



Article

A New RSA Variant Based on Elliptic Curves

Maher Boudabra¹ and Abderrahmane Nitaj^{2,*}

¹ Department of Computing and Mathematics, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia; maher.boudabra@gmail.com

² Department of Mathematics, LMNO, Normandie University, UNICAEN, CNRS, LMNO, 14000 Caen, France

* Correspondence: abderrahmane.nitaj@unicaen.fr

Abstract: In this paper, we propose a new scheme based on ephemeral elliptic curves over a finite ring with an RSA modulus. The new scheme is a variant of both the RSA and the KMOV cryptosystems and can be used for both signature and encryption. We study the security of the new scheme and show that it is immune to 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 in 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

1. Introduction

The RSA system was proposed in 1977 by Rivest, Shamir, and Adleman [1] as a public key cryptosystem. The algorithm is based on a trap-door function that utilizes the Fermat–Euler theorem. The RSA algorithm's 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 [2,3]). On the other hand, to improve the efficiency of RSA, many variants have been proposed such as Batch RSA [4], Multi-Prime RSA [5], Prime Power RSA [6], CRT-RSA [7], Rebalanced RSA [8], Dual RSA [9], and DRSA [10].

In 1985, Koblitz [11] and Miller [12] showed independently how to use elliptic curves over finite fields for the design of cryptosystems. Such schemes contribute to 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 [13], key agreement such as ECDH [14], and Bitcoin [15].

In 1991, Koyama et al. [16] 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 of KMOV is that $(p+1)(q+1)P = \mathcal{O}$ holds for any point P on the elliptic curve, where \mathcal{O} is the point at infinity. In 1993, Demytko [17] 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 on 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.



Citation: Boudabra, M.; Nitaj, A. A New RSA Variant Based on Elliptic Curves. *Cryptography* **2023**, *7*, 37. <https://doi.org/10.3390/cryptography7030037>

Academic Editor: Josef Pieprzyk

Received: 31 May 2023

Revised: 28 June 2023

Accepted: 16 July 2023

Published: 19 July 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

This paper proposes 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 on 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 on the same elliptic curve over \mathbb{F}_q is $q + 1 - 2U_q$, 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

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

and

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

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 $\mathbb{Z}/n\mathbb{Z}$.

This paper studies 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 to 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 isomorphism and homomorphism attacks and ways to overcome them.

To summarize, our scheme is a generalization of the KMOV and Demytko’s schemes, which can be used for encryption and signatures. Moreover, it is a probabilistic algorithm that is secure against known classical attacks.

It should be noted that our scheme is not secure under quantum cryptanalysis because Shor’s [18] algorithm can factor any RSA modulus in polynomial time.

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

2. Useful Lemmas

This section presents some results that will be useful 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 the upper and lower bounds for p and q in terms of n [19].

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 [8] showed that RSA with a public key $(n = pq, e)$ is insecure if the private exponents d satisfy $ed - k(p - 1)(q - 1) = 1$ with $d < \frac{1}{3}n^{\frac{1}{4}}$. His method is based on the continued fraction algorithm and makes use of Theorem 184 in [20].

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

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

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

In 1996, Coppersmith [21] described a polynomial-time algorithm for finding small solutions of univariate modular polynomial equations. The method is based on lattice reduction. Since then, the Coppersmith method has been extended to solve modular polynomial equations with more variables and has been used for cryptanalysis, especially with regard to the RSA system. To illustrate this point, Boneh and Durfee [22] 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 [22–24]).

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

This section presents the main definitions and properties of elliptic curves. For more properties, see [25–28].

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, which is 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 the nonzero discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$. The set of points $P = (x, y)$ satisfying the equation, along with the infinity point \mathcal{O} , is denoted as $E(\mathbb{F}_p)$. The total number of points on $E(\mathbb{F}_p)$ is called the order of E and is denoted as $\#E(\mathbb{F}_p)$. 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 finding the exact value of $\#E(\mathbb{F}_p)$ for specific elliptic curves (see Theorem 5, page 307, Section 4, Chapter 18 of [29]).

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,

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

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 provides an explicit solution for $\left(\frac{a}{\pi}\right)_4 \pmod{\pi}$ (see page 122, Proposition 9.8.2 of [29]).

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 for 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 $(u_p v_p^{-1})^2 \equiv -1 \pmod{p}$. Next, let $a \in \mathbb{F}_p$ with $a \neq 0$. According to 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

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

and $a^{\frac{p-1}{4}} \equiv \pm u_p v_p^{-1} \pmod{p}$. To summarize, we have $a^{\frac{p-1}{4}} \in \{\pm 1, \pm u_p v_p^{-1}\}$ for modulo p . This concludes the proof. \square

The following result provides a simple proof for the estimation of $\#E(\mathbb{F}_p)$ when $p \equiv 1 \pmod{4}$. Alternative proofs can be found in [28] (Section 4.4 p. 115) and [29] (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,

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

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

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

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 $-u_p v_p^{-1} - i \equiv 0 \pmod{\pi}$ and $-u_p v_p^{-1} \equiv i \pmod{\pi}$. 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, $u_p v_p^{-1} \equiv -i \pmod{\pi}$ 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 concludes the proof. \square

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

This section briefly describes the theory of elliptic curves over the ring $\mathbb{Z}/n\mathbb{Z}$, where $n = pq$ is an RSA modulus (see [28], Section 2.11 and [30] 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 $P = (x, y)$ that satisfies the equation $y^2 = x^3 + ax + b \pmod{n}$, together with the point at infinity denoted as \mathcal{O}_n . According to 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 the points of the form (P_p, \mathcal{O}_q) with $P_p \neq \mathcal{O}_p$ are semi-zero points, whereas the 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 $E_n(a, b)$ using 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

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

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 $\text{gcd}(a, n) = 1$, 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

This section presents the new scheme and 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 levels.
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

$$\text{gcd}\left(e, \left((p + 1)^2 - 4u_p^2\right)\left((q + 1)^2 - 4u_q^2\right)\right) = 1.$$

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 $a \equiv (y_M^2 - r^3)r^{-1} \pmod n$. 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 $E_n(a)$. The point (x_C, y_C) is the encrypted message.

Decryption.

1. Compute $a \equiv (y_C^2 - x_C^3)x_C^{-1} \pmod n$. The elliptic curve $E_n(a)$ is defined by the equation $y^2 \equiv x^3 + ax \pmod n$.
2. Compute U_p using Formula (1) and U_q using Formula (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, $a \equiv (y_M^2 - r^3)r^{-1} \pmod{n}$ and $a' \equiv (y_M^2 - r'^3)r'^{-1} \pmod{n}$; and two elliptic curves with different equations.

5.2. A Numerical Example

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

$$\begin{aligned} u_1 &= 3253473156, v_1 = 3239617290, \\ u_p &= 4u_1 + 3 = 13013892627, v_p = 4v_1 + 2 = 12958469162, \\ p &= u_p^2 + v_p^2 = 337283324329589943373, \\ u_2 &= 4133795239, v_2 = 4069844016, \\ u_q &= 4u_2 + 3 = 16535180959, v_q = 4v_2 + 2 = 16279376066, \\ q &= u_q^2 + v_q^2 = 538430294445129796037, \\ n &= pq = 181603559630213323475279432919469869812801, \\ e &= 233, \\ r &= 276576193905959805653341, \\ y_M &= 24123988022450690140866. \end{aligned}$$

Then, one can compute the following parameters

$$\begin{aligned} a &\equiv \frac{y_M^2 - r^3}{r} \pmod{n} \\ &= 124892799480186717332460335305220886752546, \\ C &= e(r, y_M) = (x_C, y_C), \\ x_C &= 9895932661554916108079613524266560686478, \\ y_C &= 174838551993023162117462165695082973280827, \\ a^{\frac{p-1}{4}} &\equiv 1 \pmod{p}, \text{ hence } U_p = -u_p, \\ a^{\frac{q-1}{4}} &\equiv -1 \pmod{q}, \text{ hence } U_q = u_q, \\ \phi(a, n) &= (p + 1 - 2U_p)(q + 1 - 2U_q) \\ &= 181603559633073389948874511533493403987360, \\ d &\equiv e^{-1} \pmod{\phi(a, n)} = 35073648856172972307722545145953661714297, \\ m &= d(x_C, y_C) = (r, y_M), \end{aligned}$$

which shows that the decryption is correct.

In addition to the former example, we performed extensive experiments to test the validity of our scheme, as described in Section 5, using random parameters u_1, v_1, u_2, v_2, e, r , and y_M . In all cases, the scheme was successful without failure.

5.3. The New Signature Scheme

The encryption scheme can be transformed easily into a signature scheme using a hash function as follows. There is no particular specification for the hash function, so any of the most popular hash functions can be used such SHA-2, MD6, RIPEMD, HAVAL-128, etc.

- **Key generation.** The key generation scheme is similar to that of the encryption in Section 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 $a \equiv (y_M^2 - r^3)r^{-1} \pmod{n}$. 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 $E_n(a)$. The point (x_C, y_C) is the encrypted message.
 5. Compute the signature $s = \text{Hash}(r||y_M)$.
- **Decryption.**
 1. Compute $a \equiv (y_C^2 - x_C^3)x_C^{-1} \pmod{n}$. The elliptic curve $E_n(a)$ is defined by the equation $y^2 \equiv x^3 + ax \pmod{n}$.
 2. Compute U_p using Formula (1) and U_q using Formula (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

This section presents an analysis of the resistance of our scheme to the most well-known attacks that can be applied to it.

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 currently known factorization algorithms (see [31,32]). Indeed, Pollard’s rho method is ineffective since its run time is $\mathcal{O}(\sqrt{p}(\log(n))^2)$ and depends on the size of the prime number p found. This is similar to 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 [33] 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

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

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 $(x_1 y_1^{-1})^2 \equiv (x_2 y_2^{-1})^2 \equiv -1 \pmod{n}$. It follows that decomposing n as the sum of two squares in two different ways will provide 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

$t^2 \equiv -1 \pmod{n}$. This is known to be equivalent to factoring n , as in the quadratic sieve factoring algorithm [34] and in Rabin’s cryptosystem [35].

It is also known that by applying the continued fraction algorithm to \sqrt{n} , it is possible to find one representation of n (see [36]) as $n = x^2 + y^2$. This leads to one of the systems

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

This is insufficient for solving either of the two systems. Consequently, the representation of n as a sum of two squares by the continued fraction method is inadequate to factorize 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 [20]), that is, $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$. The number of decomposing n is such that a sum is denoted as $r_4(n)$, and for odd n , Jacobi’s four-square theorem formula gives $r_4(n) = 8 \sum_{m|n} m$ (Proposition 17.7.2 of [20]). For the modulus $n = pq = (u_p^2 + v_p^2)(u_q^2 + v_q^2)$, a specific decomposition as a 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 $n = pq = (u_p^2 + v_p^2)(u_q^2 + v_q^2)$. 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 obtain

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

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 the positive integers u_p and v_p that satisfy $u_p \equiv 3 \pmod{4}$, is unique, p can be decomposed as $p = r^2 + s^2$ with the 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 factorization 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 $r_4(n) = 8(1 + p + q + n)$, which represents 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. [37] 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 $\#E_q(a) = q + 1 - 2U_q$ using a specific algorithm to determine the order of an elliptic curve over a finite field such as the Schoof–Elkies–Atkin algorithm [38]. 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 obtain $V_p = v_p$, and

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

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

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

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

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

As a consequence, we have

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

and

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

By combining the former inequalities, we obtain

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

This implies that the order $\#E_n(a) = (p + 1 - 2U_p)(q + 1 - 2U_q)$ is sufficiently large. Moreover, with a high probability, it can take any shape, and consequently, there is no efficient method to factor it with a classical computer. Hence, finding p and q is not feasible in general.

It is important to note that the work of Kunihiro and Koyama [39] 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 [39], an oracle is needed that can count the number of points on every elliptic curve over $\mathbb{Z}/n\mathbb{Z}$, whereas in our situation, only $\#E_n(a) = (p + 1 - 2U_p)(q + 1 - 2U_q)$ 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 $n^{0.133}$, whereas in RSA, it should be larger than $n^{0.292}$.

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,

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

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,

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

Hence,

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

from which we deduce that

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

Similarly, we obtain

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

This leads to

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

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

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

This concludes the proof. \square

The following result shows that with regard to Wiener’s attack, the private exponent d can be very small in our scheme compared 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 $d < \frac{\sqrt{2}}{4}n^{\frac{1}{8}}$, 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 obtain

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

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

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

Then,

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

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

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

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 among the convergents of the continued expansion of $\frac{e}{n}$. Since the continued fraction algorithm computes the convergents of $\frac{e}{n}$ with complexity $\mathcal{O}(\log(n))$, one finds k and d in polynomial time. \square

Theorem 5 shows that when $d < \frac{\sqrt{2}}{4}n^{\frac{1}{8}}$, it is possible to retrieve the private exponent d . If $d > \frac{\sqrt{2}}{4}n^{\frac{1}{8}}$, the continued fraction attack does not apply and d may not be found using this technique.

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 $d < n^{0.133}$, 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

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

By combining (4) and (5) with Lemma 1, we obtain

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

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 Equation (7). This allows us 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 $d = \frac{k(n-s)+1}{e}$. \square

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 $U_p \in \{\pm u_p, \pm v_p\}$, $U_q \in \{\pm u_q, \pm v_q\}$. According to (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 [40] for extracting p and q cannot be applied. As a consequence, finding p and q using the continued fraction method or the 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 . The ECDLP is still resistant to several non-quantum algorithms and is the foundation of the security of elliptic curve cryptography (see [41] 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 the ECDLP in both $E(\mathbb{F}_p)$ and $E(\mathbb{F}_q)$. Hence, solving the ECDLP on $E(\mathbb{Z}/n\mathbb{Z})$ is more difficult. This problem is used to build several elliptic curve-based cryptosystems [16,17,42–44].

One more crucial fact of our scheme is that a new elliptic curve is generated each time a message is encrypted. This ensures that any generic or global discrete-logarithm attacks on our scheme are 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 $a' = u^4a$ for some $u \in \mathbb{Z}/n\mathbb{Z}$. As in KMOV [16], it is possible to launch an isomorphism attack on our scheme. Moreover, the encryption and decryption are homomorphic, that is,

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

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 isomorphism and homomorphism attacks, a hash function should be applied, as shown in the signature in Section 5.3. This is sufficient to ensure that the new scheme is immune to the two types of attacks.

6.8. Other Attacks

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

In [45], 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 [46], Kurosawa et al. showed that both the KMOV and Demytko's schemes are not secure when the same message is encrypted with a suitably large number of distinct keys.

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

7. Conclusions

In this paper, 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 the equation $y^2 = x^3 + ax$ over the finite ring $\mathbb{Z}/n\mathbb{Z}$. The encryption is probabilistic, such that each encryption generates a new curve that results in a new ciphertext with each call. We analyzed the security of the scheme and showed that it is resistant to known attacks on the topic.

Author Contributions: Conceptualization, M.B. and A.N.; methodology, M.B. and A.N.; software, M.B. and A.N.; validation, M.B. and A.N.; formal analysis, M.B. and A.N.; investigation, M.B. and A.N.; resources, M.B. and A.N.; data curation, M.B. and A.N.; writing—original draft preparation, M.B. and A.N.; writing—review and editing, M.B. and A.N.; visualization, M.B. and A.N.; supervision, M.B. and A.N.; project administration, M.B. and A.N.; funding acquisition, M.B. and A.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rivest, R.; Shamir, A.; Adleman, L. A Method for Obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
2. Boneh, D. Twenty years of attacks on the RSA cryptosystem. *Not. Am. Math. Soc.* **1999**, *46*, 203–213.
3. Hinek, M. *Cryptanalysis of RSA and its Variants*; Cryptography and Network Security Series; Chapman & Hall/CRC Press: Boca Raton, FL, USA, 2009.
4. Fiat, A. Batch RSA. In Proceedings of the Crypto 1989, 9th Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 1989. Brassard, G., Ed.; Volume 435 of LNCS; Springer: Berlin/Heidelberg, Germany, 1989; pp. 175–185.
5. Collins, T.; Hopkins, D.; Langford, S.; Sabin, M. Public Key Cryptographic Apparatus and Method. U.S. Patent, 5,848,159, 16 January 1997.
6. Takagi, T. Fast RSA-type Cryptosystem Modulo p^kq . In Proceedings of the Crypto 1998, 18th Annual International Cryptology Conference, Santa Barbara, CA, USA, 23–27 August 1998; Krawczyk, H., Ed.; Volume 1462 of LNCS; Springer: Berlin/Heidelberg, Germany, 1998; pp. 318–326.
7. Couvreur, C.; Quisquater, J.J. Fast Decipherment Algorithm for RSA Public-Key Cryptosystem. *Electron. Lett.* **1982**, *18*, 905–907.
8. Wiener, M. Cryptanalysis of short RSA secret exponents. *IEEE Trans. Inf. Theory* **1990**, *36*, 553–558. [CrossRef]
9. Sun, H.M.; Wu, M.E.; Ting, W.C.; Hinek, M.J. Dual RSA and its security analysis. *IEEE Trans. Inf. Theory* **2007**, *53*, 2922–2933.
10. Pointcheval, D. New public key cryptosystem based on the dependent RSA problem. In *Advances in Cryptology-EUROCRYPT'99*. EUROCRYPT 1999; Stern, J., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1592, pp. 239–254.
11. Koblitz, N. Elliptic curve cryptosystems. *Math. Comput.* **1987**, *48*, 203–209. [CrossRef]
12. Miller, V.S. Use of elliptic curves in cryptography. In *Advances in Cryptology-CRYPTO'85*; Lecture Notes in Computer Science; Williams, H.C., Ed.; Springer: Berlin/Heidelberg, Germany, 1986; Volume 218, pp. 417–426.
13. *Federal Information Processing Standards Publication, FIPS PUB 186-2*; National Institute of Standards and Technology, Digital Signature Standard: Gaithersburg, MD, USA, 2000.
14. Certicom Research. Standards for Efficient Cryptography, SEC 2 : Recommended Elliptic Curve Domain Parameters. 27 January 2010 Version 2.0. Available online: <https://www.secg.org/sec2-v2.pdf> (accessed on 10 July 2023).
15. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 10 July 2023).
16. Koyama, K.; Maurer, U.M.; Okamoto, T.; Vanstone, S.A. New Public-Key Schemes Based on Elliptic Curves over the Ring Z_n . In *Annual International Cryptology Conference*; Lecture Notes in Computer Science 576; Springer: Berlin/Heidelberg, Germany, 1991; pp. 252–266.
17. Demytko, N. A new elliptic curve based analogue of RSA. In *Advances in Cryptology—EUROCRYPT'93: Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, Norway, 23–27 May 1993*; Lecture Notes in Computer Science 765; Hellesteth, T., Ed.; Springer: Berlin/Heidelberg, Germany, 1994; pp. 40–49.
18. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509. [CrossRef]
19. Nitaj, A. Another generalization of Wiener's attack on RSA. In *International Conference on Cryptology in Africa, AFRICACRYPT 2008*; Vaudenay, S., Ed.; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5023, pp. 174–190.
20. Hardy, G.H.; Wright, E.M. *An Introduction to Theory of Numbers*, 5th ed.; The Clarendon Press Oxford University Press: New York, NY, USA, 1979.
21. Coppersmith, D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. Cryptol.* **1997**, *10*, 233–260 [CrossRef]
22. Boneh, D.; Durfee, G. Cryptanalysis of RSA with private key d less than $N^{0.292}$. In *Advances in Cryptology-EUROCRYPT'99: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, 2–6 May 1999*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1592, pp. 1–11.
23. Takayasu, A.; Kunihiro, N. General bounds for small inverse problems and its applications to multi-prime RSA. In *Proceedings of the Information Security and Cryptology—ICISC 2014, Seoul, Korea, 3–5 December 2014*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 3–17.
24. de Weger, B. Cryptanalysis of RSA with small prime difference. *Appl. Algebra Eng. Commun. Comput.* **2002**, *13*, 17–28. [CrossRef]
25. Husemöller, D. *Elliptic Curves*, 2nd ed.; Springer: Berlin/Heidelberg, Germany, 2004.
26. Schmitt, S.; Zimmer, H.G.; ProQuest (Firm). *Elliptic Curves: A Computational Approach*; Walter de Gruyter: Berlin, Germany; New York, NY, USA, 2003.
27. Silverman, J.H. *The Arithmetic of Elliptic Curves*; Graduate Texts in Mathematics; Springer: Berlin/Heidelberg, Germany, 1986; Volume 106.
28. Washington, L.C. *Elliptic Curves: Number Theory and Cryptography*; Chapman & Hall/CRC: Boca Raton, FL, USA, 2003.
29. Ireland, K.; Rosen, M. *A Classical Introduction to Modern Number Theory*, 2nd ed.; Volume 84 of Graduate Texts in Mathematics; Springer: Berlin/Heidelberg, Germany, 1990.
30. Lenstra, H. Factoring integers with elliptic curves. *Ann. Math.* **1987**, *126*, 649–673. [CrossRef]

31. Brent, R.P. Recent Progress and Prospects for Integer Factorisation Algorithms. In *Proceedings of the Computing and Combinatorics. 6th Annual International Conference, COCOON 2000, Sydney, Australia, 26–28 July 2000*; Lecture Notes in Computer Science; Du, D.Z., Eades, P., Estivill-Castro, V., Lin, X., Sharma, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2000; Volume 1858.
32. Boneh, D.; Durfee, G.; Howgrave-Graham, N. Factoring $N = p^r q$ for Large r . In *Crypto'99*; Lecture Notes in Computer Science 1666; Wiener, M., Ed.; Springer: Berlin/Heidelberg, Germany, 1999; pp. 326–337.
33. Lenstra, A.K.; Lenstra, H.W., Jr. *The Development of the Number Field Sieve*; Lecture Notes in Mathematics 1554; Springer: Berlin/Heidelberg, Germany, 1993.
34. Pomerance, C. The quadratic sieve factoring algorithm. In *Workshop on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1985; pp. 169–182.
35. Rabin, M.O. *Digital Signatures and Public Key Functions as Intractable as Factoring*; MIT Technical Report, MIT/LCS/TR-212; 1979.
36. Elia, M. Continued Fractions and Factoring. *arXiv* **2019**, arXiv:1905.10704.
37. Martín, S.; Morillo, P.; Villar, J.L. Computing the order of points on an elliptic curve modulo N is as difficult as factoring N . *Appl. Math. Lett.* **2001**, *14*, pp. 341–346. [[CrossRef](#)]
38. Blake, I.; Seroussi, G.; Smart, N. *Elliptic Curves in Cryptography*; Volume 265 of London Mathematical Society Lecture Note Series. Cambridge: Cambridge University Press, 1999.
39. Kunihiko, N.; Koyama, K. Equivalence between counting the number of points on elliptic curves over the ring \mathbb{Z}_n and factoring n . In *LNCS 1403, Proceedings of Eurocrypt 1998*; 1998; pp. 47–58.
40. Nitaj, A.; Fouotsa, E. A new attack on RSA and Demytko's elliptic curve cryptosystem. *J. Discret. Math. Sci. Cryptogr.* **2019**, *22*, 391–409. [[CrossRef](#)]
41. Galbraith, S.D.; Gaudry, P. Recent progress on the elliptic curve discrete logarithm problem. *Des. Codes Cryptogr.* **2016**, *78*, 51–72. [[CrossRef](#)]
42. Koyama, K. Fast RSA type scheme based on singular cubic curve $y^2 + axy = x^3 \pmod{n}$. In *Advances in Cryptology—EUROCRYPT'95: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, 21–25 May 1995*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1995; Volume 921, pp. 329–339.
43. Kuwakado, H.; Koyama, K.; Tsuruoka, Y. A new RSA-type scheme based on singular cubic curves $y^2 = x^3 + bx^2 \pmod{n}$. *IEICE Trans. Fundam.* **1995**, *E78-A*, 27–33.
44. Paillier, P. Trapdoor Discrete Logarithms on Elliptic Curves over Rings. In *Advances in Cryptology—ASIACRYPT 2000*; Lecture Notes in Computer Science; Okamoto, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2000; Volume 1976, pp. 573–584.
45. Bleichenbacher, D. On the Security of the KMOV Public Key Cryptosystem; In *Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 1997; pp. 235–248.
46. Kurosawa, K.; Okada, K.; Tsujii, S. Low exponent attack against elliptic curve RSA. *Inf. Process. Lett.* **1995**, *53*, 77–83. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.