 3, we construct encoding functions into the cubic Pell curve over $\mathbb{Z}/n\mathbb{Z}$ when $N = \prod_{i=1}^{l} p_i$, $p_i \equiv 2 \pmod 3$. In Section 4, we present our new scheme. The security analysis of our scheme is presented in Section 5. We conclude the paper in Section 6.

2 Preliminaries

In this section, we revisit some properties concerning cubic residues modulo prime powers and encoding functions into elliptic curves, with a particular emphasis on the Boneh and Franklin encoding[6]. Additionally, we explore properties associated with the cubic Pell curve $\mathcal{C}_a : x^3 + ay^3 + a^2z^3 - 3axyz = 1$ over a field $\mathbb{F}$ or the ring $\mathbb{Z}/N\mathbb{Z}$ where $N = p^r q^s$ is a prime power modulus.

2.1 Cubic residues modulo prime powers and encoding functions

Definition 2.1 (cubic residue)**.** Let p be a prime number. We say that an integer a is a cube (or 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.

Theorem 2.2 ([34])**.** Let $n = p^r$ be a prime power integer. 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 $d = \gcd(k, \phi(n))$ and $\phi(n) = p^{r-1}(p-1)$. If the congruence has a solution, then it actually has d incongruent solutions modulo n.

Corollary 2.3. *Let p be a prime number. An integer a is a cubic residue modulo p if and only if $a^{(p-1)/\gcd(3,p-1)} = 1$ in $\mathbb{Z}/p\mathbb{Z}$.*

Lemma 2.4 ([6, 20])**.** *Let $q = p^n$ be a prime power with $p \equiv 2 \pmod 3$ and $\mathbb{F}_q$ be a finite field with q elements. Then the map*

$$\mathbb{F}_q \to \mathbb{F}_q : x \mapsto x^3$$

is a bijection and the inverse function is given by

$$\mathbb{F}_q \to \mathbb{F}_q : y \mapsto y^{1/3} = y^{\frac{2q-1}{3}}.$$

The previous map allows to construct injection encoding functions into elliptic curve $E_{a,b} : y^2 = x^3 + ax + b$ over $\mathbb{F}_q$.

An elliptic curve E over $\mathbb{F}_p$ is called supersingular if it has exactly $p + 1$ points. When $p \equiv 2 \pmod 3$, the following result shows a first encoding in elliptic curves.

Lemma 2.5 (Boneh-Franklin encoding [6]). *Let $E_b : y^2 = x^3 + b$ be a supersingular elliptic curve over $\mathbb{F}_q$ with $q = p^n$, $p > 3$, and $p \equiv 2 \pmod 3$. Then the map*

$$\phi_1 : \mathbb{F}_q \to E_b : u \mapsto \left((u^2 - b)^{\frac{2q-1}{3}}, u\right)$$

is a one-to-one encoding and its inverse is given by $(x, y) \in E_b \mapsto y \in \mathbb{F}_q$.

2.2 The cubic Pell Curve over fields

The Pell hyperbola $H_d : x^2 - dy^2 = 1$ can be generalized in the cubic setting as

$$\mathcal{C}_a : x^3 + ay^3 + a^2z^3 - 3axyz = 1.$$

Let $\mathbb{F}$ be a field and let $a \in \mathbb{F}$. Define the quotient ring $R_a = \mathbb{F}[t]/\left(t^3 - a\right)$ where an element $w \in R_a$ is represented as $w = x + yt + zt^2$ with $(x, y, z) \in \mathbb{F}^3$. The product of two elements $w_1 = x_1 + y_1t + z_1t^2$ and $w_2 = x_2 + y_2t + z_2t^2$ of $\in R_a$ is defined by (see [1])

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

The norm of $w = x + yt + zt^2$ is defined by

$$N_a(w) = x^3 + ay^3 + a^2z^3 - 3axyz.$$

Consider the set $\mathcal{U}_a$ of unit 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 $\mathbb{F}$

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

The natural product on $\mathcal{U}_a$ induces the generalized Brahmagupta product on $\mathcal{C}_a$ that we also denote by $\oplus$. This product is 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 $w_1 = (x_1, y_1, z_1) \in \mathcal{C}_a$ and $w_2 = (x_2, y_2, z_2) \in \mathcal{C}_a$. Notice that $(\mathcal{C}_a, \oplus)$ is a group with neutral element $(1, 0, 0)$, and the inverse of $w = (x, y, z)$ is given by $w^{-1} = (x^2 - ayz, az^2 - xy, y^2 - xz)$.

Consider the quotient ring $\mathbb{B}_a = R_a^*/\mathbb{F}^*$. Then, an element $w = [x + yt + zt^2] = (x : y : z) \in \mathbb{B}_a$ is an equivalent class defined by

$$(x : y : z) = w = \left\{\lambda x + \lambda yt + \lambda zt^2 \in \mathbb{F}[t] : \lambda \in \mathbb{F}^*\right\}.$$

Any element $(x : y : z) \in \mathbb{B}_a$ can be rewritten as follows

$$(x : y : z) = \begin{cases} (x_1 : y_1 : 1) & \text{if } z \neq 0, \\ (x_2 : 1 : 0) & \text{if } z = 0 \text{ and } y \neq 0, \\ (1 : 0 : 0) & \text{if } y = z = 0. \end{cases}$$

With the product $\oplus$, $\mathbb{B}_a$ is a commutative group with identity $(1 : 0 : 0)$ and inverse of $(x : y : z)$ is given by $(x^2 - ayz : az^2 - xy : y^2 - xz)$.

Theorem 2.6 ([15]). Let $\mathbb{F}_q$ be a finite field with $q \equiv 1 \pmod 3$. Let b a non zero element of $\mathbb{F}_q$ and $a = b^3$. The map

$$\begin{aligned}\psi_b : (\mathbb{B}_a, \oplus) &\to (\mathcal{C}_a, \oplus)\\ (l:m:n) &\mapsto \left(\frac{l^3 + 2b^2l(m^2+bmn+b^2n^2) + b^4mn(m+bn)}{N_a((l,m,n))}, \right.\\ &\qquad \frac{b^2m^3 + 2m(l^2+b^2ln+b^4n^2) + bln(l+b^2n)}{N_a((l,m,n))},\\ &\qquad \left. \frac{b^5n^3 + 2bn(l^2+blm+b^2m^2) + lm(l+bm)}{bN_a((l,m,n))} \right)\end{aligned}$$

is a group isomorphism and the inverse ψ_b^{-1} is given by :

$$\begin{aligned}\psi_b^{-1} : (\mathcal{C}_a, \oplus) &\to (\mathbb{B}_a, \oplus)\\ (x,y,z) &\mapsto (b^2(1+2x-by-b^2z) : b(1-x+2by-b^2z) : 1-x-by+2b^2z)\end{aligned}$$

2.3 The cubic Pell Curve over $\mathbb{Z}/n\mathbb{Z}$ with $n = p^r q^s$

Proposition 2.7 ([39]). *Let N be integer greater that 3. Let a be an element of $\mathbb{Z}/N\mathbb{Z}$. The cubic Pell curve*

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

is nonsingular.

Theorem 2.8 ([39]). Let p, q be two prime numbers with $p, q \equiv 1 \pmod 3$, $p \neq q$. Let r and s be two positive integers and $N = p^r q^s$. Define the values

$$\begin{aligned}\psi_1(N) &= p^{2(r-1)}q^{2(s-1)}\left(p^2+p+1\right)\left(q^2+q+1\right),\\ \psi_2(N) &= p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2,\\ \psi_3(N) &= p^{2(r-1)}q^{2(s-1)}\left(p^2+p+1\right)(q-1)^2,\\ \psi_4(N) &= p^{2(r-1)}q^{2(s-1)}(p-1)^2\left(q^2+q+1\right).\end{aligned} \tag{1}$$

For $a \in \mathbb{Z}/N\mathbb{Z}$ with $\gcd(a, N) = 1$, the number of solutions of the cubic Pell curve equation $x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod N$ is then

$$|\mathcal{C}_a(N)| = \begin{cases}\psi_1(N) & \text{if } a \notin \mathcal{R}^3(p) \text{ and } a \notin \mathcal{R}^3(q),\\ \psi_2(N) & \text{if } a \in \mathcal{R}^3(p) \text{ and } a \in \mathcal{R}^3(q),\\ \psi_3(N) & \text{if } a \notin \mathcal{R}^3(p) \text{ and } a \in \mathcal{R}^3(q),\\ \psi_4(N) & \text{if } a \in \mathcal{R}^3(p) \text{ and } a \notin \mathcal{R}^3(q).\end{cases}$$

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.

A scalar multiplication $\otimes$ can be defined over $\mathcal{C}_a(N)$ as follows. For a solution $w = (x, y, z) \in \mathcal{C}_a(N)$ and an integer $n \geq 1$,

$$n \otimes (x,y,z) = \underbrace{(x,y,z) \oplus (x,y,z) \oplus (x,y,z) \ldots \oplus (x,y,z)}_{n \text{ times}}.$$

Lemma 2.9 ([39]). *Let $\mathcal{C}_a(N)$ be the set of the solutions of the cubic Pell curve $x^3+ay^3+a^2z^3-3axyz=1$ in $(\mathbb{Z}/N\mathbb{Z})^3$. Then $(\mathcal{C}_a(N),\oplus)$ is an abelian group with order $|\mathcal{C}_a(N)|$. The neutral element of $\mathcal{C}_a(N)$ is $(1,0,0)$ and the inverse of a solution $(x,y,z)\in\mathcal{C}_a(N)$ is $\left(x^2-ayz, az^2-xy, y^2-xz\right) \pmod N$. Furthermore for any positive integer k, and any solution $(x,y,z)\in\mathcal{C}_a(N)$,*

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

In $\mathcal{C}_a(N)$, the addition $(x_1,y_1,z_1)\oplus(x_2,y_2,z_2)$, the doubling $2\otimes(x_1,y_1,z_1)$, and the scalar multiplication by an integer $n\otimes(x_1,y_1,z_1)$ are summarized in the following algorithms [39].

Algorithm 1 Addition in $\mathcal{C}_a(N)$

Input: $N=p^rq^s$, $a\in\mathbb{Z}/N\mathbb{Z}\backslash\{0\}$, and $(x_1,y_1,z_1),(x_2,y_2,z_2)\in\mathcal{C}_a(N)$.
Output: $(x_3,y_3,z_3)=(x_1,y_1,z_1)\oplus(x_2,y_2,z_2)\in\mathcal{C}_a(N)$.
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 2 Doubling in $\mathcal{C}_a(N)$

Input: $N=p^rq^s$, $a\in\mathbb{Z}/N\mathbb{Z}\backslash\{0\}$, and $(x_1,y_1,z_1)\in\mathcal{C}_a(N)$.
Output: $(x_3,y_3,z_3)=2\otimes(x_1,y_1,z_1)\in\mathcal{C}_a(N)$.
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 3 Left-to-right scalar multiplication in $\mathcal{C}_a(N)$

Input: $N=p^rq^s$, $a\in\mathbb{Z}/N\mathbb{Z}\backslash\{0\}$, $(x_1,y_1,z_1)\in\mathcal{C}_a(N)$, and an integer $n\geq 2$.
Output: $(x_2,y_2,z_2)=n\otimes(x_1,y_1,z_1)\in\mathcal{C}_a(N)$.
1: $n:=(n_{k-1}n_{k-2}\dots n_1n_0)_2$.
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: Return (x_2,y_2,z_2).

3 Encoding into the cubic Pell curve

In this section, we construct two encoding functions into the cubic Pell curve

$$\mathcal{C}_a(N): x^3+ay^3+a^2z^3-3axyz=1$$

over $\mathbb{Z}/N\mathbb{Z}$.

3.1 Encoding into the cubic Pell curve when $N = \prod_{i=1}^{l} p_i$ with $p_i \equiv 2 \pmod 3$

The following result will be used to construct the first encoding.

Lemma 3.1. *Let $N = \prod_{i=1}^{l} p_i$ with distinct prime factors, and $\phi(N) = \prod_{i=1}^{l}(p_i - 1)$. Then, for all $a \in \mathbb{Z}/N\mathbb{Z}$ and all $k \geq 1$,*

$$a^{k\phi(N)+1} \equiv a \pmod N.$$

Proof. For $a = 0$, we have $0^{k\phi(N)+1} \equiv 0 \pmod N$. Suppose that $a \in \mathbb{Z}/N\mathbb{Z}$ with $0 < a < N$. Then $a = a_1 a_2$ where $\gcd(a_1, N) = 1$, and $\gcd(a_2, N) = q_1 \dots q_r$ where each q_i is a divisor of N. Set $Q = q_1 \dots q_r$, and $P = \frac{N}{Q}$. Let k be a positive integer. We have

$$a^{k\phi(N)+1} \equiv a_1^{k\phi(N)+1} a_2^{k\phi(N)+1} \equiv a_1 a_2^{k\phi(N)+1} \pmod N. \tag{2}$$

Since $\gcd(P, a_2) = 1$, then

$$a_2^{k\phi(N)} \equiv \left(a_2^{k\phi(P)}\right)^{\phi(Q)} \equiv 1 \pmod P,$$

or equivalently $a_2^{k\phi(N)} = 1 + Pz$ with an integer z. Since $a_2 \equiv 0 \pmod Q$, then

$$a_2^{k\phi(N)+1} \equiv a_2(1 + Pz) \equiv a_2 + Pa_2 z \equiv a_2 \pmod N.$$

Plugging this in (2), we get $a^{k\phi(N)+1} \equiv a_1 a_2 \equiv a \pmod N$. □

The following result concerns the cube map.

Proposition 3.2. *Let $N = \prod_{i=1}^{l} p_i$ with distinct prime factors, $p_i \equiv 2 \pmod 3$, and $\phi(N) = \prod_{i=1}^{l}(p_i - 1)$. The function*

$$\psi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z} : x \mapsto x^3,$$

is a bijection and its inverse is given by

$$\psi^{-1} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z} : y \mapsto y^{\frac{2\phi(N)+1}{3}}.$$

Proof. Since $N = \prod_{i=1}^{l} p_i$ with $p_i \equiv 2 \pmod 3$, then $p_i - 1 \equiv 1 \pmod 3$, and

$$\phi(N) = \prod_{i=1}^{l}(p_i - 1) \equiv 1 \pmod 3.$$

Hence $2\phi(N) + 1 \equiv 0 \pmod 3$, and $\frac{2\phi(N)+1}{3}$ is an integer. This sows that ψ^{-1} is well defined.

To show that ψ is bijective, if suffices to show that $\psi \circ \psi^{-1} = 1_{\mathbb{Z}/N\mathbb{Z}}$ and that $\psi^{-1} \circ \psi = 1_{\mathbb{Z}/N\mathbb{Z}}$. Using Lemma 3.1, we get

$$\psi^{-1} \circ \psi(y) \equiv \psi \circ \psi^{-1}(y) \equiv y^{2\phi(N)+1} \equiv y \pmod N.$$

□

The following result shows how to encode from $\mathbb{Z}/N\mathbb{Z}$ into the cubic Pell curve $\mathcal{C}_a(N)$. It employs a technique similar to the Boneh-Franklin encoding defined in Lemma 2.5.

Proposition 3.3. *Let $N = \prod_{i=1}^{l} p_i$ with distinct prime factors, $p_i \equiv 2 \pmod 3$, and $\phi(N) = \prod_{i=1}^{l}(p_i - 1)$. For $a \in \mathbb{Z}/N\mathbb{Z}$ with $a \neq 0$, let $\mathcal{C}_a(N) : x^3 + ay^3 + a^2 z^3 - 3axyz = 1$ be a cubic Pell curve over $\mathbb{Z}/N\mathbb{Z}$. The map*

$$f_a : \mathbb{Z}/N\mathbb{Z} \to \mathcal{C}_a(N) : u \mapsto \left((1 - au^3)^{\frac{2\phi(N)+1}{3}}, u, 0\right).$$

is an injective and invertible encoding.

Proof. For $u \in \mathbb{Z}/N\mathbb{Z}$, let $x = (1-au^3)^{\frac{2\phi(N)+1}{3}} \pmod N$, $y = u \pmod N$ and $z = 0 \pmod N$. Then, using Lemma 3.1, we get

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

Thus f_a is well defined. Clearly f_a is injective, and for any $(m,u,0) \in \mathrm{Im}(f_a)$, $f_a(u) = (m,u,0)$. This show that f_a is invertible. □

Notice that in the previous Proposition, we have encoded an element $u \in \mathbb{Z}/N\mathbb{Z}$ into a point in the form $(x_u, y_u, 0) \in \mathcal{C}_a(N)$. One can also encode an element $v \in \mathbb{Z}/N\mathbb{Z}$ into a point in the form $(x_v, 0, z_v) \in \mathcal{C}_a(N)$ by the map

$$g_a : \mathbb{Z}/N\mathbb{Z} \to \mathcal{C}_a(N) : v \mapsto \left(\left(1-a^2v^3\right)^{\frac{2\phi(N)+1}{3}}, 0, v\right).$$

Similarly, an element $w \in \mathbb{Z}/N\mathbb{Z}$ can be encoded into a point in the form $(0, y_w, z_w) \in \mathcal{C}_a(N)$ by the map

$$h_a : \mathbb{Z}/N\mathbb{Z} \to \mathcal{C}_a(N) : w \mapsto \left(0, \left(a^{-1}\left(1-a^2w^3\right)\right)^{\frac{2\phi(N)+1}{3}}, w\right).$$

3.2 Encoding into the cubic Pell curve when $p_i \equiv 1 \pmod 3$

In this section, we consider the situation where the modulus is in the form $N = p^r q^s$ with small positive integers r and s, where p, q are two distinct primes satisfying $p, q \equiv 1 \pmod 3$.

An encoding function. Let $N = p^r q^s$ be a prime power modulus, and $b \in \mathbb{Z}/N\mathbb{Z}$ with $b \neq 0$. The map ψ_b in Theorem 2.6 can be used to encode into the cubic Pell curve $\mathcal{C}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod N$ where $a = b^3 \pmod N$. In Algorithm 4, we show how to encode an element $(m_x, m_y) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ into a point $(x,y,z) \in \mathcal{C}_a(N)$ using ψ_b.

Algorithm 4 The encoding algorithm **Encode2Curve**$((m_x, m_y), b, N)$

Input: An integer N, an element $b \in \mathbb{Z}/N\mathbb{Z}$, a couple $(m_x, m_y) \in (\mathbb{Z}/N\mathbb{Z})^2$
Output: A point $(x,y,z) \in \mathcal{C}_a(N)$ with $a \equiv b^3 \pmod N$.

1: $a := b^3 \pmod N$;
2: $(l,m,n) := (m_x, m_y, 1)$; ▷ $(l:m:n) \in \mathbb{B}_a$
3: $x_2 := l^3 + 2b^2l(m^2 + bmn + b^2n^2) + b^4mn(m + bn) \pmod N$;
4: $y_2 := b^2m^3 + 2m(l^2 + b^2ln + b^4n^2) + bln(l + b^2n) \pmod N$;
5: $z_2 := b^5n^3 + 2bn(l^2 + blm + b^2m^2) + lm(l + bm) \pmod N$;
6: $g := (l^3 + am^3 + a^2n^3 - 3almn) \pmod N$
7: $x := \left(x_2g^{-1}\right) \pmod N$; $y := \left(y_2g^{-1}\right) \pmod N$; $z := \left(z_2(bg)^{-1}\right) \pmod N$;
8: **return** (x,y,z)

A straightforward calculation shows that

$$x^3 + ay^3 + a^2z^3 - 3axyz = 1,$$

and that Algorithm 4 is correct. Moreover, this algorithm is well defined if and only if $g := x_m^3 + ay_m^3 + a^2 - 3ax_my_m \pmod N$ and b are invertible in $\mathbb{Z}/N\mathbb{Z}$, that is $\gcd(bg, N) = 1$. This condition is satisfied with overwhelming probability since otherwise, a factor of N can be found. So as well as the problem of factoring large composite integers is difficult, we can assume that g and b are invertible modulo N.

Decoding function. The map ψ_b^{-1} in Theorem 2.6 can be used to decode from the cubic Pell curve $\mathcal{C}_a(N): x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod N$ where $a = b^3 \pmod N$. In Algorithm 5, we show how to decode a point $(x, y, z) \in \mathcal{C}_a(N)$ to get the corresponding point $(m_x, m_y) \in (\mathbb{Z}/N\mathbb{Z})^2$ using ψ_b^{-1}.

Algorithm 5 The decoding algorithm **DecodeFromCurve**$((x, y, z), b, N)$

Input: An integer N, $b \in \mathbb{Z}/N\mathbb{Z}$, $(x, y, z) \in \mathcal{C}_a(N)$ with $a = b^3$.
Output: $(m_x, m_y) \in (\mathbb{Z}/N\mathbb{Z})^2$.

1: $a := b^3 \pmod N$;
2: $x_2 := b^2(1 + 2x - by - b^2z) \pmod N$;
3: $y_2 := b(1 - x + 2by - b^2z) \pmod N$;
4: $z_2 := 1 - x - by + 2b^2z \pmod N$;
5: $g := z_2^{-1} \pmod N$
6: $m_x := (x_2 g) \pmod N$; $m_y := (y_2 g) \pmod N$; ▷ $(m_x : m_y : 1) \in \mathbb{B}_a$
7: **return** (m_x, m_y)

Notice that in the computation of DecodeFromCurve$((x, y, z), b, N)$, the point $(x_2 : y_2 : z_2) \in \mathbb{B}_a$ can be uniquely represented in the form $(x_2/z_2 : y_2/z_2 : 1)$ as well as z_2 is invertible modulo N, which will happen with overwhelming probability. Also the following properties hold, with overwhelming probability

$$\text{DecodeFromCurve}\Big(\text{Encode2Curve}((m_x, m_y), b, N), b, N\Big) = (m_x, m_y), \tag{3}$$

and

$$\text{Encode2Curve}\,(\text{DecodeFromCurve}((x, y, z), b, N), b, N) = (x, y, z). \tag{4}$$

4 A New RSA-like Scheme

In this section, we propose a new public key encryption scheme as an RSA variant. It could be also categorized as a variant of the scheme of Murru and Saettone [28] for two reasons.

- In our scheme, the modulus is $N = p^r q^s$, while it is $N = pq$ in the scheme of Murru and Saettone.
- In our scheme, we use cubic residues $a \equiv b^3 \pmod N$ to construct the cubic Pell curve, while in the scheme of Murru and Saettone, a is a cube non-residue. As a consequence, in our scheme, the public and the private exponents satisfy $ed \equiv 1 \pmod{p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2}$ while they satisfy $ed \equiv 1 \pmod{\Big(p^2 + p + 1\Big)\Big(q^2 + q + 1\Big)}$ in the scheme of Murru and Saettone.

4.1 The new scheme

In the following Figure 1, we describe the template of our scheme. It uses encoding/decoding functions and compression/decompression functions.

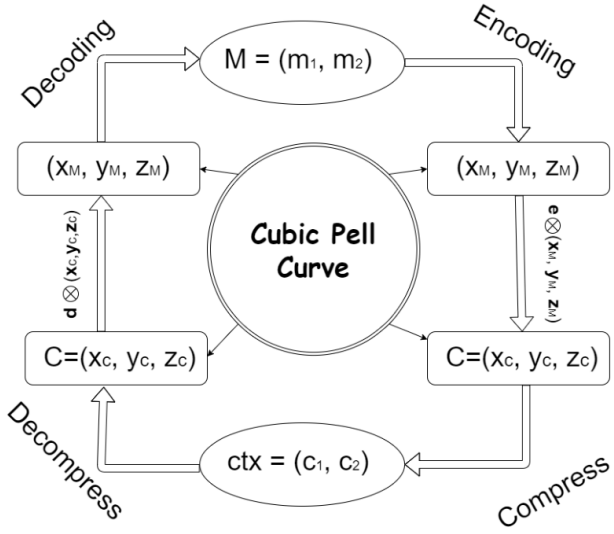

Figure 1: Template of our public key encryption scheme with compression

The key generation, encryption, and decryption phases are described in Algorithm 6, 7, and 8 respectively.

Algorithm 6 Key Generation

Input: A security parameter λ, and two small positive integers r and s.
Output: A public key pk and a private key sk.

1: Choose randomly a prime number p of λ bits with $p \equiv 1 \pmod 3$.
2: Choose randomly a prime number q of λ bits with $q \equiv 1 \pmod 3$.
3: Compute $N = p^r q^s$.
4: Choose randomly an integer $b \in \mathbb{Z}/N\mathbb{Z}$ such that $a = b^3 \pmod N$ is nonzero cubic residue modulo p and modulo q.
5: Choose an integer $e \in \mathbb{Z}/N\mathbb{Z}$ with $\gcd(e, pq(p-1)(q-1)) = 1$.
6: Compute

$$d \equiv e^{-1} \pmod{p^{2(r-1)} q^{2(s-1)} (p-1)^2 (q-1)^2}.$$

7: The public key is $pk = (N, b, e)$.
8: The private key is $sk = (N, b, d)$.
9: Return the key pair (pk, sk).

Algorithm 7 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 $pk = (N, b, e)$.
Output: The ciphertext of M.

1: Compute $a := b^3 \pmod N$;
2: $(x, y, z) :=$ Encode2Curve$((x_M, y_M), b, N)$; ▷ Encoding of M into $\mathcal{C}_a(N)$
3: Compute $C = (x_C, y_C, z_C) := e \otimes (x, y, z)$ on the cubic Pell curve $\mathcal{C}_a(N)$;
4: $(c_x, c_y) :=$ DecodeFromCurve(C, b, N); ▷ Compression of C
5: Return the ciphertext $ctx = (c_x, c_y)$.

Algorithm 8 Decryption Process

Input: A ciphertext $ctx = (c_x, c_y) \in (\mathbb{Z}/N\mathbb{Z})^2$ and a private key $sk = (N, b, d)$.
Output: The decryption of C.

1: Compute $a := b^3 \pmod N$;
2: $(x_C, y_C, z_C) :=$ Encode2Curve$((c_x, c_y), b, N)$; ▷ Decompression of the ciphertext
3: Compute $(x, y, z) := d \otimes (x_C, y_C, z_C)$ on the cubic Pell curve $\mathcal{C}_a(N)$;
4: $(x_m, y_m) :=$ DecodeFromCurve$((x, y, z), b, N)$; ▷ Decoding of the point (x, y, z)
5: Return the plaintext (x_m, y_m)

Notice that at Line 4 in the encryption Algorithm 7, the compression function specified in the template of our scheme (Figure 1) is instantiated by the decoding function DecodeFromCurve which is the inverse of encoding function Encode2Curve. It means that in our scheme, the compression function and the decoding function are the same as well as the decompression function and the encoding function.

Encryption/Decryption Failures : The encryption process of a message $M = (x_M, y_M) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ fails when the encoding into $\mathcal{C}_a(N)$ of (x_M, y_M) or the compression process DecodeFromCurve(C, b, N) in Line 4 of Algorithm 7 fails. This occurs only when g defined in Algorithm 4 and 5 are not invertible modulo N. We know that with overwhelming probability $\gcd(g, N) = 1$; otherwise, a factor of N can be efficiently found. Similarly, the decryption process of a ciphertext $ctx = (c_x, c_y) \in (\mathbb{Z}/N\mathbb{Z})^2$ will be done correctly; otherwise, a factor of N can be found. Therefore, we can assume that the encryption and decryption process will be error-free whenever the problem of factoring large composite integers N is difficult.

4.2 A numerical example for the new scheme

In this subsection, we present a numerical example with all computation details. Notice that a proof of concept implementation of our scheme with SimulaMath [41] and SageMath [35] is provided in [36].

- **Key Generation :** Let $p = 877636073161$, $q = 427943630539$, $r = 1$ and $s = 2$. Then

$$N = p \times q^2 = 160726541291854510481081390266346881.$$

Consider the parameters

$$e = 130172055750281760449762497750803727,$$
$$b = 89196535984971849298838982218600 16.$$

We can then compute

$$\begin{aligned}\psi(N) &= p^{2(r-1)} q^{2(s-1)} (p-1)^2 (q-1)^2 \\ &= 258330210754626124707135160100591316232211010 6588\backslash \\ &\quad 6025452264850972934400, \\ d &\equiv e^{-1} \pmod{\psi(N)} \\ &= 220088664496335695890253540969892081673932767809 61\backslash \\ &\quad 045235918145369812463.\end{aligned}$$

The public key is $pk = (N, b, e)$ and the private key is $sk = (N, b, d)$.

- **Encryption :** Consider the plaintext $M = (m_1, m_2)$ with

$$m_1 = 301193270699565353432935824284814 97,$$
$$m_2 = 874496077175839632169740386605913 67.$$

To encrypt using the public key $pk = (N, b, e)$, one first computes

$$a \equiv b^3 \pmod{N} \equiv 110984846909034778402177655906954357,$$

and defines the cubic Pell curve

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

One then encodes the message (m_1, m_2) into $\mathcal{C}_a(N)$ using Algorithm 4. This gives (x_M, y_M, z_M) with

$$x_M = 140951064022017564592779260398752129,$$
$$y_M = 148299166162508601153120654776829594,$$
$$z_M = 145736964847022157345025797688945229.$$

Then, one computes $(x_C, y_C, z_C) = e \otimes (x_M, y_M, z_M)$ on $\mathcal{C}_a(N)$ using Algorithm 3. This gives

$$x_C = 614001465150212997844506822042966 04,$$
$$y_C = 110225425660605993200354996873666 42,$$
$$z_C = 615076344946219679236750583864483 09.$$

To compress (x_C, y_C, z_C), one uses Algorithm 3. This gives (c_1, c_2) where

$$c_1 = 119272817221858365069165947063984272,$$
$$c_2 = 108837536797780384448758029507481222.$$

Then (c_1, c_2) is the ciphertext to be transmitted to the recipient.

- **Decryption :** To decrypt the ciphertext (c_x, c_y) using the private key $sk = (N, b, d)$, one first decodes it to (x_C, y_C, z_C) using Algorithm 4, and obtain

$$x_C = 614001465150212997844506822042966 04,$$
$$y_C = 110225425660605993200354996873666 42,$$
$$z_C = 615076344946219679236750583864483 09.$$

Then, using Algorithm 3, one computes $(x_M, y_M, z_M) = d \otimes (x_C, y_C, z_C)$ on $\mathcal{C}_a(N)$, and obtain

$$x_M = 140951064022017564592779260398752129,$$
$$y_M = 148299166162508601153120654776829594,$$
$$z_M = 145736964847022157345025797688945229.$$

Finally, one decodes (x_M, y_M, z_M) using Algorithm 5 to get the plaintext $M = (m_1, m_2)$ with

$$m_1 = 301193270699565353432935824284814 97,$$
$$m_2 = 874496077175839632169740386605913 67.$$

5 Security Analysis

In this section, we analyze the security of the new scheme by presenting two possible attacks. The first attack is based on the continued fraction algorithm, and the second is based on Coppersmith's method [12]. Both attacks are based on the modular relation $ed \equiv 1 \pmod{p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2}$ between the public exponent e and the private exponent d.

5.1 A possible attack with the continued fraction algorithm

In [39], Seck and Nitaj studied the equation

$$ed - kp^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2 = 1,$$

and showed that, when d is sufficiently small, it can be found among the denominators of the convergents of the continued fraction expansion of $\frac{e}{N^2}$. The bound of d is presented in the following result.

Theorem 5.1. [39] Let $N = p^r q^s$ be a prime power modulus with $q < p < 2q$. Let e be a public exponent, and d be the private exponent satisfying $d \equiv e^{-1} \pmod{\psi(N)}$ where $\psi(N) = p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2$. 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.

5.2 A possible attack with Coppersmith's method

Coppersmith's method [12] is a technique based on lattice basis reduction used to find the small solutions of polynomial equations. It is intensively deployed for the cryptanalysis of RSA and its variants. For univariate polynomial equations, it relies on the following two important results.

Theorem 5.2 (LLL [24, 27]). Let $\mathcal{L}$ be a lattice with a basis $(u_1, \ldots, u_\omega)$. The LLL algorithm outputs a new basis $(b_1, \ldots, b_\omega)$ of $\mathcal{L}$ satisfying

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

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

Theorem 5.3 (Howgrave-Graham [19]). Let $h(x) = \sum a_i x^i \in \mathbb{Z}[x]$ be a polynomial with at most ω monomials and norm

$$\|h(x)\| = \sqrt{\sum a_i^2}.$$

Let M be a positive integer. If $|y| < X$, and

$$h(y) \equiv 0 \pmod{M}, \quad \|h(Xx)\| < \frac{M}{\sqrt{\omega}},$$

then $h(y) = 0$ holds over the integers.

Using the former two theorems, the following result gives a lower bound for d in our scheme. Note that, in [26, 30], related methods have been used to solve the equations $ed \equiv 1 \pmod{p^{r-1}q^{l-1}}$ and $ex \equiv z \pmod{p^{r-1}q^{s-1}}$ respectively.

Theorem 5.4. Let $N = p^r q^s$ be an RSA prime power modulus with $r > s \geq 1$ where p and q are of the same bit-size. Let e be a public exponent satisfying $ed \equiv 1 \pmod{p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2}$ with $d < N^\delta$. Then, one can factor N in polynomial time if

$$\delta < 2 - \frac{2(3r+s)}{(r+s)^2}.$$

Proof. Let $N = p^r q^s$ with $r > s \geq 1$, and $\psi(N) = p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2$. The equation $ed \equiv 1 \pmod{\psi(N)}$ implies that $ed - 1 \equiv 0 \pmod{p^{2(r-1)}q^{2(s-1)}}$. Let $a \equiv e^{-1} \pmod{N}^2$. Then $x_0 = d$ is solution of the equation $f(x) = x - a$ modulo $p^{2(r-1)}q^{2(s-1)}$.

Let m, t_1, and t_2 be three parameters to be optimized later with $t_1 < t_2$. Let

$$k_0 = \left\lceil \frac{s(r-1)t_1 - r(s-1)t_2}{r-s} \right\rceil,$$

be the smallest integer k such that

$$\left\lceil \frac{2(s-1)(t_2-k)}{s} \right\rceil \geq \left\lceil \frac{2(r-1)(t_1-k)}{r} \right\rceil.$$

We can check that $k_0 \leq t_1 < t_2$.

For $k = 0, \ldots, m$, consider the polynomials

$$G_k(x) = \begin{cases} f(x)^k & \text{if } t_2 \leq k, \\ f(x)^k N^{\left\lceil \frac{2(s-1)(t_2-k)}{s} \right\rceil} & \text{if } k_0 \leq k < t_2, \\ f(x)^k N^{\left\lceil \frac{2(r-1)(t_1-k)}{r} \right\rceil} & \text{if } k < k_0. \end{cases}$$

Since $f(x_0) \equiv 0 \pmod{p^{2(r-1)}q^{2(s-1)}}$, then we get

$$G_k(x_0) \equiv 0 \pmod{p^{2(r-1)t_1}q^{2(s-1)t_2}}.$$

Let $X = N^\delta$ be an upper bounds for $x_0 = d$. Consider the lattice $\mathcal{L}$ generated by the matrix where the rows are spanned by the coefficients of the polynomials $G_k(xX)$. The matrix is triangular if we consider the ordering $G_k(xX) \prec G_{k'}(xX)$ if $k < k'$. Similarly, the columns are ordered following the rule that $x^k \prec x^{k'}$ if $k < k'$.

Since the matrix of the lattice is triangular, its determinant is the product of the diagonal terms, that is

$$\det(\mathcal{L}) = X^{e_X} N^{e_N}, \tag{5}$$

where $e_X = \sum_{k=0}^{m} k = \frac{1}{2}m(m+1)$. The dimension of the lattice is $\omega = \sum_{k=0}^{m} 1 = m+1$. Using k_0, the exponent e_N can be computed as

$$e_N = \sum_{k=0}^{k_0-1} \left\lceil \frac{2(r-1)(t_1-k)}{r} \right\rceil + \sum_{k=k_0}^{t_2} \left\lceil \frac{2(s-1)(t_2-k)}{s} \right\rceil.$$

We set $t_1 = \tau_1 m$, and $t_2 = \tau_2 m$. Then, the dominant parts in e_X and e_N are

$$e_X = \frac{1}{2}m^2 + o\left(m^2\right), \tag{6}$$

$$e_N = \frac{r-1}{r(r-s)}\left(rs(\tau_1-\tau_2)^2 + 2r\tau_1\tau_2 - r\tau_2^2 - s\tau_1^2\right)m^2 + o\left(m^2\right). \tag{7}$$

Next, apply the LLL algorithm to the lattice $\mathcal{L}$. It outputs a new matrix with reduced vectors. Collecting the rows of the new matrix, we build ω polynomials $h_j(xX)$ with $j = 1,\dots,\omega$ satisfying $h_j(x_0) \equiv 0 \pmod{p^{2(r-1)t_1} q^{2(s-1)t_2}}$. Taking $i = 1$ in Theorem 5.2, we get

$$\|h_1(xX)\|\| \leq 2^{\frac{\omega-1}{4}} \det(L)^{\frac{1}{\omega}}.$$

Then, to use Theorem 5.3, we let

$$2^{\frac{\omega-1}{4}} \det(\mathcal{L})^{\frac{1}{\omega}} < \frac{p^{2(r-1)t_1} q^{2(s-1)t_2}}{\sqrt{\omega}}.$$

Since p and q are of the same bit size, then $p \approx q \approx N^{\frac{1}{r+s}}$. Using this with $\det(\mathcal{L}) = X^{e_X} N^{e_N}$ where $X = N^{\delta}$, the former inequality becomes

$$2^{\frac{\omega-1}{4}} \left(N^{\delta e_X} N^{e_N}\right)^{\frac{1}{\omega}} < \frac{N^{\frac{2(r-1)t_1 + 2(s-1)t_2}{r+s}}}{\sqrt{\omega}}.$$

Then, using $t_1 = m\tau_1$, $t_2 = m\tau_2$, (6), (7), and solving the former inequality, we get $\delta < F(\tau_1, \tau_2)$ where

$$F(\tau_1, \tau_2) = \frac{4((r-1)\tau_1 + (s-1)\tau_2)}{r+s} - \frac{2(r-1)}{r(r-s)} \left(rs(\tau_1 - \tau_2)^2 + 2r\tau_1\tau_2 - r\tau_2^2 - s\tau_1^2\right).$$

The optimal values for τ_1 and τ_2 are obtained by solving the system of equations

$$\frac{\partial F}{\partial \tau_1}(\tau_1, \tau_2) = 0, \quad \frac{\partial F}{\partial \tau_2}(\tau_1, \tau_2) = 0.$$

This gives the following values

$$\tau_1^{(0)} = \frac{r(r+s-2)}{r^2 + rs - r - s}, \quad \tau_2^{(0)} = 1.$$

Plugging these values in the bound of δ, we get

$$\delta < F\left(\tau_1^{(0)}, \tau_2^{(0)}\right) = 2 - \frac{2(3r+s)}{(r+s)^2}.$$

Under this condition, one can solve the equation $h_1(x) = 0$ over the integers and get the root $x_0 = d$. Then, using d, we get

$$g = \gcd(ed - 1, N^2) = p^{2(r-1)} q^{2(s-1)}, \quad pq = \sqrt{\frac{N^2}{g}},$$

and finally

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

This completes the proof. □

5.3 On IND-CPA and CCA Security

It is well known that deterministic public key encryption schemes, including plain RSA, are not secure neither under the chosen-ciphertext attack (CCA) [2] nor meet the indistinguishability under chosen-plaintext attack (IND-CPA) [2]. Bellare and Rogaway [3] published the Optimal Asymmetric Encryption Padding (OAEP) framework at Eurocrypt 1994, which can transform a partial-domain one-way trapdoor permutation scheme into a CCA [2] secure cryptosystem in the random oracle model. When the OAEP transformation is instantiated with plain RSA, we get the RSA-OAEP cryptosystem which is shown to be CCA2 secure [17] in the random oracle model under the RSA assumption. Later Shoup [40, 32] proposed OAEP+ transformation, a slight modification of OAEP which allows to get a CCA secure cryptosystem from a one-way trapdoor permutation scheme.

To transform our scheme into an IND-CPA and CCA secure public key encryption scheme, we apply the OAEP+ framework as follows.

Let $N = p^r q^s$ be a $k+1$ bit integer with p and q prime. Let $(\mathrm{KGen}, \mathcal{E}, \mathcal{D})$ our public key encryption scheme defined by Algorithms 6, 7 and 8. Let n, k_0 and k_1 be integers such that $n + k_1 = k$ and $k_0 \leq k$. Define the random functions $G : \{0,1\}^{k_0} \to \{0,1\}^n$, $H : \{0,1\}^{n+k_1} \to \{0,1\}^{k_0}$ and $H' : \{0,1\}^{n+k_0} \to \{0,1\}^{k_1}$. For a binary vector $b = b_0 b_1 b_2 \dots b_i b_{i+1} \dots b_j b_{j+1} \dots b_k$, we denote by $b[i \dots j]$ the partial binary vector $b_i b_{i+1} \dots b_j$.

- Key Generation: Generate (pk, sk) with Algorithm 6. Then the public key is the function $\mathcal{E}_{pk} : (x_1, x_2) \mapsto \mathcal{E}((x_1, x_2), pk)$, and the private key is the function $\mathcal{D}_{sk} : (y_1, y_2) \mapsto \mathcal{D}((y_1, y_2), sk)$.
- Encryption process: To encrypt a message $m \in \{0,1\}^n$ with the public key $\mathcal{E}_{pk}$, proceed as follows. First, pick a random value $r \in \{0,1\}^{k_0}$. Then compute $s = (G(r) \oplus m) \parallel H'(r \parallel m)$ and $t = r \oplus H(s)$ where $\parallel$ means concatenation. Finally, output $c = \mathcal{E}_{pk}(s, t)$.
- Decryption process: To decrypt a ciphertext c with the secret key $\mathcal{D}_{sk}$, compute $(s, t) = \mathcal{D}_{sk}(c)$, then $r = t \oplus H(s)$, $m = s[0 \dots n-1] \oplus G(r)$ and $y = s[n \dots n + k_1 - 1]$. If $y = H'(r \parallel m)$ return m; otherwise return $\perp$.

6 Conclusion

We presented a study of three topics related to the cubic Pell curve $\mathcal{C}_a(N) : x^3 + ay^3 + a^2 z^3 - 3axyz \equiv 1 \pmod N$ where N is a composite integer, and $a \in \mathbb{Z}/N\mathbb{Z}$. The first topic shows how to encode and decode from $\mathbb{Z}/N\mathbb{Z}$ into $\mathcal{C}_a(N)$ when $N = \prod_{i=1}^{l} p_i$ with distinct prime factors, $p_i \equiv 2 \pmod 3$. The second topic shows how to encode and decode from $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ into $\mathcal{C}_a(N)$ when $N = p^r q^s$, $p \equiv q \equiv 1 \pmod 3$. The third topic presents a new scheme based on the arithmetic of the cubic Pell equation, and on encoding and decoding functions for efficiency reasons. The security of the new scheme is analyzed.

References

[1] E. J. Barbeau, Pell equation, Chapter 7: The Cubic Analogue of Pell Equation. Springer, New York (2003).

[2] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway, Relations among notions of security for public-key encryption schemes. In: Crypto '98, Lect. Notes Comput. Sci., 1462, Springer-Verlag, Berlin (1998), 26–45.

[3] M. Bellare and P. Rogaway, Optimal asymmetric encryption: how to encrypt with RSA. In: Eurocrypt '94, Lect. Notes Comput. Sci., 950, Springer-Verlag, Berlin (1995), 92–111.

[4] D. J. Bernstein, M. Hamburg, A. Krasnova and T. Lange, Elligator: elliptic-curve points indistinguishable from uniform random strings. In: V. Gligor, M. Yung (eds.) CCS, ACM (2013).

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

[6] D. Boneh and M. K. Franklin, Identity-based encryption from the Weil pairing. In: J. Kilian (ed.), CRYPTO, Lect. Notes Comput. Sci., 2139, Springer (2001), 213–229.

[7] D. Boneh, G. Durfee and Y. Frankel, An attack on RSA given a small fraction of the private key bits. In: ASIACRYPT (1998), 25–34.

[8] D. Boneh, G. Durfee and N. Howgrave-Graham, Factoring $N = p^r q$ for large r. In: CRYPTO (1999), 326–337.

[9] D. Boneh and G. Durfee, Cryptanalysis of RSA with private key d less than $N^{0.292}$. In: Eurocrypt '99, Lect. Notes Comput. Sci., 1592, Springer-Verlag (1999), 1–11.

[10] M. Boudabra and A. Nitaj, A new generalization of the KMOV cryptosystem. J. Appl. Math. Comput., 57(1–2) (2017), 229–245.

[11] M. Boudabra and A. Nitaj, A new public key cryptosystem based on Edwards curves. J. Appl. Math. Comput., 61 (2019), 431–450.

[12] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptol., 10(4) (1997), 233–260.

[13] N. Demytko, A new elliptic curve based analogue of RSA. In: T. Helleseth (ed.), Eurocrypt 1993, Lect. Notes Comput. Sci., 765, Springer-Verlag (1994), 40–49.

[14] W. Diffie and M. Hellman, New directions in cryptography. IEEE Trans. Inf. Theory, 22(6) (1976), 644–654.

[15] S. Dutto and N. Murru, On the cubic Pell equation over finite fields. arXiv:2203.05290 (2022).

[16] P. A. Fouque, A. Joux and M. Tibouchi, Injective encodings to elliptic curves. In: Information Security and Privacy, 18th Australasian Conference, ACISP 2013, Lect. Notes Comput. Sci., Springer, Berlin Heidelberg (2013), 203–218.

[17] E. Fujisaki, T. Okamoto, D. Pointcheval and J. Stern, RSA-OAEP is secure under the RSA assumption. In: Annual Int. Cryptology Conf., Lect. Notes Comput. Sci., Springer, Berlin Heidelberg (2001), 260–274.

[18] J. Hastad, Using RSA with low exponent in a public key network. In: Advances in Cryptology—CRYPTO '85, Lect. Notes Comput. Sci., 5, Springer-Verlag (1986), 403–408.

[19] N. Howgrave-Graham, Finding small roots of univariate modular equations revisited. In: Cryptography and Coding, Lect. Notes Comput. Sci., 1355, Springer-Verlag (1997), 131–142.

[20] T. Icart, How to hash into elliptic curves. In: Annual Int. Cryptology Conf., Lect. Notes Comput. Sci., Springer, Berlin Heidelberg (2009), 303–316.

[21] K. Koyama, Fast RSA type scheme based on singular cubic curve $y^2 + axy = x^3 \pmod{n}$. Lect. Notes Comput. Sci., 921 (1995), 329–339.

[22] K. Koyama, U. M. Maurer, T. Okamoto and S. A. Vanstone, New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$. Lect. Notes Comput. Sci., 576 (1991), 252–266.

[23] 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 (1995), 27–33.

[24] A. K. Lenstra, H. W. Lenstra and L. Lovász, Factoring polynomials with rational coefficients. Math. Ann., 261 (1982), 513–534.

[25] S. Lim, S. Kim, I. Yie and H. Lee, A generalized Takagi-cryptosystem with a modulus of the form $p^r qs$. In: Indocrypt, Springer (2000), 283–294.

[26] Y. Lu, L. Peng and S. Sarkar, Cryptanalysis of an RSA variant with moduli $N = p^r q^l$. 9th Int. Workshop Coding Cryptogr. (2015), Paris, France. https://inria.hal.science/hal-01276463/document.

[27] A. May, New RSA vulnerabilities using lattice reduction methods. PhD Thesis, Univ. Paderborn (2003). https://digital.ub.uni-paderborn.de/ubpb/urn/urn:nbn:de:hbz:466-20030101205.

[28] N. Murru and F. M. Saettone, A novel RSA-like cryptosystem based on a generalization of the Rédei rational functions. Lect. Notes Comput. Sci., 10737 (2018), Springer, Cham.

[29] A. Nitaj, Another generalization of Wiener's attack on RSA. Lect. Notes Comput. Sci., 5023 (2008), 174–190.

[30] A. Nitaj, W. Susilo and J. Tonien, A generalized attack on the multi-prime power RSA. Lect. Notes Comput. Sci., 13503 (2022), 537–549.

[31] M. O. Rabin, Digitalized signatures and public key functions as intractable as factorisation. MIT/LCS/TR-212 (1979).

[32] D. Pointcheval, How to encrypt properly with RSA. CryptoBytes, 5(1) (2002), 10–19.

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

[34] K. H. Rosen, Elementary Number Theory and Its Applications. Addison-Wesley, 3rd ed. (1993), 285–302.

[35] SageMath, The Sage Mathematics Software System (Version 10.1). Sage Developers (2023). https://www.sagemath.org.

[36] M. Seck, Proof of concept implementation of the proposed encryption scheme. GitHub Repository. https://github.com/mseckept/pkeencodingsecknitaj.git.

[37] M. Seck, H. Boudjou, N. Diarra and A. Y. O. C. Khlil, On indifferentiable hashing into the Jacobian of hyperelliptic curves of genus 2. Lect. Notes Comput. Sci. (2017), 205–222.

[38] M. Seck and N. Diarra, Unified formulas for some deterministic almost-injective encodings into hyperelliptic curves. Lect. Notes Comput. Sci. (2018), 183–202.

[39] M. Seck and A. Nitaj, A new public key cryptosystem based on the cubic Pell curve. Cryptol. ePrint Arch. (2024).

[40] V. Shoup, OAEP reconsidered. J. Cryptol., 15 (2002), 223–249.

[41] SimulaMath, A software for learning, teaching and research in mathematics (Version 1.1). SimulaMath Developers (2023). https://simulamath.org.

[42] T. Takagi, Fast RSA-type cryptosystem modulo $p^k q$. Lect. Notes Comput. Sci., 1462 (1998), 318–326.

[43] G. Teseleanu and P. Cotan, Small private key attack against a family of RSA-like cryptosystems. Cryptol. ePrint Arch. (2023). https://eprint.iacr.org/2023/1356.

[44] B. de Weger, Cryptanalysis of RSA with small prime difference. Appl. Algebra Eng. Commun. Comput., 13(1) (2002), 17–28.

[45] M. Wiener, Cryptanalysis of short RSA secret exponents. IEEE Trans. Inf. Theory, 36 (1990), 553–558.