A New RSA Variant Based on Elliptic Curves

Maher Boudabra[1] and Abderrahmane Nitaj[2]

[1] Department of Computing and Mathematics, King Fahd University of Petroleum and Minerals, Saudi Arabia,
maher.boudabra@kfupm.edu.sa
[2] Normandie Univ, UNICAEN, CNRS, LMNO, 14000 Caen, France
abderrahmane.nitaj@unicaen.fr

Abstract. We propose a new scheme based on ephemeral elliptic curves over the ring $\mathbb{Z}/n\mathbb{Z}$ where $n = pq$ is an RSA modulus with $p = u_p^2 + v_p^2$, $q = u_q^2 + v_q^2$, $u_p \equiv u_q \equiv 3 \pmod 4$. The new scheme is a variant of both the RSA and the KMOV cryptosystems. The scheme can be used for both signature and encryption. We study the security of the new scheme and show that is immune against factorization attacks, discrete logarithm problem attacks, sum of two squares attacks, sum of four squares attacks, isomorphism attacks, and homomorphism attacks. Moreover, we show that the private exponents can be much smaller than the ordinary exponents for RSA and KMOV, which makes the decryption phase in the new scheme more efficient.

Keywords. Public key Cryptography, RSA, KMOV, Demytko's scheme, Elliptic curves, Continued fractions, Coppersmith's method.

Mathematics Subject Classification. 94A60, 68P25, 11A55. 14H52.

1 Introduction

The RSA system was proposed in 1977 by Rivest, Shamir, and Adleman [37] as a public key cryptosystem. The algorithm is based on a trap door function that utilizes Fermat-Euler theorem. The RSA algorithm strength depends on the difficulty of factorizing a large integer n which is the product of two large primes p and q. In RSA, the public exponent is an integer e and the private exponent is an integer d such that $ed \equiv 1 \pmod{(p-1)(q-1)}$.

Since its publication, the RSA cryptosystem has been intensively studied for vulnerabilities using various methods (see [4,16]). On the other hand, to improve the efficiency of RSA, many variants have been proposed such as Batch RSA [13], Multi-prime RSA [8], Prime-power RSA [41], CRT-RSA [10], Rebalanced-RSA [45], Dual RSA [40] and DRSA [34].

In 1985, Koblitz [21] and Miller [28] showed independently how to use elliptic curves over finite fields for the design of cryptosystems. Such schemes contribute to the elliptic curve cryptography (ECC) and their security is based on the hardness of the elliptic curve discrete logarithm (ECDLP). ECC offers high security with smaller keys and more efficient implementations than traditional public key cryptosystems such as RSA. ECC is increasingly used in industry for digital signatures such as ECDSA [30], key agreement such as ECDH [7] and Bitcoin [29].

In 1991, Koyama et al. [20] proposed a new scheme called KMOV, by adapting RSA to the elliptic curve with an equation $y^2 \equiv x^3 + b \pmod{n}$ over the ring $\mathbb{Z}/n\mathbb{Z}$, where $n = pq$ is an RSA modulus satisfying $p \equiv q \equiv 2 \pmod{3}$. In KMOV, b is computed during the encryption process in terms of the plaintext (x, y) as $b \equiv y^2 - x^3 \pmod{n}$. The main property in KMOV is that $(p+1)(q+1)P = \mathcal{O}$ for any point P of the elliptic curve where $\mathcal{O}$ is the point at infinity. In 1993, Demytko [11] proposed a variant of RSA where the elliptic curve with the equation $y^2 \equiv x^3 + ax + b \pmod{n}$ over $\mathbb{Z}/n\mathbb{Z}$ is fixed. The advantage of Demytko's scheme over KMOV is that it uses only the x-coordinate of the points of the elliptic curve. One of the common properties of both schemes is that their security is based on the hardness of factoring large composite integers.

In this paper, we propose a new RSA variant based on the elliptic curve with the equation $y^2 = x^3 + ax$ over the ring $\mathbb{Z}/n\mathbb{Z}$ where $n = pq$ is an RSA modulus with $p = u_p^2 + v_p^2$, $q = u_q^2 + v_q^2$, $u_p \equiv 3 \pmod{4}$ and $u_q \equiv 3 \pmod{4}$. The number of points of the elliptic curve $y^2 = x^3 + ax$ over the finite field $\mathbb{F}_p$ is $p + 1 - 2U_p$ with $U_p \in \{\pm u_p, \pm v_p\}$. Similarly, the number of points of the same elliptic curve over $\mathbb{F}_p$ is $q + 1 - 2V_p$ with $U_q \in \{\pm u_q, \pm v_q\}$.

The new scheme is a variant of both RSA and KMOV and works as follows. The public exponent is an integer e satisfying $\gcd(e, \psi(n)) = 1$ where

$$\psi(n) = (p + 1 - 2U_p)(q + 1 - 2U_q),$$

with $U_p \in \{\pm u_p, \pm v_p\}$, and $U_q \in \{\pm u_q, \pm v_q\}$. To encrypt a message m, one generates a random integer r with $1 \leq r < n$, computes $a = \frac{m^2 - r^3}{r} \pmod{n}$, and $C = (x_C, y_C) = e(r, m)$ on the elliptic curve with equation $y^2 = x^3 + ax$ over the ring $\mathbb{Z}/n\mathbb{Z}$. The point C is then the encrypted message. To decrypt C, one first computes $a \equiv \frac{y_C^2 - x_C^3}{x_C} \pmod{n}$ and the two values U_p and U_q such that

$$U_p = \begin{cases} -u_p & \text{if } a^{\frac{p-1}{4}} \equiv 1 \pmod{p}, \\ u_p & \text{if } a^{\frac{p-1}{4}} \equiv -1 \pmod{p}, \\ v_p & \text{if } a^{\frac{p-1}{4}} \equiv \dfrac{u_p}{v_p} \pmod{p}, \\ -v_p & \text{if } a^{\frac{p-1}{4}} \equiv -\dfrac{u_p}{v_p} \pmod{p}, \end{cases} \tag{1}$$

and

$$U_q = \begin{cases} -u_q & \text{if } a^{\frac{q-1}{4}} \equiv 1 \pmod{q}, \\ u_q & \text{if } a^{\frac{q-1}{4}} \equiv -1 \pmod{q}, \\ v_q & \text{if } a^{\frac{q-1}{4}} \equiv \dfrac{u_q}{v_q} \pmod{q}, \\ -v_q & \text{if } a^{\frac{q-1}{4}} \equiv -\dfrac{u_q}{v_q} \pmod{q}. \end{cases} \tag{2}$$

Using U_p and U_q, one computes $\psi(n) = (p+1-2U_p)(q+1-2U_q)$, and $d \equiv e^{-1} \pmod{\psi(n)}$. Finally, one computes the initial message $(r, m) = d(x_C, y_C)$ on the elliptic curve with equation $y^2 = x^3 + ax$ over the ring $\mathbb{Z}/n\mathbb{Z}$.

We study the security of the new scheme regarding the modulus n, the private multiplier d and the elliptic curve with an equation $y^2 \equiv x^3 + ax \pmod{n}$. For the modulus $n = pq$, we study its resistance against factorization algorithms, and its decomposition as the sum of two or four squares. We show that knowing the order $\psi(n) = (p+1-2U_p)(q+1-2U_q)$ with $U_p \in \{\pm u_p, \pm v_p\}$, and $U_q \in \{\pm u_q, \pm v_q\}$ is not sufficient to factor n. For the private multiplier d, we show that the attacks based on the continued fraction algorithm or Coppersmith's method are applicable only if $d < n^{0.133}$. For comparison, the former techniques are applicable for RSA and KMOV when their private exponent and multiplier d' is such that $d' < n^{0.292}$. Finally, we study the discrete logarithm problem for an elliptic curve with the equation $y^2 \equiv x^3 + ax \pmod{n}$. We also study the isomorphism and the homomorphism attacks and the way to overcome them.

The rest of the paper is organized as follows. In Section 2, we present three results that will be used in the paper. In Section 3 and Section 4, we present the theory of elliptic curves over a finite field $\mathbb{F}_p$ and a finite ring $\mathbb{Z}/n\mathbb{Z}$ respectively. In Section 5, we present the new scheme. In Section 6, we present a detailed analysis of the security of the new scheme. We conclude the paper in Section 7.

2 Useful Lemmas

In this section, we present some results that will be convenient for the security analysis of our new scheme.

Let $n = pq$ be an RSA modulus with balanced prime factors p and q, typically, $q < p < 2q$. The following result gives upper and lower bounds for p and q in terms of n [31].

Lemma 1. *Let $n = pq$ be the product of two unknown integers such that $q < p < 2q$. Then*

$$\frac{\sqrt{2}}{2}\sqrt{n} < q < \sqrt{n} < p < \sqrt{2}\sqrt{n}.$$

In 1990, Wiener [45] showed that RSA with a public key $(n = pq, e)$ is insecure if the private exponents d satisfies $ed - k(p-1)(q-1) = 1$ with $d < \frac{1}{3}n^{\frac{1}{4}}$. His method is based on the continued fraction algorithm and makes use of the following result (Theorem 184 of [15]).

Theorem 1. *Let ξ be a real number. Let a and b be two positive integers satisfying* $\gcd(a, b) = 1$ *and*

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

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

In 1996, Coppersmith [9] described a polynomial-time algorithm for finding small solutions of univariate modular polynomial equations. The method is based on lattice reduction. Since then, Coppersmith method has been extended to solve modular polynomial equations with more variables, and has been used for cryptanalysis, especially in regards with the RSA system. To illustrate this point, Boneh and Durfee [6] presented an attack on RSA by transforming the RSA key equation $ed - k(p-1)(q-1) = 1$ into the small inverse problem $x(n+y) \equiv 1 \pmod{e}$. Using Coppersmith's method, they improved Wiener's attack up to $d < N^{0.292}$.

The following result is a generalization of the method of Boneh and Durfee for solving the small inverse problem (see [6,44,42]).

Lemma 2. *Let n and e be two distinct integers of the same size. Let x and y be two integers such that $|x| < n^{\delta}$, $|y| < n^{\beta}$, and $x(n+y) \equiv 1 \pmod{e}$. If $\frac{1}{4} < \beta < 1$ and $\delta < 1 - \sqrt{\beta}$, then one can find x and y in polynomial time.*

3 Elliptic Curves over the Finite Field $\mathbb{F}_p$

In this section, we present the main definitions and properties of elliptic curves. For more properties, see [39,43,38,17].

Let p be a prime number and $\mathbb{F}_p$ be the finite field with p elements. An elliptic curve E over $\mathbb{F}_p$ is an algebraic curve with no singular points, given by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_i \in \mathbb{F}_p$ for $i \in \{1,2,3,4,6\}$. When $p \geq 5$, the equation can be transformed into the short Weierstrass equation $y^2 = x^3 + ax + b$, with nonzero discriminant $\Delta = -16\left(4a^3 + 27b^2\right) \neq 0$. The set of points $P = (x, y)$ satisfying the equation, along with the infinity point $\mathcal{O}$ is denoted $E(\mathbb{F}_p)$. The total number of points on $E(\mathbb{F}_p)$ is called the order of E and is denoted $\#E(\mathbb{F}_p)$. It is well known that $\#E(\mathbb{F}_p)$ can be written as $\#E(\mathbb{F}_p) = p+1-t$ where t is bounded by the following result of Hasse $0 \leq |t| \leq 2\sqrt{p}$. An addition law is defined over $E(\mathbb{F}_p)$ using the chord-tangent method.

The following result is fundamental to find the exact value of $\#E(\mathbb{F}_p)$ for specific elliptic curves (see Theorem 5, page 307, Section 4, Chapter 18 of [18]).

Theorem 2. *Let $p = u_p^2 + v_p^2$ be a prime number with $p \equiv 1 \pmod{4}$. Let $a \in \mathbb{F}_p$ with $a \neq 0$. Consider the elliptic curve E_p with equation $y^2 = x^3 + ax$ over $\mathbb{F}_p$. Then*

$$\#E(\mathbb{F}_p) = p + 1 - \overline{\left(\frac{-a}{\pi}\right)_4}\pi - \left(\frac{-a}{\pi}\right)_4 \overline{\pi},$$

where $\pi = u_p + iv_p \equiv 1 \pmod{(2+2i)}$, $i^2 = -1$, and $\left(\frac{\alpha}{\pi}\right)_4 = \alpha^{\frac{p-1}{4}} \pmod{\pi}$ is the biquadratic (or quartic) residue character of α modulo π.

The following result gives an explicit solution for $\left(\frac{a}{\pi}\right)_4 \pmod{\pi}$ (See page 122, Proposition 9.8.2 of [18]).

Theorem 3. *Let $p = u_p^2 + v_p^2$ be a prime number with $p \equiv 1 \pmod 4$. Let $a \in \mathbb{F}_p$ with $a \neq 0$. Then*

$$a^{\frac{p-1}{4}} \equiv \pm 1, \pm i \pmod \pi,$$

where $\pi = u_p + iv_p$, $i^2 = -1$.

The following result is valid when the residue quartic character is computed modulo p.

Lemma 3. *Let $p = u_p^2 + v_p^2$ be a prime number with $p \equiv 1 \pmod 4$. Let $a \in \mathbb{F}_p$ with $a \neq 0$. Then*

$$a^{\frac{p-1}{4}} \equiv \pm 1, \pm u_p v_p^{-1} \pmod p.$$

Proof. Let $p = u_p^2 + v_p^2$ be a prime number. First, we have $u_p^2 + v_p^2 \equiv 0 \pmod p$ and $\left(u_p v_p^{-1}\right)^2 \equiv -1 \pmod p$. Next, let $a \in \mathbb{F}_p$ with $a \neq 0$. By Fermat's Little Theorem, we have $a^{p-1} \equiv 1 \pmod p$. Then $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ or $a^{\frac{p-1}{2}} \equiv -1 \pmod p$. If $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, then $a^{\frac{p-1}{4}} \equiv \pm 1 \pmod p$, and if $a^{\frac{p-1}{2}} \equiv -1 \pmod p$, then

$$a^{\frac{p-1}{2}} \equiv \left(u_p v_p^{-1}\right)^2 \pmod p,$$

and $a^{\frac{p-1}{4}} \equiv \pm u_p v_p^{-1} \pmod p$. Summarizing, we have $a^{\frac{p-1}{4}} \in \{\pm 1, \pm u_p v_p^{-1}\}$ modulo p. This terminates the proof. □

In the following result, we give a simple proof for the estimation of $\#E(\mathbb{F}_p)$ when $p \equiv 1 \pmod 4$. Alternative proofs can be found in [43] (Section 4.4 p. 115) and [18] (Section 4 in Chapter 18).

Lemma 4. *Let $p = u_p^2 + v_p^2$ be a prime number with $u_p = 4u + 3$ and $v_p = 4v + 2$. For $a \in \mathbb{F}_p$ with $a \neq 0$, let $E_a(p)$ be the elliptic curve with the equation $y^2 = x^3 + ax$ over $\mathbb{F}_p$. Then*

$$\#E(\mathbb{F}_p) = \begin{cases} p + 1 + 2u_p & \text{if } a^{\frac{p-1}{4}} \equiv 1 \pmod p, \\ p + 1 - 2u_p & \text{if } a^{\frac{p-1}{4}} \equiv -1 \pmod p, \\ p + 1 - 2v_p & \text{if } a^{\frac{p-1}{4}} \equiv \dfrac{u_p}{v_p} \pmod p, \\ p + 1 + 2v_p & \text{if } a^{\frac{p-1}{4}} \equiv -\dfrac{u_p}{v_p} \pmod p, \end{cases}$$

Proof. Let $p = u_p^2 + v_p^2$ with $u_p = 4u + 3$ and $v_p = 4v + 2$. We set $p = \pi\overline{\pi}$ with $\pi = u_p + iv_p$. Then

$$\frac{p-1}{4} = 4u^2 + 4v^2 + 6u + 4v + 3,$$

and

$$\left(\frac{-1}{\pi}\right)_4 = (-1)^{\frac{p-1}{4}} = (-1)^3 = -1.$$

Also, we have

$$u_p + iv_p = 1 + (2+2i)(1+u-v+i(v-u)) \equiv 1 \pmod{2+2i}.$$

We apply Theorem 2 to the elliptic curve with equation $y^2 = x^3 + ax$ over $\mathbb{F}_p$. We get

$$\begin{aligned}\#E(\mathbb{F}_p) &= p+1-\overline{\left(\frac{-a}{\pi}\right)_4}\pi - \left(\frac{-a}{\pi}\right)_4\overline{\pi}\\ &= p+1-\overline{\left(\frac{-1}{\pi}\right)_4}\,\overline{\left(\frac{a}{\pi}\right)_4}\pi - \overline{\left(\frac{-1}{\pi}\right)_4}\left(\frac{a}{\pi}\right)_4\overline{\pi}\\ &= p+1+\overline{\left(\frac{a}{\pi}\right)_4}\pi + \left(\frac{a}{\pi}\right)_4\overline{\pi}.\end{aligned}$$

Theorem 3 asserts that $a^{\frac{p-1}{4}} \equiv \pm 1, \pm u_p v_p^{-1} \pmod p$. First, assume that $a^{\frac{p-1}{4}} \equiv 1 \pmod p$. Then $a^{\frac{p-1}{4}} \equiv 1 \pmod \pi$ and

$$\#E(\mathbb{F}_p) = p+1+(u_p+iv_p)+(u_p-iv_p) = p+1+2u_p.$$

Next, assume that $a^{\frac{p-1}{4}} \equiv -1 \pmod p$. Then $a^{\frac{p-1}{4}} \equiv -1 \pmod \pi$ and

$$\#E(\mathbb{F}_p) = p+1-(u_p+iv_p)-(u_p-iv_p) = p+1-2u_p.$$

Now, assume that $a^{\frac{p-1}{4}} \equiv -\frac{u_p}{v_p} \pmod p$. Since $u_p + iv_p \equiv 0 \pmod \pi$, then $-u_pv_p^{-1} - i \equiv 0 \pmod \pi$ and $-u_pv_p^{-1} \equiv i \pmod \pi$. Hence $a^{\frac{p-1}{4}} \equiv i \pmod \pi$ and

$$\#E(\mathbb{F}_p) = p+1-i(u_p+iv_p)+i(u_p-iv_p) = p+1+2v_p.$$

Finally, assume that $a^{\frac{p-1}{4}} \equiv \frac{u_p}{v_p} \pmod p$. Then $u_pv_p^{-1} \equiv -i \pmod \pi$ and $a^{\frac{p-1}{4}} \equiv -i \pmod \pi$ which gives

$$\#E(\mathbb{F}_p) = p+1+i(u_p+iv_p)-i(u_p-iv_p) = p+1-2v_p.$$

This terminates the proof. □

4 Elliptic Curves over the Ring $\mathbb{Z}/n\mathbb{Z}$

In this section, we briefly describe the theory of elliptic curves over the ring $\mathbb{Z}/n\mathbb{Z}$ where $n = pq$ is an RSA modulus (see [43], Section 2.11 and [25] for more details).

Let $a, b \in \mathbb{Z}/n\mathbb{Z}$ with $\gcd(4a^3+27b^2, n) = 1$. The elliptic curve $E_n(a,b)$ is the set of points $P = (x,y)$ satisfying the equation $y^2 = x^3+ax+b \pmod n$, together with the point at infinity, denoted $\mathcal{O}_n$. By the Chinese remainder Theorem, the set $E_n(a,b)$ is isomorphic to the direct sum $E_p(a,b) \oplus E_q(a,b)$ where $E_p(a,b)$ is the elliptic curve with equation $y^2 = x^3+ax+b \pmod p$ over $\mathbb{F}_p$ with the point at infinity $\mathcal{O}_p$, and $E_q(a,b)$ is the elliptic curve with equation $y^2 = x^3 + ax + b \pmod{q}$ over $\mathbb{F}_q$ with the point at infinity $\mathcal{O}_q$. Hence, the point at infinity of $E_n(a,b)$ is $\mathcal{O}_n = (\mathcal{O}_p, \mathcal{O}_q)$. The points of the form $(\mathcal{O}_p, P_q)$ with $P_q \neq \mathcal{O}_q$ and of the form $(P_p, \mathcal{O}_q)$ with $P_p \neq \mathcal{O}_p$ are semi-zero points while ordinary points are of the form $P = (P_p, P_q)$ with $P_p \neq \mathcal{O}_p$ and $P_q \neq \mathcal{O}_q$. A group law can be given for $E_n(a,b)$ by the chord and tangent addition law. However, the addition law is not always well-defined when using analytical expressions since there are elements in $\mathbb{Z}/n\mathbb{Z}$ that are not invertible modulo n. To overcome this, the projective coordinates $(x : y : z) \in \mathbb{P}^2(\mathbb{Z}_n)$ are used with the equation $y^2z = x^3 + axz^2 + bz^3 \pmod{n}$. Hence, for any point P of the elliptic curve $E_n(a,b)$, we have

$$\operatorname{lcm}(\#E_p(a,b), \#E_q(a,b) \cdot P = \mathcal{O}_n.$$

In this paper, the arithmetic of the new scheme is based on the elliptic curve $E_n(a,b)$ with $a \in \mathbb{Z}/n\mathbb{Z}$ and $b = 0$ where $n = pq$ with large prime numbers. Consequently, the sum of two points of $E_n(a,0)$ is defined with overwhelming probability.

The following result gives an explicit value for the order $\#E_n(a,0)$.

Theorem 4. *Let $n = pq$ be an RSA modulus with $p = u_p^2 + v_p^2$, $q = u_q^2 + v_q^2$, $u_p \equiv u_q \equiv 3 \pmod 4$ and $v_p \equiv v_q \equiv 2 \pmod 4$. For $a \in \mathbb{Z}/n\mathbb{Z}$ with $\gcd(a,n) = 1$, let $E_n(a)$ be the elliptic curve with the equation $y^2 = x^3 + ax$ over $\mathbb{Z}/n\mathbb{Z}$. Then for any point P on $E_n(a)$, we have*

$$(p + 1 - 2U_p)(q + 1 - 2U_q) \cdot P = \mathcal{O}_n,$$

where U_p satisfies (1) and U_q satisfies (2).

5 The New Scheme

In this section, we present the new scheme and give a small numerical example.

5.1 The new encryption scheme

Key generation.

1. Choose a size $l \geq 4096$ for the modulus to guarantee at least 128 security level.
2. Choose two large integers u_1 and v_1 of size $l/4$.
3. Compute $u_p = 4u_1 + 3$ and $v_p = 4v_1 + 2$.
4. Compute $p = u_p^2 + v_p^2$.
5. If p is not prime, return to Step 2.
6. Choose two large integers u_2 and v_2 of size $l/4$.
7. Compute $u_q = 4u_2 + 3$ and $v_q = 4v_2 + 2$.
8. Compute $q = u_q^2 + v_q^2$.
9. If q is not prime, return to Step 6.
10. Compute $n = pq$.

11. Choose an integer e such that
$$\gcd\left(e, \left((p+1)^2 - 4u_p^2\right)\left((q+1)^2 - 4u_q^2\right)\right) = 1.$$
The pair (n, e) represents the public key, and (u_p, v_p, u_q, v_q) represents the private key.

Encryption.

1. Generate a random integer $r \in \mathbb{Z}/n\mathbb{Z}$.
2. Use the message y_M as $M = (r, y_M) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
3. Compute $a \equiv \left(y_M^2 - r^3\right) r^{-1} \pmod{n}$. The elliptic curve $E_n(a)$ is defined by the equation $y^2 \equiv x^3 + ax \pmod{n}$.
4. Compute $(x_C, y_C) = e(r, y_M)$ on $E_a(n)$. The point (x_C, y_C) is the encrypted message.

Decryption.

1. Compute $a \equiv \left(y_C^2 - x_C^3\right) x_C^{-1} \pmod{n}$. The elliptic curve $E_a(n)$ is defined by the equation $y^2 \equiv x^3 + ax \pmod{n}$.
2. Compute U_p by one of the formulae (1), and U_q by one of the formulae (2).
3. Compute $\phi(a, n) = (p + 1 - 2U_p)(q + 1 - 2U_q)$.
4. Compute $d \equiv e^{-1} \pmod{\phi(a, n)}$.
5. Compute $M = (r, y_M) = d(x_C, y_C)$ on $E_n(a)$. The point (r, y_M) is the original message.

The role of the random integer r is to serve as the x-coordinate of M on the elliptic curve with the equation $y^2 \equiv x^3 + ax \pmod{n}$. If the same message y_M is encrypted twice, this yields two different couples (r, y_M) and (r', y_m), two values $a \equiv \left(y_M^2 - r^3\right) r^{-1} \pmod{n}$ and $a' \equiv \left(y_M^2 - r'^3\right) r'^{-1} \pmod{n}$, and then two elliptic curves with different equations.

5.2 Numerical Example

The following is a numerical example with small integers demonstrating the system parameters and a pair of plaintext-ciphertext.

$$\begin{aligned}
u_1 &= 3253473156,\ v_1 = 3239617290,\\
u_p &= 4u_1 + 3 = 13013892627,\ v_p = 4v_1 + 2 = 12958469162,\\
p &= u_p^2 + v_p^2 = 337283324329589943373,\\
u_2 &= 4133795239,\ v_2 = 4069844016,\\
u_q &= 4u_2 + 3 = 16535180959,\ v_q = 4v_2 + 2 = 16279376066,\\
q &= u_q^2 + v_q^2 = 538430294445129796037,\\
n &= pq = 181603559630213323475279432919469869812801,\\
e &= 233,\\
r &= 276576193905959805653341,\\
y_M &= 241239880224506901 40866.
\end{aligned}$$

Then, one can compute the following parameters

$$\begin{aligned}
a &\equiv \frac{y_M^2 - r^3}{r} \pmod{n}\\
&= 1248927994801867173324603353052208867525 46,\\
C &= e(r, y_M) = (x_C, y_C),\\
x_C &= 98959326615549161080796135242665606864 78,\\
y_C &= 17483855199302316211746216569508297328 0827,\\
a^{\frac{p-1}{4}} &\equiv 1 \pmod{p}, \text{ hence } U_p = -u_p,\\
a^{\frac{q-1}{4}} &\equiv -1 \pmod{q}, \text{ hence } U_q = u_q,\\
\phi(a, n) &= (p + 1 - 2U_p)(q + 1 - 2U_q)\\
&= 181603559633073389948874511533493403987360,\\
d &\equiv e^{-1} \pmod{\phi(a, n)} = 350736488561729723077225451459536617 14297,\\
m &= d(x_C, y_C) = (r, y_M),
\end{aligned}$$

which shows that the decryption is correct.

5.3 The new signature scheme

The encryption scheme can be transformed easily into a signature scheme using a hash function Hash as follows.

- **Key generation.** The key generation scheme is similar to that of the encryption scheme 5.1.
- **Encryption.**
  1. Generate a random integer $r \in \mathbb{Z}/n\mathbb{Z}$.
  2. Represent the message as $M = (r, y_M) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
  3. Compute $a \equiv \left(y_M^2 - r^3\right) r^{-1} \pmod{n}$. The elliptic curve $E_n(a)$ is defined by the equation $y^2 \equiv x^3 + ax \pmod{n}$.
  4. Compute $(x_C, y_C) = e(r, y_M)$ on $E_a(n)$. The point (x_C, y_C) is the encrypted message.
  5. Compute the signature $s = \text{Hash}(r \| y_M)$.
- **Decryption.**
  1. Compute $a \equiv \left(y_C^2 - x_C^3\right) x_C^{-1} \pmod{n}$. The elliptic curve $E_a(n)$ is defined by the equation $y^2 \equiv x^3 + ax \pmod{n}$.
  2. Compute U_p by one of the formulae (1), and U_q by one of the formulae (2).
  3. Compute $\phi(a, n) = (p + 1 - 2U_p)(q + 1 - 2U_q)$.
  4. Compute $d \equiv e^{-1} \pmod{\phi(a, n)}$.
  5. Compute $M = (r, y_M) = d(x_C, y_C)$ on $E_n(a)$.
  6. Compute $s' = \text{Hash}(r \| y_M)$
  7. Accept the message if $s' = s$.

As in the encryption scheme, the random number r serves as the x-coordinate of the point $M = (r, y_M)$ on the elliptic curve with the equation $y^2 \equiv x^3 + ax \pmod{n}$. Note that r is random, which implies that the signature scheme is probabilistic.

6 Security Analysis

6.1 Resistance against factorization methods

When p and q are sufficiently large, factoring the RSA modulus $n = pq$ is believed to be hard for all current known factorization algorithms (see [5,3]). Indeed, Pollard's rho method is not affective since its run time is $\mathcal{O}\left(\sqrt{p}(\log(n))^2\right)$ and depends on the size of the prime number p found. This is similar for Lenstra's Elliptic Curve Method (ECM) for which the run time is $\mathcal{O}\left(\exp\left(\sqrt{2}\sqrt{\ln p \ln\ln p}\right)\right)$. The Number Field Sieve [26] is also ineffective for large primes p and q. Its run time is $\mathcal{O}\left(\exp\left(c\sqrt[3]{\ln n}\sqrt[3]{(\ln\ln n)^2}\right)\right)$ where c is a constant.

6.2 Resistance against decomposition as sum of two squares

It is well known that if $n = pq$ with $p \equiv q \equiv 1 \pmod 4$, then n can be expressed as the sum of two squares as $n = x^2 + y^2$. In the new scheme, the modulus is in the form $n = pq = \left(u_p^2 + v_p^2\right)\left(u_q^2 + v_q^2\right)$. Then, the Brahmagupta-Fibonacci identity expresses n as a sum of two squares in two different ways, namely

$$n = (u_p u_q - v_p v_q)^2 + (u_p v_q + v_p u_q)^2 = (u_p u_q + v_p v_q)^2 + (u_p v_q - v_p u_q)^2.$$

Euler observed that if $n = x_1^2 + y_1^2 = x_2^2 + y_2^2$ with $x_1 \equiv x_2 \equiv 0 \pmod 2$ and $x_1 \not\equiv \pm x_2 \pmod n$, then

$$n = \left(\frac{r^2}{4} + \frac{u^2}{4}\right)\left(s^2 + t^2\right),$$

where

$$r = \gcd(x_1 - x_2, y_2 - y_1),\ u = \gcd(x_1 + x_2, y_2 + y_1),\ s = \frac{x_1 - x_2}{r},\ t = \frac{y_2 - y_1}{r}.$$

On the other hand, we have $\left(x_1 y_1^{-1}\right)^2 \equiv \left(x_2 y_2^{-1}\right)^2 \equiv -1 \pmod n$. It follows that decomposing n as the sum of two squares in two different ways will give a solution to the equation $t_1^2 \equiv t_2^2 \pmod n$ with $t_1 \not\equiv \pm t_2 \pmod n$, and two solutions of the congruence $t^2 = -1 \pmod n$. This is known to be equivalent to factoring n as in the quadratic sieve factoring algorithm [35] and in Rabin's cryptosystem [36].

It is also known that by applying the continued fraction algorithm to $\sqrt{n}$, it is possible to find one representation of n (see [12]) as $n = x^2 + y^2$. This leads to one of the systems

$$\begin{cases} u_p u_q - v_p v_q &= x, \\ u_p v_q + v_p u_q &= y, \end{cases} \quad \begin{cases} u_p u_q + v_p v_q &= x, \\ u_p v_q - v_p u_q &= y. \end{cases}$$

This is not sufficient the solve anyone of the two systems. Consequently, the representation of n as a sum of two squares by the continued fraction method is not sufficient to factor it.

6.3 Resistance against decomposition as sum of four squares

Lagrange's four-square theorem states that every positive integer n is the sum of four squares (Theorem 369 in [15]), that is $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$. The number of decomposing n as a such a sum is denoted $r_4(n)$, and for odd n, Jacobi's four-square theorem formula gives (Proposition 17.7.2 of [15]) $r_4(n) = 8\sum_{m|n} m$. For the modulus $n = pq = \left(u_p^2 + v_p^2\right)\left(u_q^2 + v_q^2\right)$, a specific decomposition as sum of four squares is

$$n = (u_p u_q)^2 + (u_p v_q)^2 + (v_p u_q)^2 + (v_p v_q)^2.$$

Conversely, let $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ be a decomposition of n leading to the factorization $n = pq = \left(u_p^2 + v_p^2\right)\left(u_q^2 + v_q^2\right)$. Then

$$u_p u_q = |x_1|, \quad u_p v_q = |x_2|, \quad v_p u_q = |x_3|, \quad v_p v_q = |x_4|,$$

from which we get

$$\gcd(|x_1|, |x_2|) = \gcd(u_p u_q, u_p v_q) = u_p \gcd(u_q, v_q) = u_p.$$

Similarly, we have

$$v_p = \gcd(|x_3|, |x_4|), \quad u_q = \gcd(|x_1|, |x_3|), \quad v_q = \gcd(|x_2|, |x_4|).$$

As the decomposition of $p = u_p^2 + v_p^2$ with positive integers u_p and v_p satisfying $u_p \equiv 3 \pmod 4$ is unique, then p can be decomposed as $p = r^2 + s^2$ with integers r and s in eight ways, namely

$$p = (\pm u_p)^2 + (\pm v_p)^2 = (\pm v_p)^2 + (\pm u_p)^2.$$

This is also true for q. Consequently, among the representations of n as a sum of four squares $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$, only 64 decompositions can lead to the factorisation of n by using

$$u_p u_q = |x_1|, \quad u_p v_q = |x_2|, \quad v_p u_q = |x_3|, \quad v_p v_q = |x_4|.$$

This is negligible compared to $r_4(n) = 8(1 + p + q + n)$, the number of decompositions of a large modulus $n = pq$ as the sum of four squares.

6.4 Resistance against solving the order

In RSA, it is well known that solving Euler's totient function $\phi(n) = (p-1)(q-1)$ is equivalent to factoring $n = pq$. This is also true for solving the order $N_n = (p+1)(q+1)$ in the KMOV system. For an elliptic curve E over a finite ring $\mathbb{Z}/n\mathbb{Z}$ with an RSA modulus n, Martin et al. [27] proved that computing the order $\#E$ is as difficult as factoring n. Moreover, for our scheme, we have the following facts.

Let $a \in \mathbb{Z}/n\mathbb{Z}$ be fixed. In our scheme, the order of the elliptic curves $E_n(a)$ is of the form

$$\#E_n(a) = (p+1-2U_p)(q+1-2U_q),$$

with $U_p \in \{\pm u_p, \pm v_p\}$ and $U_q \in \{\pm u_q, \pm v_q\}$. Assume that the factorization of n is known. Then one can compute $\#E_p(a) = p+1-2U_p$ and $\#E_q(a) = q+1-2U_q$ by a specific algorithm to determine the order of an elliptic curve over a finite field such as the Schoof-Elkies-Atkin algorithm [1]. This implies that $\#E_n(a) = (p+1-2U_p)(q+1-2U_q)$ can be computed. Conversely, assume that $\#E_n(a) = (p+1-2U_p)(q+1-2U_q)$ is known where $U_p \in \{\pm u_p, \pm v_p\}$ and $U_q \in \{\pm u_q, \pm v_q\}$. Let $V_p \in \{v_p, u_p\}$ and $V_q \in \{v_q, u_q\}$ such that

$$V_p^2 = p - U_p^2, \quad V_q^2 = q - U_q^2.$$

Assume that u_p and v_p are of the same size so that $u_p < 2v_p$ and $v_p < 2u_p$. Then, if $U_p = \pm u_p$, we get $V_p = v_p$, and

$$p = U_p^2 + V_p^2 = u_p^2 + v_p^2 < 5v_p^2 = 5V_p^2.$$

Also, if if $U_p = \pm v_p$, we get $V_p = u_p$, and

$$p = U_p^2 + V_p^2 = v_p^2 + u_p^2 < 5v_p^2 = 5U_p^2.$$

Hence, using Lemma 1, we get

$$\min\left(U_p^2, V_p^2\right) > \frac{p}{5} > \frac{\sqrt{n}}{5}.$$

Similarly, assuming that u_q and v_q are of the same size with $u_q < 2v_q$ and $v_q < 2u_p$, we get

$$\min\left(U_q^2, V_q^2\right) > \frac{q}{5} > \frac{\sqrt{2}\sqrt{n}}{10}.$$

As a consequence, we have

$$p+1-2U_p = (U_p-1)^2 + V_p^2 > V_p^2 > \frac{\sqrt{n}}{5},$$

and

$$q+1-2U_q = (U_q-1)^2 + V_q^2 > V_q^2 > \frac{\sqrt{2}\sqrt{n}}{10}.$$

Combining the former inequalities, we get

$$(p+1-2U_p)(q+1-2U_q) > \frac{\sqrt{n}}{5} \cdot \frac{\sqrt{2}\sqrt{n}}{10} = \frac{\sqrt{2}}{50}n. \tag{3}$$

This implies that the order $\#E_n(a) = (p+1-2U_p)(q+1-2U_q)$ is sufficiently large and there is no efficient method to factor it. Hence, finding p and q is not feasible in general.

It is important to notice that the work of Kunihiro and Koyama [22] on the equivalence between factoring n and counting the number of points on elliptic curves over $\mathbb{Z}/n\mathbb{Z}$ does not apply when the order $\#E_n(a) = (p+1-2U_p)(q+1-2U_q)$ is known for a fixed a. The reason is that in [22] an oracle is needed that count the number of points on every elliptic curve over $\mathbb{Z}/n\mathbb{Z}$, while, in our situation, just $\#E_n(a) = (p+1-2U_p)(q+1-2U_q)$ is known.

6.5 Resistance against small private exponent attacks

The main small private exponent attacks on RSA are based on the key equation $ed' - k'(p-1)(q-1) = 1$. Wiener's attack is based on the continued fraction algorithm which exploits the approximation $(p-1)(q-1) = n+1-p-q \approx n$. It leads to the factorization of n under the condition $d' < \frac{1}{3}n^{\frac{1}{4}}$. The attack of Boneh and Durfee is based on Coppersmith's method and exploits the existence of a small solution (x, k') to the modular equation $k'(n+1-x) \equiv 1 \pmod{e}$. It works for $d' < n^{0.292}$.

In the following, we show that the private exponent d in our scheme can be small enough without undermining its security. Typically, it should be larger than $n^{0.133}$ while it should be larger than $n^{0.292}$ for RSA.

Lemma 5. *Let $n = pq$ be an RSA modulus with $p = u_p^2 + v_p^2$, $q = u_q^2 + v_q^2$, $u_p \equiv u_q \equiv 3 \pmod{4}$, $u_p \approx v_p$, and $u_q \approx v_q$. If d satisfies the key equation $ed - k(p+1-2U_p)(q+1-2U_q) = 1$ where $U_p \in \{\pm u_p, \pm v_p\}$ and $U_q \in \{\pm u_q, \pm v_q\}$, then*

$$|ed - kn| < 7k(2n)^{\frac{3}{4}}.$$

Proof. Rewrite the key equation in the form

$$ed - k(p+1-2U_p)(q+1-2U_q) = 1,$$

with $U_p \in \{\pm u_p, \pm v_p\}$, $U_q \in \{\pm u_q, \pm v_q\}$. We have

$$(p+1-2U_p)(q+1-2U_q) = n + p(1-2U_q) + q(1-2U_p) + (1-2U_p)(1-2U_q).$$

Then

$$\begin{aligned}
|ed - kn| &= |k(p+1-2U_p)(p+1-2U_q) + 1 - kn| \\
&= |k((p+1-2U_p)(p+1-2U_q) - n) + 1| \\
&= |k(p(1-2U_q) + q(1-2U_p) + (1-2U_p)(1-2U_q)) + 1| \\
&\le kp|1-2U_q| + kq|1-2U_p| + k|1-2U_p||1-2U_q| + 1.
\end{aligned}$$

Suppose that u_p and v_p are of the same bit-size so that $u_p < 2v_p$ and $v_p < 2u_p$. Then

$$\max(u_p, v_p)^2 < 2u_pv_p < u_p^2 + v_p^2 = p.$$

Hence

$$\max(u_p, v_p) < \sqrt{p},$$

from which we deduce

$$|1-2U_p| \leq 2|U_p| + 1 < 2\sqrt{p} + 1 < 3\sqrt{p}. \tag{4}$$

Similarly, we get

$$|1-2U_q| < 3\sqrt{q}. \tag{5}$$

This leads to

$$\begin{aligned}
|ed-kn| &\leq kp|1-2U_q| + kq|1-2U_p| + k|1-2U_p||1-2U_q| + 1 \\
&< 3kp\sqrt{q} + 3kq\sqrt{p} + 9k\sqrt{p}\sqrt{q} + 1 \\
&< 3kp\sqrt{p} + 3kp\sqrt{p} + 9k\sqrt{p}\sqrt{q} + 1 \\
&< 6kp\sqrt{p} + 10k\sqrt{p}\sqrt{q} \\
&< 7kp\sqrt{p},
\end{aligned}$$

where we used $10k\sqrt{p}\sqrt{q} + 1 < kp\sqrt{p}$ which is valid since $10\sqrt{q} < p$. Using Lemma 1, we get

$$|ed-kn| < 7kp\sqrt{p} < 7k(2n)^{\frac{3}{4}}.$$

This terminates the proof. □

The following result shows that, in regard to Wiener's attack, the private exponent d can be very small in our scheme comparing to the private exponent in RSA.

Theorem 5. *Let $n = pq$ be an RSA modulus with $p = u_p^2 + v_p^2$, $q = u_q^2 + v_q^2$ and $u_p \equiv u_q \equiv 3 \pmod 4$. Let e be a public exponent such that $e < (p+1-2U_p)(q+1-2U_q)$ with $U_p \in \{\pm u_p, \pm v_p\}$, and $U_q \in \{\pm u_q, \pm v_q\}$. If d satisfies the equation $ed - k(p+1-2U_p)(q+1-2U_q) = 1$ with $d < \frac{\sqrt{2}}{4} n^{\frac{1}{8}}$, then one can find d and k in polynomial time.*

Proof. The key equation is in the form

$$ed - k(p+1-2U_p)(q+1-2U_q) = 1,$$

with $U_p \in \{\pm u_p, \pm v_p\}$, and $U_q \in \{\pm u_q, \pm v_q\}$. Then, Lemma 5 gives

$$|ed-kn| < 7k(2n)^{\frac{3}{4}}.$$

Dividing by nd, we get

$$\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{7k(2n)^{\frac{3}{4}}}{nd}. \tag{6}$$

Using the key equation $ed - k(p+1-2U_p)(q+1-2U_q) = 1$, we get

$$k(p+1-2U_p)(q+1-2U_q) = ed - 1 < ed.$$

Then

$$\frac{k}{d} < \frac{e}{(p+1-2U_p)(q+1-2U_q)}.$$

Assuming $e < (p+1-2U_p)(q+1-2U_q)$, this implies that $k < d$. Then (6) implies

$$\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{7(2n)^{\frac{3}{4}}}{n}.$$

The solutions in d of the inequality $\frac{7(2n)^{\frac{3}{4}}}{n} < \frac{1}{2d^2}$ satisfy

$$d < \frac{1}{\sqrt{14 \cdot 2^{\frac{3}{4}}}} n^{\frac{1}{8}}.$$

For such solutions, we have

$$\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

This implies that $\frac{k}{d}$ can be found amongst the convergents of the continued expansion of $\frac{e}{n}$. Since the continued fraction algorithm computes the convergents of $\frac{e}{n}$ with complexity $\mathcal{O}(\log(n))$, then one finds k and d in polynomial time. □

The following result makes use of lattice reduction techniques.

Theorem 6. *Let $n = pq$ be an RSA modulus with $p = u_p^2 + v_p^2$, $q = u_q^2 + v_q^2$ and $u_p \equiv u_q \equiv 3 \pmod 4$. Let e be a public exponent such that $e < (p+1-2U_p)(q+1-2U_q)$ with $U_p \in \{\pm u_p, \pm v_p\}$, and $U_q \in \{\pm u_q, \pm v_q\}$. If d satisfies the equation $ed - k(p+1-2U_p)(q+1-2U_q) = 1$ with $d < n^{0.133}$, then one can find d and k in polynomial time.*

Proof. Since d satisfies an equation of the form $ed-k(p+1-2U_p)(q+1-2U_q) = 1$, with $U_p \in \{\pm u_p, \pm v_p\}$, $U_q \in \{\pm u_q, \pm v_q\}$, we rewrite

$$\begin{aligned}(p+1-2U_p)(q+1-2U_q) &= n + p(1-2U_q) + q(1-2U_p) + (1-2U_p)(1-2U_q)\\ &= n - s,\end{aligned}$$

where $s = -p(1-2U_q) - q(1-2U_p) - (1-2U_p)(1-2U_q)$. Then the key equation can be transformed into the modular equation

$$(-k)(n-s) \equiv 1 \pmod e. \tag{7}$$

We set the bound $k < X = e^{\delta}$ for some $\delta > 0$. On the other hand, we have

$$\begin{aligned}|s| &= |p(1-2U_q) + q(1-2U_p) + (1-2U_p)(1-2U_q)|\\ &\le p|1-2U_q| + q|1-2U_p| + |1-2U_p||1-2U_q|.\end{aligned}$$

Using (4) and (5), and combining with Lemma 1, we get

$$|s| < 3p\sqrt{q} + 3q\sqrt{p} + 9\sqrt{pq} < 7p\sqrt{p} < 7(2n)^{\frac{3}{4}}.$$

Then, we set the bound $|s| < Y = 7(2n)^{\frac{3}{4}} = n^{\beta}$ with $\beta \approx \frac{3}{4}$. Now, we can apply Lemma 2 to the equation (7). It allows to find k and s in polynomial time under the condition $\delta < 1 - \sqrt{\beta} = 1 - \sqrt{\frac{3}{4}} \approx 0.133$. Using k and s, one can find d since $d = \frac{k(n-s)+1}{e}$. □

Remark 1. The bound on d in Theorem 6 is slightly better than the bound in Theorem 5. In both cases, one can find d and k which gives

$$(p + 1 - 2U_p)(q + 1 - 2U_q) = \frac{ed - 1}{k},$$

with $U_p \in \{\pm u_p, \pm v_p\}$, $U_q \in \{\pm u_q, \pm v_q\}$. By 3, we know that $(p + 1 - 2U_p)(q + 1 - 2U_q) > \frac{\sqrt{2}}{50} n$. This is large enough, and in general is hard to factor when n is large. Consequently, the method described in [32] to extract p and q can not be applied. As a consequence, finding p and q by the continued fraction method, or by lattice reduction techniques when the multiplier d is small is infeasible.

6.6 Resistance against discrete logarithm problem

The elliptic curve discrete logarithm problem (ECDLP) over a finite field $\mathbb{F}_p$ is the following computational problem: *Given an elliptic curve E over $\mathbb{F}_p$ and two points $P, Q \in E(\mathbb{F}_p)$, find an integer x, if any, such that $Q = aP$ in E.* ECDLP is still resistant to several non quantum algorithms and is behind the security of the elliptic curve cryptography (see [14] for more details).

For an elliptic curve defined over a finite ring such as $\mathbb{Z}/n\mathbb{Z}$ where $n = pq$ is an RSA modulus, the elliptic curve discrete logarithm problem can be solved if one knows p and q and if one can solve ECDLP in both $E(\mathbb{F}_p)$ and $E(\mathbb{F}_p)$. Hence, solving ECDLP on $E(\mathbb{Z}/n\mathbb{Z})$ is more difficult. This problem is used to build several elliptic curve based cryptosystems [20,11,19,24,33].

One more and crucial fact in our scheme is that a new elliptic curve is generated each time that a message is encrypted. This will make any generic or global discrete logarithm attack on our scheme infeasible.

6.7 Resistance against isomorphism and homomorphism attacks

Let $E_n(a)$ and $E_n(a')$ be two elliptic curves with equations $y^2 \equiv x^3 + ax \pmod{n}$ and $y^2 \equiv x^3 + a'x \pmod{n}$, arising from our scheme. Then $E_n(a)$ and $E_n(a')$ are isomorphic if and only if $a' = u^4 a$ for some $u \in \mathbb{Z}/n\mathbb{Z}$. As in KMOV [20], it is possible to launch an isomorphism attack on our scheme. Moreover, the encryption and decryption are homomorphic, that is

$$\mathrm{enc}(m_1 + m_2) = \mathrm{enc}(m_1) + \mathrm{enc}(m_2), \text{ and } \mathrm{dec}(c_1 + c_2) = \mathrm{dec}(c_1) + \mathrm{dec}(c_2),$$

when using the same elliptic curve. Also, it is possible to launch a homomorphism attack on our scheme, similar to that on KMOV. To overcome the isomorphism as well as the homomorphism attack, a hash function should be applied as shown in the signature scheme 5.3. This is sufficient to make the new scheme immune against the two kind of attacks.

6.8 Other attacks

There are more attacks in the literature that are related to some elliptic variants of RSA.

In [2], Bleichenbacher proposed four attacks on KMOV when one of the following situations is satisfied.

1. The ciphertext and half of the plaintext are known.
2. Three encryptions of the same message are encrypted with distinct public keys.
3. Six encryptions of linearly related messages are encrypted with distinct public keys.
4. Two encryptions of linearly related messages are encrypted with the same public key.

Similarly, in [23], Kurosawa et al. showed that both the KMOV scheme and Demytko's scheme are not secure when the same message is encrypted with a suitably large number of distinct keys.

We note that the former attacks are not applicable to our scheme since the encryption process is probabilistic. This implies that, to the contrary of the KMOV scheme and Demytko's scheme, if we encrypt the same message twice even with the same key in the new scheme, then the cyphertexts are different with a high probability because they depend on a randomly generated number in the encryption phase.

7 Conclusion

We proposed a new variant of RSA with a modulus of the form $n = pq$ where p and q are large prime numbers satisfying $p = u_p^2 + v_p^2$, $q = u_q^2 + v_q^2$, $u_p \equiv 3 \pmod 4$ and $u_q \equiv 3 \pmod 4$. The arithmetic of the new scheme uses elliptic curves with equations $y^2 = x^3 + ax$ over the finite ring $\mathbb{Z}/n\mathbb{Z}$. The encryption is probabilistic such that each encryption generates a new curve which result in new ciphertext in each call. We analyzed the security of the scheme and show that it is at least as hard as factoring.

References

1. Blake, I., Seroussi, G., Smart, N.: Elliptic curves in cryptography, volume 265 of London Math. Soc. Lecture Note Ser. Cambridge University Press, (1999)
2. Bleichenbacher, D.: On the security of the KMOV public key cryptosystem, LNCS 1294, Proc. Crypto 97, Springer-Verlag, (1997), pp. 235248.
3. Brent, R.P.: Recent Progress and Prospects for Integer Factorisation Algorithms, In: Du DZ., Eades P., Estivill-Castro V., Lin X., Sharma A. (eds) Computing and Combinatorics. COCOON 2000. Lecture Notes in Computer Science, vol 1858. Springer, Berlin, Heidelberg
4. Boneh, D.: Twenty years of attacks on the RSA cryptosystem, Notices Amer. Math. Soc. 46 (2). 203–213 (1999)

5. Boneh, D., Durfee, G., and Howgrave-Graham, N.: Factoring $N = p^r q$ for Large r. In M. Wiener, Ed., Crypto'99, Lecture Notes in Computer Science 1666, Springer-Verlag, p. 326–337 (1999)
6. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$, Advances in Cryptology-Eurocrypt'99, Lecture Notes in Computer Science Vol. 1592, Springer-Verlag, pp. 1–11 (1999)
7. Certicom Research. Standards for efficient cryptography 2: Recommended elliptic curve domain parameters. Standard SEC2, Certicom, 2000.
8. T. Collins, D. Hopkins, S. Langford, and M. Sabin. Public Key Cryptographic Apparatus and Method. US Patent #5,848,159. Jan. 1997.
9. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 10(4), pp. 233–260 (1997)
10. Couvreur, C., Quisquater, J.J.: Fast Decipherment Algorithm for RSA Public-Key Cryptosystem. Electronics Letters 18, pp. 905–907 (1982)
11. Demytko N.: A new elliptic curve based analogue of RSA, in T. Helleseth (ed.), EUROCRYPT 1993, Lecture Notes in Computer Science 765, Springer-Verlag, 40–49 (1994)
12. M. Elia, Continued Fractions and Factoring, arXiv:1905.10704 (2019) https://arxiv.org/abs/1905.10704
13. A. Fiat.: Batch RSA, In G. Brassard (ed.), Proceedings of Crypto 1989, vol. 435 of LNCS, pp. 175–185. Springer-Verlag (1989)
14. Galbraith, S.D., Gaudry, P.: Recent progress on the elliptic curve discrete logarithm problem. Des. Codes Cryptogr. 78, pp. 51-72 (2016)
15. Hardy, G.H., Wright, E.M.: An Introduction to Theory of Numbers, 5th Edition, The Clarendon Press Oxford University Press, New York (1979)
16. Hinek, M.: Cryptanalysis of RSA and its Variants, Chapman & Hall/CRC, Cryptography and Network Security Series, Boca Raton (2009)
17. D. Husemöller, Elliptic Curves, 2nd edn., Springer, 2004.
18. K. Ireland and M. Rosen. A Classical Introduction to Modern Number Theory, volume 84 of Graduate Texts in Mathematics. Springer-Verlag, 2nd edition (1990)
19. Koyama K.: Fast RSA type scheme based on singular cubic curve $y^2 + axy = x^3 \pmod{n}$. Proc. Eurocrypt'95, Lecture Notes in Computer Science, vo.921, Springer, Berlin, 1995, 329–339 (1995)
20. K. Koyama, U.M. Maurer, T. Okamoto, S.A. Vanstone, New Public-Key Schemes Based on Elliptic Curves over the Ring Z_n, CRYPTO 1991, Lecture Notes in Computer Science 576, 252-266.
21. Koblitz, N.: Elliptic curve cryptosystems. Mathematics of Computation, 48: pp. 203–209, (1987)
22. N. Kunihiro and K. Koyama, Equivalence between counting the number of points on elliptic curves over the ring $\mathbb{Z}_n$ and factoring n, LNCS 1403, Proceedings of Eurocrypt 1998, pp. 47-58 (1998)
23. Kaoru Kurosawa, Koji Okada, Shigeo Tsujii, Low exponent attack against elliptic curve RSA, Information Processing Letters, Volume 53, Issue 2, 1995, Pages 77-83,
24. H. Kuwakado, K. Koyama, and Y. Tsuruoka, A new RSA-type scheme based on singular cubic curves $y^2 = x^3 + bx^2 \pmod{n}$, IEICE Transactions on Fundamentals, vol. E78-A (1995) pp. 27–33.
25. Lenstra, H.: Factoring integers with elliptic curves, Annals of Mathematics, Vol. 126, pp. 649–673 (1987)
26. A. K. Lenstra, A.K., H. W. Lenstra, H.W. Jr.: The Development of the Number Field Sieve, Lecture Notes in Mathematics 1554, Springer-Verlag (1993)

27. S. Martín, P. Morillo, J.L. Villar, Computing the order of points on an elliptic curve modulo N is as difficult as factoring N, Applied Mathematics Letters Volume 14, Issue 3, April 2001, pp. 341-346 (2001)
28. Miller, V.S.: Use of elliptic curves in cryptography. In H. C. Williams, editor, Advances in Cryptology - CRYPTO'85, Vol. 218 of Lecture Notes in Computer Science, Springer-Verlag, pp. 417–426 (1986)
29. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system (2009) `https://bitcoin.org/bitcoin.pdf`
30. NIST: National Institute of Standards and Technology, Digital Signature Standard, FIPS PUB 186-2 (2000)
31. Nitaj, A.: Another generalization of Wiener's attack on RSA, In: Vaudenay, S. (eds.) Africacrypt 2008. LNCS, vol. 5023. 174190. Springer, Heidelberg (2008)
32. Nitaj, A., Fouotsa, E.: A new attack on RSA and Demytko's elliptic curve cryptosystem, Journal of Discrete Mathematical Sciences and Cryptography 22 (3), pp. 391-409 (2019)
33. Paillier, P.: Trapdooring Discrete Logarithms on Elliptic Curves over Rings, Trapdooring Discrete Logarithms on Elliptic Curves over Rings. In: Okamoto T. (eds) Advances in Cryptology ASIACRYPT 2000. ASIACRYPT 2000. Lecture Notes in Computer Science, vol 1976, Springer, Berlin, Heidelberg, pp. 573-584 (2000)
34. D. Pointcheval, "New public key cryptosystem based on the dependent RSA problem", Eurocrypt99 Springer-Verlag, 1999, 1592: pp. 239-254.
35. Pomerance, C.: The quadratic sieve factoring algorithm, Advances in Cryptology, Proc. Eurocrypt'84, LNCS 209, Springer-Verlag, Berlin, pp. 169182 (1985)
36. Rabin, M.O.: Digital signatures and public key functions as intractable as factoring. MIT Technical Report, MIT/LCS/TR-212 (1979)
37. Rivest, R., Shamir, A., Adleman, L.: A Method for Obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol. 21 (2), pp. 120–126 (1978)
38. Schmitt, S. , Zimmer, H.G., ProQuest (Firm): Elliptic curves : a computational approach, Walter de Gruyter, Berlin, New York (2003)
39. Silverman, J.H.: The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, Springer-Verlag, 106 (1986)
40. H.M Sun, M.E Wu, W.CTing and M.J Hinek, Dual RSA and its security analysis, IEEE Transactions on Information Theory, 2007; 53(8), pp. 2922-2933.
41. T. Takagi. Fast RSA-type Cryptosystem Modulo p^kq. In H. Krawczyk, ed., Proceedings of Crypto 1998, vol. 1462 of LNCS, pp. 318–326. Springer-Verlag, (1998)
42. Takayasu, A., Kunihiro N.: General bounds for small inverse problems and its applications to multi-prime RSA, Proc. ICISC 2014, LNCS 8949, pp. 3–17, Springer (2014)
43. L.C. Washington. Elliptic Curves: Number Theory and Cryptography. Chapman & Hall/CRC, Florida, 2003.
44. de Weger, B. :Cryptanalysis of RSA with small prime difference, Applicable Algebra in Engineering, Communication and Computing 13, pp. 17–28 (2002)
45. Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, pp. 553–558 (1990)