A New Public Key Cryptosystem Based on Edwards Curves

Maher Boudabra[1] and Abderrahmane Nitaj[2]

[1] Université de Monastir, Tunisia
maher_boudabra@protonmail.com
[2] LMNO, Université de Caen Normandie, France
abderrahmane.nitaj@unicaen.fr

Abstract. The elliptic curve cryptography plays a central role in various cryptographic schemes and protocols. For efficiency reasons, Edwards curves and twisted Edwards curves have been introduced. In this paper, we study the properties of twisted Edwards curves on the ring $\mathbb{Z}/n\mathbb{Z}$ where $n = p^r q^s$ is a prime power RSA modulus and propose a new scheme and study its efficiency and security.

Keywords: Elliptic curves, Twisted Edwards curves, RSA cryptosystem, KMOV cryptosystem

1 Introduction

In 2007, Edwards [9] introduced a new normal form of elliptic curves over a field $\mathbb{K}$ with characteristic not equal to 2. He showed that any elliptic curve over $\mathbb{K}$ is birationally equivalent over some extension of $\mathbb{K}$ to a curve with an equation of the form

$$x^2 + y^2 = c^2\left(1 + x^2y^2\right), \quad c \in \mathbb{K}, \quad c^5 \neq c.$$

Bernstein and Lange [2] generalized the former form to the short form

$$E_d : \ x^2 + y^2 = 1 + dx^2y^2,$$

where $d \in \mathbb{K} - \{0, 1\}$. The addition law for Edwards curves is given by

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1y_1x_2y_2}, \frac{y_2y_1 - x_2x_1}{1 - dx_1y_1x_2y_2}\right),$$

and the same formulas can also be used for doubling. For this law, the point $(0, 1)$ is the neutral element and the negative of a point (x, y) is $(-x, y)$. Moreover, it is shown in [2] that when d is not a square in K, then the sum of any two points (x_1, y_1), (x_2, y_2) is always defined.

In [1], Bernstein et al. introduced the twisted Edwards curves with an equation

$$E_{a,d} : \ ax^2 + y^2 = 1 + dx^2y^2,$$

where $a, d \in \mathbb{K}$ are non zero and distinct. The addition law is defined on $E_{a,d}$ by the rule

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 y_1 x_2 y_2}, \frac{y_2 y_1 - a x_2 x_1}{1 - d x_1 y_1 x_2 y_2} \right).$$

For this law, the identity is still $(0, 1)$ and the negative of a point (x, y) is $(-x, y)$.

The operations on twisted Edwards curves are more efficient than for most of the other forms of elliptic curves and the discrete logarithm problem is hard to solve. This makes twisted Edwards curves suitable for cryptographic applications.

In this paper, we study various properties of the twisted Edwards curves. We first give a study of the twisted Edwards curves on the finite field $\mathbb{Z}/p\mathbb{Z}$ where $p \geq 5$ is a prime number, and generalize it to the rings $\mathbb{Z}/p^r\mathbb{Z}$ and $\mathbb{Z}/p^r q^s\mathbb{Z}$. Then, using the arithmetic properties of the twisted Edwards curves on the ring $\mathbb{Z}/p^r q^s\mathbb{Z}$, we propose a new public key scheme and study its efficiency and its security. The new scheme generalizes two former schemes, namely the KMOV cryptosystem [12] with a modulus of the form $n = pq$ and an elliptic curve with equation $y^2 \equiv x^3 + b \pmod{n}$ and its extension to a prime power RSA modulus $n = p^r q^s$ with a similar equation [5]. The new scheme uses a prime power RSA modulus $n = p^r q^s$ and a twisted Edwards curve with equation

$$-dx^2 + y^2 \equiv 1 + dx^2 y^2 \pmod{n}.$$

The use of a prime power RSA in cryptography has been proposed for some cryptographic applications (see [20,10,16]). The security of such moduli was studied in [7] where it is recommended to use moduli of the form $p^r q^s$ where p, q are large prime numbers with the same size and r, s are small exponents satisfying the conditions of Table 1.

Modulus size in bits	Form of the modulus
2048	pq, p^2q
3072	pq, p^2q
3584	pq, p^2q
4096	pq, p^2q, p^3q
8192	pq, p^2q, p^3q, p^3q^2

Table 1. Optimal number of prime factors for a specific modulus size [7].

The rest of the paper is organized as follows. In Section 2, we study various arithmetical properties of a twisted Edwards curve on the finite field $\mathbb{Z}/p\mathbb{Z}$. In Section 3, we extend the former properties to the ring $\mathbb{Z}/p^r\mathbb{Z}$. Similarly, we extend the properties to $\mathbb{Z}/p^r q^s\mathbb{Z}$ in Section 4. In section 5, we present our new scheme. We study its efficiency and security in Section 6. We conclude the paper in Section 6.

2 Twisted Edwards Curves over the Field $\mathbb{Z}/p\mathbb{Z}$

In this section, we present various results on the Edwards curves over a finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ where $p \geq 5$ is a prime number and give an explicit estimation for the number of points on a twisted Edwards curve when $p \equiv 3 \pmod 4$ and $p \equiv 11 \pmod{12}$.

Let a be an integer. The Legendre symbol of a modulo p, denoted by $\left(\frac{\cdot}{p}\right)$, is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \bmod p, \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a non-quadratic residue modulo } p. \end{cases}$$

The following classical result concerns the Legendre symbol for -1 (see [6], Chapter 7).

Lemma 1. *Let p be an odd prime. Then*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

$$\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8, \\ -1 & \text{if } p \equiv \pm 3 \pmod 8, \end{cases}$$

$$\left(\frac{3}{p}\right) = 3^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12}, \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}, \end{cases}$$

A special case for the theory of Edwards curves is when the field $\mathbb{K}$ is the finite field $\mathbb{F}_p$. Let a and d be integers such that d is not a square in $\mathbb{Z}/p\mathbb{Z}$. The following result states the addition law on the twisted Edwards curve $E_{a,d,p}$ with the equation $E_{a,d,p}: \ ax^2 + y^2 \equiv 1 + dx^2y^2 \pmod p$.

Theorem 1. *Let $p > 2$ be a prime number and a and d be integer such that a is a square and d is not a square in $\mathbb{Z}/p\mathbb{Z}$. Let (x_1, y_1) and (x_2, y_2) be two points on $E_{a,d,p}$. Then the addition law*

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1y_1x_2y_2}, \frac{y_2y_1 - ax_2x_1}{1 - dx_1y_1x_2y_2}\right),$$

is always defined on the twisted Edwards curve $E_{a,d,p}$.

Proof. The proof of the theorem is presented in Appendix A

Observe that the condition that a is a square is necessary for the possibility of the addition. Indeed, let $p = 23$, $a = 19$ and $d = 14$. Then a and d are not squares in $\mathbb{Z}/p\mathbb{Z}$. The points $(x_1, y_1) = (1, 9)$ and $(x_2, y_2) = (4, 12)$ are on the curve $E_{a,d,p}$ with $1 + dx_1x_2y_1y_2 \equiv 0 \pmod p$ which implies that the sum $(x_1, y_1) + (x_2, y_2)$ is not defined on $E_{a,d,p}$. In the following results, we suppose that a and d are arbitrary integers satisfying $ad(a - d) \not\equiv 0 \pmod p$

Lemma 2. *Let $p \geq 5$ be a prime number and a, d be integers such that $ad(a-d) \neq 0$. Then the twisted Edwards curve $E_{a,d,p}$ with equation $ax^2 + y^2 \equiv 1 + dx^2y^2 \pmod{p}$ is birationally equivalent to the short Weierstrass form $W_{a,d,p}$ with equation*

$$v^2 \equiv u^3 - \frac{1}{3}\left(a^2 + 14ad + d^2\right)u - \frac{2}{27}(a+d)\left(a^2 - 34ad + d^2\right) \pmod{p},$$

with the transformation modulo p

$$(x,y) \to (u,v) = \begin{cases} \mathcal{O} & \text{if } (x,y) = (0,1) \\ \left(\frac{2}{3}(a+d), 0\right) & \text{if } (x,y) = (0,-1) \\ \left(\frac{5a-d+(a-5d)y}{3(1-y)}, \frac{2(a-d)(1+y)}{(1-y)x}\right) & \text{if } (x,y) \neq (0,1). \end{cases}$$

Proof. The proof of the theorem is presented in Appendix B

The following result gives the inverse transformation of Lemma 2.

Lemma 3. *Let $p \geq 5$ be a prime number and a and d be integers such that $ad(a-d) \neq 0$. The short Weierstrass form $W_{a,d,p}$ with the equation*

$$v^2 \equiv u^3 - \frac{1}{3}\left(a^2 + 14ad + d^2\right)u - \frac{2}{27}(a+d)\left(a^2 - 34ad + d^2\right) \pmod{p},$$

is birationally equivalent to the twisted Edwards curve $E_{a,d,p}$ with the transformation

$$(u,v) \to (x,y) = \begin{cases} (0,1) & \text{if } (u,v) = \mathcal{O} \\ (0,-1) & \text{if } (u,v) = \left(\frac{2}{3}(a+d), 0\right) \\ \left(\frac{2(3u-2a-2d)}{3v}, \frac{3u-5a+d}{3u+a-5d}\right) & \text{if } u \neq -\frac{1}{3}(a-5d) \text{ and } v \neq 0. \end{cases}$$

If ad is a square in $\mathbb{Z}/p\mathbb{Z}$, then the points $(u,v) = \left(-\frac{1}{3}\left(a + d \pm 6\sqrt{ad}\right), 0\right) \in W_{a,d,p}$ are not mapped into $E_{a,d,p}$.

If d is a square in $\mathbb{Z}/p\mathbb{Z}$, then the points $(u,v) = \left(-\frac{1}{3}(a-5d), \pm 2\sqrt{d}(a-d)\right) \in W_{a,d,p}$ are not mapped into $E_{a,d,p}$.

Proof. The proof of the theorem is presented in Appendix C

Combining Lemma 2 and Lemma 3, we easily get the following result regarding the number of points of the twisted Edwards curve $E_{a,d,p}$ in terms of the number of points of the Weierstrass curve $W_{a,d,p}$.

Lemma 4. *Let $p \geq 5$ be a prime number and a and d be integers such that $ad(a-d) \neq 0$. Then*

$$\#E_{a,d,p} = \begin{cases} \#W_{a,d,p} & \text{if } d \text{ and } ad \text{ are not squares in } \mathbb{Z}/p\mathbb{Z}, \\ \#W_{a,d,p} - 4 & \text{if } ad \text{ and } d \text{ are squares in } \mathbb{Z}/p\mathbb{Z}, \\ \#W_{a,d,p} - 2 & \text{if } ad \text{ or } d \text{ is a square in } \mathbb{Z}/p\mathbb{Z}. \end{cases}$$

Proof. First, suppose that d and ad are not squares in $\mathbb{Z}/p\mathbb{Z}$. Then by Lemma 2 and Lemma 3, the curves $E_{a,d,p}$ and $W_{a,d,p}$ are isomorphic. This implies that $\#E_{a,d,p} = \#W_{a,d,p}$.

Second, suppose that both ad and d are squares in $\mathbb{Z}/p\mathbb{Z}$. Then by Lemma 3, the points $(u,v) = \left(-\frac{1}{3}\left(a+d \pm 6\sqrt{ad}\right), 0\right) \in W_{a,d,p}$ as well as the points $(u,v) = \left(-\frac{1}{3}(a-5d), \pm 2\sqrt{d}(a-d)\right) \in W_{a,d,p}$ are not mapped in $E_{a,d,p}$. Then $\#E_{a,d,p} = \#W_{a,d,p} - 4$.

Next, suppose that ad is a square in $\mathbb{Z}/p\mathbb{Z}$ but d is not a square. Then by Lemma 3, the two points $(u,v) = \left(-\frac{1}{3}\left(a+d \pm 6\sqrt{ad}\right), 0\right) \in W_{a,d,p}$ are not mapped in $E_{a,d,p}$. Hence $\#E_{a,d,p} = \#W_{a,d,p} - 2$.

Finally, suppose that d is a square in $\mathbb{Z}/p\mathbb{Z}$ but ad is not a square. Then by Lemma 3, the two points $(u,v) = \left(-\frac{1}{3}(a-5d), \pm 2\sqrt{d}(a-d)\right) \in W_{a,d,p}$ are not mapped in $E_{a,d,p}$. This gives $\#E_{a,d,p} = \#W_{a,d,p} - 2$. □

The following result deals with two integers a and d such that $\frac{a}{d} \equiv -1 \pmod{p}$.

Lemma 5. *Let p be a prime number such that $p \equiv 3 \pmod 4$. If $\frac{a}{d} \equiv -1 \pmod p$, then one of the integers a or d is a square in $\mathbb{Z}/p\mathbb{Z}$ and the other is a non square.*

Proof. Suppose that $p \equiv 3 \pmod 4$. Then by Lemma 1, -1 is not a square in $\mathbb{Z}/p\mathbb{Z}$. Hence, if $\frac{a}{d} \equiv -1 \pmod p$, then $a \equiv -d \pmod p$ and

$$\left(\frac{a}{p}\right) = \left(\frac{-d}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d}{p}\right) = -\left(\frac{d}{p}\right).$$

It follows that a and d are of different shapes. □

The following result concerns two integers a and d such that $\frac{a}{d} \equiv -7 \pm 4\sqrt{3} \pmod p$.

Lemma 6. *Let p be a prime number such that $p \equiv 11 \pmod{12}$. If $\frac{a}{d} \equiv -7 \pm 4\sqrt{3} \pmod p$, then one of the integers a or d is a square in $\mathbb{Z}/p\mathbb{Z}$ and the other is a non square.*

Proof. Suppose that $p \equiv 11 \pmod{12}$. Then by Lemma 1, $\sqrt{3}$ exists in $\mathbb{Z}/p\mathbb{Z}$ and can be computed as $\sqrt{3} \equiv 3^{\frac{p+1}{4}} \pmod p$. Next suppose that $\frac{a}{d} \equiv -7 \pm 4\sqrt{3} \pmod p$. Then

$$a \equiv \left(-7 \pm 4\sqrt{3}\right) d \equiv -\left(2 \mp \sqrt{3}\right)^2 d \pmod p.$$

Since $p \equiv 3 \pmod 4$, then by Lemma 1, -1 is not a square in $\mathbb{Z}/p\mathbb{Z}$. Hence

$$\left(\frac{a}{p}\right) = \left(\frac{-\left(2 \mp \sqrt{3}\right)^2 d}{p}\right) = -\left(\frac{d}{p}\right),$$

and a and d are of different shapes. □

The following result deals with the integers a and d such that $\frac{a}{d} \equiv 17 \pm 12\sqrt{2} \pmod{p}$.

Lemma 7. *Let p be a prime number such that $p \equiv 7 \pmod 8$. If $\frac{a}{d} \equiv 17 \pm 12\sqrt{2} \pmod{p}$, then a and d are both squares or non squares in $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Suppose that $p \equiv 7 \pmod 8$. Then $\sqrt{2}$ exists in $\mathbb{Z}/p\mathbb{Z}$ and can be computed as $\sqrt{2} \equiv 2^{\frac{p+1}{4}} \pmod p$. Now, suppose that $\frac{a}{d} \equiv 17 \pm 12\sqrt{2} \pmod p$. Then

$$a \equiv \left(17 \pm 12\sqrt{2}\right) d \equiv \left(3 \pm 2\sqrt{2}\right)^2 d$$

It follows that

$$\left(\frac{a}{p}\right) = \left(\frac{\left(3 \pm 2\sqrt{2}\right)^2 d}{p}\right) = \left(\frac{d}{p}\right),$$

and a and d are of the same shape. □

Let $p \geq 5$ be a prime number and $E_p(a_4, a_6)$ be an elliptic curve with the equation

$$y^2 \equiv x^3 + a_4 x + a_6 \pmod p,$$

where $4a_4^3 + 27a_6^2 \not\equiv 0 \pmod p$. In some cases, it is easy to find the number of points of the curve $E_p(a_4, a_6)$. The following result gives an explicit value for the number of points on the curve $E_p(a_4, a_6)$ (see [21,11,19] for more details).

Lemma 8. *Let $E_p(a_4, a_6)$ be an elliptic curve over $\mathbb{F}_p$ with the equation the $y^2 \equiv x^3 + a_4 x + a_6 \pmod p$. The number of points on $E_p(a_4, a_6)$ is $\#E_p(a_4, a_6) = p+1$ if*

$$a_4 = 0,\ a_6 \neq 0,\ p \equiv 2 \pmod 3 \text{ or } a_4 \neq 0,\ a_6 = 0,\ p \equiv 3 \pmod 4.$$

Combining Lemma 2, Lemma 3 and Lemma 8, we get three families of twisted Edwards curve $E_{a,d,p}$ such that $\#E_{a,d,p} = p + 1$.

Lemma 9. *Let $p \geq 5$ be a prime number. Let $E_{a,d,p}$ be a twisted Edwards curve over $\mathbb{Z}/p\mathbb{Z}$. Then for $\frac{a}{d} \pmod p \in \left\{-1, -7 \pm 4\sqrt{3}\right\}$, the number of points on $E_{a,d,p}$ is $\#E_{d,p} = p + 1$ if one of the following condition is fulfilled*

1. *$p \equiv 3 \pmod 4$, $\frac{a}{d} \equiv -1 \pmod p$, and a is a square,*
2. *$p \equiv 11 \pmod{12}$, $\frac{a}{d} \equiv -7 \pm 4\sqrt{3} \pmod p$, and a is a square.*

Proof. For $p \geq 5$, let $E_{a,d,p}$ be a twisted Edwards curve. Then, by Lemma 2, $E_{a,d,p}$ is birationally equivalent to a short Weierstrass equation with equation $y^2 \equiv x^3 + a_4 x + a_6 \pmod p$ where

$$a_4 = -\frac{1}{3}\left(a^2 + 14ad + d^2\right), \quad a_6 = -\frac{2}{27}(a+d)\left(a^2 - 34ad + d^2\right).$$

First, suppose that $\frac{a}{d} \equiv -1 \pmod{p}$. Then $a_6 \equiv 0 \pmod{p}$. If a is a square and $p \equiv 3 \pmod{4}$, then by Lemma 5, d is not a square. Hence, by Lemma 4 and Lemma 8, we get $\#E_{a,d,p} = \#W_{a,d,p} = p + 1$.

Next, suppose that $\frac{a}{d} \equiv -7 \pm 4\sqrt{3} \pmod{p}$. Then $a_4 \equiv 0 \pmod{p}$ and by Lemma 1, a condition that $\sqrt{3}$ exists modulo p is that $p \equiv \pm 1 \pmod{12}$. If moreover $p \equiv 2 \pmod{3}$, then $p \equiv 11 \pmod{12}$. Under this condition, we have $\sqrt{3} \equiv 3^{\frac{p+1}{4}} \pmod{p}$. If a is a square in $\mathbb{Z}/p\mathbb{Z}$, then by Lemma 6, d is not a square and by Lemma 4 and Lemma 8, we have $\#E_{a,d,p} = \#W_{a,d,p} = p + 1$. □

As a consequence of Lemma 9, we have the following result.

Lemma 10. *Let $E_{a,d,p}$ be a twisted Edwards curve. If p is prime with $p \equiv 3 \pmod{4}$ and $\frac{a}{d} \equiv -1 \pmod{p}$, then for any point $(x, y) \in E_{a,d,p}$, we have*

$$(p+1)(x,y) = \begin{cases} (0,1) & \text{if } a \text{ is a square in } \mathbb{Z}/p\mathbb{Z}, \\ (0,1) \text{ or undefined} & \text{if } a \text{ is not a square in } \mathbb{Z}/p\mathbb{Z}. \end{cases}$$

Proof. Suppose that $\frac{a}{d} \equiv -1 \pmod{p}$ and a is a square in $\mathbb{Z}/p\mathbb{Z}$, then by Lemma 5, d is not a square and by Lemma 1, the addition is always defined. Since by Lemma 9 we have $\#E_{a,d,p} = p + 1$, then $(p + 1)(x, y) = (0, 1)$ for any point $(x, y) \in E_{a,d,p}$. If a is not a square, then d is a square and $(p + 1)(x, y)$ could not be defined on $E_{a,d,p}$. When $(p + 1)(x, y)$ is defined, then since $E_{a,d,p}$ is mapped to $W_{a,d,p}$ and $\#W_{a,d,p} = p + 1$, then $(p + 1)(x, y) = (0, 1)$. □

The following result deals with the situation where $\frac{a}{d} \equiv -7 \pm 4\sqrt{3} \pmod{p}$.

Lemma 11. *Let $E_{a,d,p}$ be a twisted Edwards curve with $\frac{a}{d} \equiv -7 \pm 4\sqrt{3} \pmod{p}$. If p is prime with $p \equiv 11 \pmod{12}$, then for any point $(x, y) \in E_{a,d,p}$, we have*

$$(p+1)(x,y) = \begin{cases} (0,1) & \text{if } a \text{ is a square in } \mathbb{Z}/p\mathbb{Z}, \\ (0,1) \text{ or undefined} & \text{if } a \text{ is not a square.} \end{cases}$$

Proof. Suppose that $\frac{a}{d} \equiv -7 \pm 4\sqrt{3} \pmod{p}$ and a is a square in $\mathbb{Z}/p\mathbb{Z}$, then by Lemma 6, d is not a square and by Lemma 1, the addition is always defined. Since by Lemma 4 we have $\#E_{a,d,p} = p + 1$, then $(p + 1)(x, y) = (0, 1)$ for any point $(x, y) \in E_{a,d,p}$. If a is not a square, then d is a square and $(p + 1)(x, y)$ could not be defined on $E_{a,d,p}$. When $(p + 1)(x, y)$ is defined, then since $E_{a,d,p}$ is mapped to $W_{a,d,p}$ and $\#W_{a,d,p} = p + 1$, then $(p + 1)(x, y) = (0, 1)$. □

3 Twisted Edwards Curves over the Ring $\mathbb{Z}/p^r\mathbb{Z}$

In this section, we define the notion of Edwards curves over the ring $\mathbb{Z}/p^r\mathbb{Z}$ where $p \geq 5$ is a prime number and $r \geq 2$. We give an explicit estimation for the number of points on a twisted Edwards curve when $p \equiv 3 \pmod{4}$ and $p \equiv 11 \pmod{12}$.

Let $r \geq 2$ be an integer and p a prime number. Let a and d be integers. We consider the twisted Edwards curve E_{a,d,p^r} over the ring $\mathbb{Z}/p^r\mathbb{Z}$ with the equation

$$E_{a,d,p^r}: \ ax^2 + y^2 \equiv 1 + dx^2y^2 \pmod{p^r}.$$

Corollary 1. *Let $p > 2$ be a prime number and d be a positive integer such that d is not a square in $\mathbb{Z}/p\mathbb{Z}$. Let (x_1, y_1) and (x_2, y_2) be two points on E_{a,d,p^r}. If a is a square in $\mathbb{Z}/p\mathbb{Z}$, then the addition law*

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1y_1x_2y_2}, \frac{y_2y_1 - ax_2x_1}{1 - dx_1y_1x_2y_2} \right),$$

is always defined on E_{a,d,p^r}.

Proof. Suppose that $p > 2$ is a prime number. Let a be a square and d a non-square in $\mathbb{Z}/p\mathbb{Z}$. Let (x_1, y_1) and (x_2, y_2) be two points on the curve E_{a,d,p^r}. Set $\delta \equiv dx_1y_1x_2y_2 \pmod{p^r}$. Suppose that $\delta \equiv \pm 1 \pmod{p}$. Then by Theorem 1, d is a square in $\mathbb{Z}/p\mathbb{Z}$. This is a contradiction. □

Observe that if a is not a square in $\mathbb{Z}/p\mathbb{Z}$, the addition on E_{a,d,p^r} is not always defined as in the following example. Consider $p^r = 11^2$, $a = 7$, $d = 6$. Then a and d are not squares and $(2, 37)$ is a point on $E_{7,6,11^2}$. Nevertheless, $2(2, 37)$ is not possible since $\gcd(1 + dx_1^2y_1^2, p^r) = p$. Hence $\left(1 + dx_1^2y_1^2\right)^{-1} \pmod{p^r}$ does not exist.

Let $\#E_{a,d,p^r}$ denote the number of points (x, y) of the twisted Edwards curve E_{a,d,p^r}. We have the following result

Theorem 2. *Let $p \geq 3$ be a prime number and d an integer such that d is not a square in $\mathbb{Z}/p\mathbb{Z}$. Then*

$$\#E_{a,d,p^r} = p^{r-1}\#E_{a,d,p}.$$

Proof. Consider the polynomial $f(x, y) = ax^2 + y^2 - 1 - dx^2y^2$. Then $E_{a,d,p}$ is the set of zeros of $f(x, y)$. The derivative of $f(x, y)$ is

$$df(x, y) = \left(\frac{\partial f}{\partial x}(x, y), \frac{\partial f}{\partial y}(x, y) \right) = 2\left(x\left(a - dy^2\right), y\left(1 - dx^2\right)\right).$$

Hence, the singular points (x, y) of $E_{a,d,p}(K)$ are the points satisfying the system of equations

$$\begin{cases} x\left(a - dy^2\right) \equiv 0 \pmod{p}, \\ y\left(1 - dx^2\right) \equiv 0 \pmod{p}, \\ ax^2 + y^2 - 1 - dx^2y^2 \equiv 0 \pmod{p}. \end{cases}$$

Since d is not a square in $\mathbb{Z}/p\mathbb{Z}$, then the second equation implies that $y = 0$. Plugging in the first equation, we get $x = 0$ which contradicts the third equation. This implies that $E_{a,d,p}$ has no singular points. Thus, using the generalized Hensel Lemma (see [5]), to the polynomial $f(x, y)$, we deduce that $\#E_{a,d,p^r} = p^{r-1}\#E_{a,d,p}$. □

Combining Theorem 2 and Lemma 9, we get the following result.

Corollary 2. *Let $p \geq 5$ be a prime number. Let E_{a,d,p^r} be a twisted Edwards curve over the ring $\mathbb{Z}/p^r\mathbb{Z}$ with $ad(a-d) \not\equiv 0 \pmod{p}$. Then the number of points on $E_{a,d,p}$ is $\#E_{a,d,p^r} = p^{r-1}(p+1)$ if one of the following condition is fulfilled*

1. *$p \equiv 3 \pmod 4$, $\frac{a}{d} \equiv -1 \pmod p$, and a is a square,*
2. *$p \equiv 11 \pmod{12}$, $\frac{a}{d} \equiv -7 \pm 4\sqrt{3} \pmod p$, and a is a square.*

Next, combining Theorem 2 and Lemma 10, we get the following result.

Corollary 3. *Let E_{a,d,p^r} be a twisted Edwards curve. If p is a prime number with $p \equiv 3 \pmod 4$ and $\frac{a}{d} \equiv -1 \pmod{p^r}$, then for any point $(x,y) \in E_{a,d,p^r}$, we have*

$$p^{r-1}(p+1)(x,y) = \begin{cases} (0,1) & \text{if } a \text{ is a square in } \mathbb{Z}/p\mathbb{Z}, \\ (0,1) \text{or undefined} & \text{if } a \text{ is not a square in } \mathbb{Z}/p\mathbb{Z}. \end{cases}$$

Finally, combining Theorem 2 and Lemma 11, we get the following result.

Corollary 4. *Let E_{a,d,p^r} be a twisted Edwards curve with $\frac{a}{d} \equiv -7 \pm 4\sqrt{3} \pmod{p^r}$. If p is a prime number with $p \equiv 11 \pmod{12}$, then for any point $(x,y) \in E_{a,d,p^r}$, we have*

$$p^{r-1}(p+1)(x,y) = \begin{cases} (0,1) & \text{if } a \text{ is a square in } \mathbb{Z}/p\mathbb{Z}, \\ (0,1) \text{or undefined} & \text{if } a \text{ is not a square.} \end{cases}$$

4 Twisted Edwards Curves over the ring $\mathbb{Z}/n\mathbb{Z}$

In this section we define the twisted Edwards curve over the ring $\mathbb{Z}/n\mathbb{Z}$ where n is an odd composite number, specifically in the form $n = p^r q^s$. Let a and d be integers. We consider the twisted Edwards curve $E_{a,d,n}$ with the equation

$$E_{a,d,n} : \ ax^2 + y^2 \equiv 1 + dx^2y^2 \pmod n.$$

The following result states the possibility of adding two points on $E_{a,d,n}$.

Theorem 3. *Let $n > 2$ be an od integer and d a positive integer such that d is not a square in all the fields $\mathbb{Z}/p\mathbb{Z}$ where p is a prime factor of n. Let a be a square in $\mathbb{Z}/n\mathbb{Z}$. Let (x_1,y_1) and (x_2,y_2) be two points on E_{a,d,p^r}. Then the addition law*

$$(x_1,y_1) + (x_2,y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1y_1x_2y_2}, \frac{y_2y_1 - ax_2x_1}{1 - dx_1y_1x_2y_2} \right),$$

is always defined on $E_{a,d,n}$.

Proof. Let d be an integer such that d is not a square in all fields $\mathbb{Z}/p\mathbb{Z}$ where p is a prime factor of n. Let a be a square in $\mathbb{Z}/n\mathbb{Z}$. Let (x_1, y_1) and (x_2, y_2) be two points of the twisted Edwards curve $E_{a,d,n}$. Suppose that $1 \pm dx_1y_1x_2y_2$ is not invertible modulo n. Then there exists a prime factor p of n such that $1 \pm dx_1y_1x_2y_2 \equiv 0 \pmod{p}$. Hence, by applying Lemma 1, d is a square in $\mathbb{Z}/p\mathbb{Z}$, which is a contradiction. □

Observe that the condition that d is not a square in all the fields $\mathbb{Z}/p\mathbb{Z}$ where p is a prime factor of n is necessary condition. A typical counter-example holds for $n = 7 \cdot 13 \cdot 19$, $a = 4$ and $d = 183$. We can check that $(x_1, y_1) = (70, 335)$ and $(x_2, y_2) = (108, 525)$ are two points on the curve $E_{a,d,n}$ but the sum $(x_1, y_1) + (x_2, y_2)$ is not defined. Indeed we have

$$\gcd(1 + dx_1y_1x_2y_2 \pmod{n}, n) = \gcd(1352, 7 \cdot 13 \cdot 19) = 13,$$

and the inverse $(1 + dx_1y_1x_2y_2)^{-1} \pmod{n}$ does not exist. In this example, d is a square in the fields $\mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/13\mathbb{Z}$ but not in the field $\mathbb{Z}/19\mathbb{Z}$.

Combining the Chinese Remainder Theorem and Corollary 3, we get the following result that gives an explicit value for $\#E_{a,d,n}$ when $n = p^r q^s$ and p, q are distinct prime factors.

Corollary 5. *Let $p \geq 5$ and $q \geq 5$ be two distinct prime numbers. For $n = p^r q^s$, let $E_{a,d,n}$ be a twisted Edwards curve over the ring $\mathbb{Z}/n\mathbb{Z}$ with $ad(a-d) \not\equiv 0 \pmod{p}$ and $ad(a-d) \not\equiv 0 \pmod{q}$. Then the number of points on $E_{a,d,n}$ is $\#E_{a,d,n} = p^{r-1}q^{s-1}(p+1)(q+1)$ if one of the following condition is fulfilled*

1. *$p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$, $\frac{a}{d} \equiv -1 \pmod{n}$, and a is a square in $\mathbb{Z}/n\mathbb{Z}$,*
2. *$p \equiv 11 \pmod{12}$, $q \equiv 11 \pmod{12}$, $\frac{a}{d} \equiv -7 \pm 4\sqrt{3} \pmod{n}$, and a is a square in $\mathbb{Z}/n\mathbb{Z}$.*

Similarly, using the Chinese Remainder Theorem and Corollary 3, we get the following result.

Corollary 6. *Let $p \geq 5$ and $q \geq 5$ be prime numbers. For $n = p^r q^s$, let $E_{a,d,n}$ be a twisted Edwards curve. If $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$ and $\frac{a}{d} \equiv -1 \pmod{n}$, then for any point $(x, y) \in E_{a,d,n}$, we have*

$$p^{r-1}q^{s-1}(p+1)(q+1)(x,y) = \begin{cases} (0,1) & \text{if } a \text{ is a square in } \mathbb{Z}/n\mathbb{Z}, \\ (0,1) \text{ or undefined} & \text{if } a \text{ is not a square in } \mathbb{Z}/n\mathbb{Z}. \end{cases}$$

Finally, using the Chinese Remainder Theorem and Corollary 4, we get the following result.

Corollary 7. *Let $p \geq 5$ and $q \geq 5$ be prime numbers. For $n = p^r q^s$, let $E_{a,d,n}$ be a twisted Edwards curve with $\frac{a}{d} \equiv -7 \pm 4\sqrt{3} \pmod{n}$. If $p \equiv 11 \pmod{12}$ and $q \equiv 11 \pmod{12}$, then for any point $(x, y) \in E_{a,d,n}$, we have*

$$p^{r-1}q^{s-1}(p+1)(q+1)(x,y) = \begin{cases} (0,1) & \text{if } a \text{ is a square in } \mathbb{Z}/n\mathbb{Z}, \\ (0,1) \text{ or undefined} & \text{if } a \text{ is not a square in } \mathbb{Z}/n\mathbb{Z}. \end{cases}$$

5 The New Scheme

In [12], Koyama et al. introduced a variant of the RSA cryptosystem based on an RSA modulus $n = pq$ and an elliptic curve with equation $y^2 \equiv x^3 + b \pmod{n}$. This was recently extended by Boudabra and Nitaj [5] using a prime power modulus $n = p^r q^s$.

In this section, we give another extension of the KMOV system by using a twisted Edwards curve with an equation $ax^2 + y^2 \equiv 1 + dx^2y^2 \pmod{n}$ where $n = p^r q^s$ is a prime power modulus.

5.1 The new system

Key generation.

1. Choose two large primes p and q such that
   (a) $p \equiv 3 \pmod{4}$,
   (b) $p + 1 = 4u$ where u is a prime number,
   (c) $q \equiv 3 \pmod{4}$,
   (d) $q + 1 = 4v$ where v is a prime number,
2. Compute the modulus $n = p^r q^s$. The exponents r and s should be chosen according to Table 1
3. Choose an integer e coprime to $p^{r-1}(p+1)\,q^{s-1}(q+1)$. The pair (n, e) represents the public key.
4. Compute the secret key k satisfying $ke \equiv 1 \pmod{p^{r-1}(p+1)\,q^{s-1}(q+1)}$. In other words k is the inverse of $e \pmod{p^{r-1}(p+1)\,q^{s-1}(q+1)}$.

Encryption scheme. To encrypt a message M, we proceed as follows.

1. Transform M as $M = (x_M, y_M) \in (\mathbb{Z}/n\mathbb{Z})^2$ with $x_M \neq 0$ and $y_M \neq \pm 1$.
2. Compute
$$d \equiv \frac{y_M^2 - 1}{(y_M^2 + 1)\,x_M^2} \pmod{n}.$$
3. Compute $C = (x_C, y_C) = e(x_M, y_M)$ on the twisted Edwards curve $E_{-d,d,n}$ with the equation $-dx^2 + y^2 \equiv 1 + dx^2y^2 \pmod{n}$.
4. The ciphertext is $C = (x_C, y_C)$.

Decryption scheme. To decrypt, we proceed as follows.

1. Compute
$$d \equiv \frac{y_C^2 - 1}{(y_C^2 + 1)\,x_C^2} \pmod{n}.$$
2. Using the private key k, compute $M = (x_M, y_M) = k(x_C, y_C)$ on the twisted Edwards curve $E_{-d,d,n}$ with the equation $-dx^2 + y^2 \equiv 1 + dx^2y^2 \pmod{n}$.
3. The plaintext is $M = (x_C, y_C)$.

5.2 Correctness of the cryptosystem.

Since $ke \equiv 1 \pmod{p^{r-1}(p+1)q^{s-1}(q+1)}$, then there exists an integer λ such that $ke = 1 + \lambda p^{r-1}(p+1)\,q^{s-1}(q+1)$. Thus

$$\begin{aligned} k(x_C, y_C) &= ke(x_M, y_M) \\ &= \left(1 + \lambda p^{r-1}(p+1)q^{s-1}(q+1)\right)(x_M, y_M) \\ &= (x_M, y_M) + \lambda p^{r-1}(p+1)q^{s-1}(q+1)(x_M, y_M) \\ &= (x_M, y_M). \end{aligned}$$

Notice that if d is a square, then a is not a square and the scalar multiplication $C = (x_C, y_C) = e(x_M, y_M)$ can be not possible. As we will see, this scenario is negligible with an overwhelming probability.

5.3 A numerical example

As an example, consider the following prime numbers, the modulus and the public key

$$\begin{aligned} p &= 1654301903279, \\ q &= 3471055860911, \\ n &= p^2 q = 94992899017264031594779389052753871 51, \\ e &= 9829. \end{aligned}$$

The message is $M = (x_M, y_M)$ with

$$\begin{aligned} x_M &= 89849396786068261135545783141071083 14, \\ y_M &= 12160750074996134610886734058980761 88, \end{aligned}$$

Then, we get the coefficient d of the twisted Edwards curve

$$\begin{aligned} d &\equiv \frac{y_M^2 - 1}{(y_M^2 + 1)\,x_M^2} \equiv 94439904003086708787047291133628916 79 \pmod{n}, \\ k &\equiv e^{-1} \equiv 36261405749627914789175411017580429 89 \pmod{n}. \end{aligned}$$

For the encryption, we compute the ciphertext $(x_C, y_C) = e(x_M, y_M)$, and get

$$\begin{aligned} x_C &= 66625813533708478222463296061792787 81, \\ y_C &= 30369671944255282981349042693607972 04. \end{aligned}$$

To decrypt, we use the private key k and compute $(x_M, y_M) = k(x_C, y_C)$. Indeed, the computation gives

$$\begin{aligned} x_M &= 89849396786068261135545783141071083 14, \\ y_M &= 12160750074996134610886734058980761 88. \end{aligned}$$

This shows that the decryption is correct.

6 Efficiency and Security Analysis

In this section, we discuss the efficiency and the security of our proposed cryptosystem by studying the possibility of factoring of the modulus, impossible inversion, finding the order of the twisted Edwards curve $E_{-d,d,n}$, solving the discrete logarithm problem on $E_{-d,d,n}$ and solving the key equation

$$ek - u\left(p^{r-1}(p+1)q^{s-1}(q+1)\right) = 1.$$

6.1 Efficiency

There are many forms for representing points on an Edwards curve such as affine form, projective form and inverted form (see [3] for various representations and additions). For such forms, the addition law is suitably efficient for use in cryptography. For example, in the projective form, the twisted Edwards curve is represented by an equation with three variables

$$aX^2Z^2 + Y^2Z^2 = Z^4 + dX^2Y^2, \quad (X : Y : Z) \in \mathbb{P}^2,$$

where $\mathbb{P}^2$ is the projective space. In [2], it is shown that adding two points takes $10M + 1S + 1A + 1D$ operations with 10 multiplications, 1 squaring, 1 multiplication by a, and 1 multiplication by d. Doubling a point is also efficient as it takes only $3M + 4S + 1A$. As a consequence, the operations involved in our new schemes can be efficiently performed using a suitable representation of the twisted Edwards curve with affine equation $-dx^2 + y^2 \equiv 1 + dx^2y^2 \pmod{n}$.

6.2 Factoring the modulus

It is widely believed that factoring a modulus of the form $n = p^r q^s$ directly by existing algorithms is infeasible when p, q are large prime numbers and r, s satisfy the conditions of Table 1. The most powerful method are the Number Field Sieve [14] and the Elliptic Curve Method [13]. When p and q are large enough, such methods are ineffective.

6.3 Impossible inversion

In our scheme, the parameter d is computed using the original message (x_M, y_M) as

$$d \equiv \frac{y_M^2 - 1}{(y_M^2 + 1)\, x_M^2} \pmod{n}.$$

It might be a square in $\mathbb{Z}/n\mathbb{Z}$, and so we could face a non defined inversion in the ring $\mathbb{Z}/n\mathbb{Z}$ when $\gcd(n, 1 + dx_1y_1x_2y_2 \pmod{n}) \neq 1$ for some points $(x_1, y1)$, (x_2, y_2) on the twisted Edwards curve $E_{-d,d,n}$. This will lead to the factorisation of n as in the elliptic curve method for factorization [13]. This scenario is unlikely to happen for the following reasons.

– The elliptic curve method is inefficient when the prime factors p, q are sufficiently large and r, s are chosen according to Table 1.
– In $\mathbb{Z}/n\mathbb{Z}$, the number of terms of the form $1 \pm dx_1y_1x_2y_2 \pmod n$ satisfying $\gcd(n, 1 \pm dx_1y_1x_2y_2 \pmod n) \neq 1$ is at most $n - \phi(n)$ where $\phi(n) = p^{r-1}q^{s-1}(p-1)(q-1)$ is the Euler totient function. Hence, the probability that d is a square in $\mathbb{Z}/n\mathbb{Z}$ and $1 \pm dx_1y_1x_2y_2 \pmod n$ is not invertible modulo n is upper bounded by

$$\frac{n-\phi(n)}{n} = \frac{p^rq^s - p^{r-1}q^{s-1}(p-1)(q-1)}{p^rq^s} = \frac{p+q-1}{pq}. \tag{1}$$

Moreover, if p and q are of the same bit-size, then $p \approx q$, and we get the approximation $n = p^rq^s \approx p^{r+s} \approx q^{r+s}$, from which we deduce

$$p \approx q \approx n^{\frac{1}{r+s}}.$$

Hence, the probability (1) becomes

$$\frac{n-\phi(n)}{n} \approx \frac{2n^{\frac{1}{r+s}}}{n^{\frac{2}{r+s}}} = \frac{2}{n^{\frac{1}{r+s}}}.$$

This is a negligible probability when n is sufficiently large.

6.4 Finding the order of $E_{-d,d,n}$

Our new scheme uses a prime power RSA modulus of the form $n = p^rq^s$ where p and q are prime numbers satisfying $p \equiv q \equiv 3 \pmod 4$. By Corollary 7, for such primes, the order of the twisted elliptic curve $E_{-d,d,n}$ is $p^{r-1}q^{s-1}(p+1)(q+1)$. It follows that finding the order of $E_{-d,d,n}$ leads to factoring n. This can be done by computing

$$g = \gcd\left(n, p^{r-1}q^{s-1}(p+1)(q+1)\right) = p^{r-1}q^{s-1},$$

and

$$h = \frac{p^{r-1}q^{s-1}(p+1)(q+1)}{p^{r-1}q^{s-1}} = (p+1)(q+1).$$

Then combining the equations $h = (p+1)(q+1)$ and $p^rq^s = n$, one can find p and q. On the hand, it is obvious that factoring n leads immediately to finding the order of $E_{-d,d,n}$. As a consequence, finding the order of $E_{-d,d,n}$ is equivalent to factoring the modulus n. This situation is similar to the RSA modulus $N = pq$ for which finding the Euler totient function $\phi(N) = (p-1)(q-1)$ is computationally equivalent to factoring N.

6.5 Solving the discrete logarithm problem on $E_{-d,d,n}$

The security of the elliptic curve cryptography is based on the difficulty of solving the elliptic curve discrete logarithm: given two points P and Q on an elliptic curve

such that $Q = tP$, find t. In our scheme, the public equation is $C = (x_C, y_C) = eM = e(x_M, y_M)$ where the unknown is the point $M = (x_M, y_M)$ on the twisted Edwards curve $E_{-d,d,n}$. This is not vulnerable to the discrete logarithm attacks.

On the other hand, assume that an attacker knows a point P on $E_{-d,d,n}$ and a value u such that $C = uP$. Then M satisfies $M = vP$ for some unknown v. This gives $C = eM = evP$ and the problem transforms to finding $ev \pmod{p^{r-1}q^{s-1}(p+1)(q+1)}$. This is not possible under the hardness of elliptic discrete logarithm.

6.6 Solving the key equation

In our scheme, the publik key is e and the private key is k. They are related by the key equation is

$$ek - up^{r-1}q^{s-1}(p+1)(q+1) = 1,$$

in the unknown parameters k, u, p, q. This equation is similar to the key equations in some variants of RSA and could be solved by the continued fraction algorithm or by Coppersmith's method when k is suitably small (see [8,4,15,18]). To avoid small key attacks, it is preferable to use sufficiently large private key.

7 Conclusion

We have studied the arithmetical properties of the twisted Edwards curves on the finite field $\mathbb{Z}/p\mathbb{Z}$ and generalized them to the rings $\mathbb{Z}/p^r\mathbb{Z}$ and $\mathbb{Z}/p^rq^s\mathbb{Z}$. Using these properties, we have proposed a new public key scheme which can be seen as a generalization of two former public key schemes: the KMOV cryptosystem [12] with an RSA modulus and its generalization to a prime power RSA modulus [5].

References

1. Bernstein, D.J., Birkner, T.P., Joye, M., Lange, T., Peters, C.: Twisted Edwards curves. In: Vaudenay, S. (ed.), AFRICACRYPT 2008, Springer Lecture Notes in Computer Science, Springer **5023**, 389–405 (2008)
2. Bernstein, D.J., Lange, T.: Faster addition and doubling on elliptic curves. In: Kurosawa, K. (eds) Advances in Cryptology - ASIACRYPT 2007. ASIACRYPT 2007. Lecture Notes in Computer Science, **4833**. Springer, Berlin, Heidelberg, 29–50 (2007)
3. Bernstein, D. J., Lange, T.: Explicit-formulas database (2007). `http://hyperelliptic.org/EFD.Citationsinthisdocument`.
4. Boneh, D., Durfee, G., Howgrave-Graham, N.: Factoring $N = p^rq$ for large r. In: Wiener, M. (eds) Advances in Cryptology âĂŤ CRYPTOâĂŹ 99. CRYPTO 1999. Lecture Notes in Computer Science, **1666**. Springer, Berlin, Heidelberg, 326–337 (1999)
5. Boudabra, M., Nitaj, A.: A new generalization of the KMOV cryptosystem, Journal of Applied Mathematics and Computing, June 2018, **57**, Issue 1âĂŞ2, 229âĂŞ245 (2017)

6. Bressoud, D.M.: Factorization and Primality Testing, Undergraduate Texts in Mathematics, 1989th Edition, Springer-Verlag (1989)
7. Compaq Computer Corporation: Cryptography Using Compaq MultiPrime Technology in a Parallel Processing Environment (2000)
8. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities, Journal of Cryptology, **10**(4), 233–260 (1997)
9. Edwards, H.M.: A normal form for elliptic curves, Bulletin of the American Mathematical Society **44**, 393–422 (2007)
10. Fujioka, A., Okamoto, T., Miyaguchi, S: ESIGN: An efficient digital signature implementation for smard cards. EUROCRYPT 1991, Lecture Notes in Computer Science **547**, 446–457 (1991)
11. Ireland, K., Rosen M.: A Classical Introduction to Modern Number Theory, Springer-Verlag (1990)
12. K. Koyama, K., Maurer, U.M., Okamoto, T., Vanstone S. A.: New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$, Advances in Cryptology - CRYPTO'91, Lecture Notes in Computer Science, Springer-Verlag, 252–266 (1991)
13. Lenstra, H.: Factoring integers with elliptic curves, Annals of Mathematics, **126**, 649–673 (1987)
14. Lenstra, A.K., Lenstra, H.W. Jr. (eds.): The Development of the Number Field Sieve, Lecture Notes in Mathematics, **1554**, Berlin, Springer-Verlag (1993)
15. Nitaj, A., Rachidi, T.: New attacks on RSA with moduli $N = p^r q$. In: El Hajji S., Nitaj A., Carlet C., Souidi E. (eds) Codes, Cryptology, and Information Security. C2SI 2015. Lecture Notes in Computer Science, **9084**. Springer, Cham, 352–360 (2015)
16. Okamoto, T., Uchiyama, S.: A New public key cryptosystem as secure as factoring. EUROCRYPT 1998, Lecture Notes in Computer Science **1403**, 308–318 (1998)
17. Rivest, R., Shamir, A., Adleman, L.: A Method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, **21** (2), 120–126 (1978)
18. Sarkar, S.: Revisiting prime power RSA, Discrete Applied Mathematics, **203** Issue C, April 2016, 127–133 (2016)
19. Schmitt, S., Zimmer, H.G.: Elliptic Curves: A Computational Approach. Walter de Gruyter, Berlin (2003)
20. Takagi, T.: Fast RSA-type cryptosystem modulo $p^k q$. In: Krawczyk H. (eds) Advances in Cryptology - CRYPTO'98. CRYPTO 1998. Lecture Notes in Computer Science, vol 1462. Springer, Berlin, Heidelberg (1998)
21. Washington, L.C.: Elliptic Curves: Number Theory and Cryptography, Second Edition, CRC Press, Taylor & Francis Group (2008)

A Proof of Theorem 1

Let $p > 2$ be a prime number. Suppose that d is a non-square in $\mathbb{Z}/p\mathbb{Z}$ and a a square with $a \equiv b^2 \pmod{p}$. Let (x_1, y_1), (x_2, y_2) be two points on the curve $E_{a,d,p}$. Suppose that $dx_1y_1x_2y_2 \equiv \delta \equiv \pm 1 \pmod{p}$. Then $x_1y_1x_2y_2 \neq 0 \pmod{p}$ and

$$\begin{aligned} ax_1^2 + y_1^2 &\equiv dx_1^2y_1^2 + 1 \\ &\equiv dx_1^2y_1^2 + d^2x_1^2y_1^2x_2^2y_2^2 \pmod{p} \\ &\equiv dx_1^2y_1^2\left(1 + dx_2^2y_2^2\right) \pmod{p} \\ &\equiv dx_1^2y_1^2\left(ax_2^2 + y_2^2\right) \pmod{p}. \end{aligned}$$

Hence, since $\delta^2 \equiv 1 \pmod{p}$ and $ax_1^2 + y_1^2 \equiv dx_1^2y_1^2\left(ax_2^2 + y_2^2\right) \pmod{p}$, we get

$$\begin{aligned}(bx_1 + \delta y_1)^2 &= b^2x_1^2 + y_1^2 + 2b\delta x_1y_1 \\ &\equiv dx_1^2y_1^2\left(ax_2^2 + y_2^2\right) + 2bdx_1^2y_1^2x_2y_2 \pmod{p} \\ &\equiv dx_1^2y_1^2\left(b^2x_2^2 + y_2^2 + 2bx_2y_2\right) \pmod{p} \\ &\equiv dx_1^2y_1^2(bx_2 + y_2)^2 \pmod{p}.\end{aligned}$$

If $bx_2 + y_2 \not\equiv 0 \pmod{p}$, then, since $x_1y_1 \neq 0 \pmod{p}$, we have $\gcd(x_1y_1(bx_2 + y_2), p) = 1$, and

$$d \equiv \frac{(bx_1 + \delta y_1)^2}{x_1^2y_1^2(bx_2 + y_2)^2} \pmod{p},$$

is a square which is a contradiction. Similarly, we have

$$(bx_1 - \delta y_1)^2 \equiv dx_1^2y_1^2(bx_2 - y_2)^2 \pmod{p}.$$

If $bx_2 - y_2 \not\equiv 0 \pmod{p}$, then $\gcd(x_1y_1(bx_2 - y_2), p) = 1$, and

$$d \equiv \frac{(bx_1 - \delta y_1)^2}{x_1^2y_1^2(bx_2 - y_2)^2} \pmod{p},$$

is a square which is a contradiction. It follows that $bx_2 + y_2 \equiv 0 \pmod{p}$ and $bx_2 - y_2 \equiv 0 \pmod{p}$, from which we deduce $x_2 \equiv 0 \pmod{p}$ and $y_2 \equiv 0 \pmod{p}$. This is also a contradiction. As a consequence, we have always $\delta \not\equiv \pm 1 \pmod{p}$ and the denominators in the addition law never vanish. This terminates the proof.

B Proof of Lemma 2

Let (x, y) be a point on the curve $ax^2 + y^2 \equiv 1 + dx^2y^2 \pmod{p}$ with $ad(a-d) \neq 0$. If $x \neq 0$, then $y \neq \pm 1$ and

$$\frac{1 - y^2}{x^2} \equiv a - dy^2 \pmod{p}.$$

Since $d \neq a$ and $y \neq \pm 1$, then multiplying both sides by $\frac{4(1+y)}{(1-y)^3(a-d)}$, we get

$$\frac{4(1 + y)^2}{(1 - y)^2(a - d)x^2} \equiv \frac{4\left(a - dy^2\right)(1 + y)}{(1 - y)^3(a - d)} \pmod{p}.$$

Setting $Y \equiv \frac{2(1+y)}{(1-y)x} \pmod{p}$ and transforming the right side, we get

$$\frac{1}{a - d}Y^2 \equiv \frac{(1 + y)^3}{(1 - y)^3} + \frac{((a + 3d)y + 3a + d)(1 + y)}{(1 - y)^2(a - d)} \pmod{p}.$$

Setting $X \equiv \frac{1+y}{1-y} \pmod{p}$ and plugging it in the right side of the former equality, we get

$$\frac{1}{a - d}Y^2 \equiv X^3 + \frac{2(a + d)}{a - d}X^2 + X \pmod{p}.$$

Multiplying by $(a-d)^3$, we get

$$(a-d)^2Y^2 \equiv (a-d)^3X^3 + 2(a+d)(a-d)^2X^2 + (a-d)^3X \pmod{p}.$$

Setting $U \equiv (a-d)X \pmod{p}$ and $V \equiv (a-d)Y \pmod{p}$, this transforms to $V^2 = U^3 + 2(a+d)U^2 + (a-d)^2U \pmod{p}$ which can be rewritten as

$$V^2 \equiv \left(U + \frac{2(a+d)}{3}\right)^3 - \frac{4(a+d)^2}{3}U - \frac{8(a+d)^3}{27} + (a-d)^2U \pmod{p},$$

that is

$$V^2 \equiv \left(U + \frac{2(a+d)}{3}\right)^3 - \frac{a^2+14ad+d^2}{3}U - \frac{8(a+d)^3}{27} \pmod{p}.$$

Let $u \equiv U + \frac{2(a+d)}{3} \pmod{p}$ and $v \equiv V \pmod{p}$. Then using u and v, we get

$$v^2 \equiv u^3 - \frac{1}{3}\left(a^2+14ad+d^2\right)u - \frac{2}{27}(a+d)\left(a^2-34ad+d^2\right) \pmod{p}. \quad (2)$$

Summarizing the transformations, we get for $x \neq 0$,

$$u \equiv \frac{5a-d+(a-5d)y}{3(1-y)} \pmod{p}, \quad v \equiv \frac{2(a-d)(1+y)}{(1-y)x} \pmod{p}. \quad (3)$$

Now, if $x = 0$, then $y^2 = 1$ and $y = \pm 1$. If $y = 1$, then the transformations (3) are not valid and the point $(0,1)$ is transformed to the point at infinity $\mathcal{O}$. If $y = -1$, then $u \equiv \frac{2}{3}(a+d) \pmod{p}$. Plugging this in the equation (2), we get $v = 0$. Hence, the point $(0,-1)$ on $E_{a,d,p}$ is transformed to the point $\left(\frac{2}{3}(a+d), 0\right)$ on the equation (2). This terminates the proof.

C Proof of Lemma 3

Since $\mathcal{O}$ and $(0,1)$ are the neutral elements in $W_{a,d,p}$ and $E_{a,d,p}$ respectively, then they correspond to each other. For $u \neq \frac{5d-a}{3}$ and $v \neq 0$, we can invert (3) to get

$$(x,y) = \left(\frac{2(3u-2a-2d)}{3v}, \frac{3u-5a+d}{3u+a-5d}\right). \quad (4)$$

Observe that (4) is not defined for $v = 0$ and for $3u + a - 5d \equiv 0 \pmod{p}$.

First, for $v = 0$, suppose that $(u,0) \in W_{a,d,p}$. Then u satisfies the equation

$$\left(u - \frac{2(a+d)}{3}\right)\left(u + \frac{a+d+6\sqrt{ad}}{3}\right)\left(u + \frac{a+d-6\sqrt{ad}}{3}\right) \equiv 0 \pmod{p}. \quad (5)$$

The first root of (5) is $u = \frac{2}{3}(a+d)$. Plugging this in the second coordinate of (4), we get $y = -1$. Plugging $y = -1$ in the equation $ax^2 + y^2 = 1 + dx^2y^2$

of $E_{a,d,p}$, we get $ax^2 = dx^2$. Since $a \neq d$, then $x = 0$. Therefore the point $(\frac{2}{3}(a+d), 0) \in W_{a,d,p}$ is mapped to $(0,-1) \in E_{a,d,p}$.

In the case ad is a square in $\mathbb{Z}/p\mathbb{Z}$, then the second and third roots of (5) are $u = -\frac{1}{3}\left(a + d \pm 6\sqrt{ad}\right)$. Then the second coordinate of (4) is

$$y = \frac{3u - 5a + d}{3u + a - 5d} = \pm\sqrt{\frac{a}{d}}.$$

Plugging $y = \mp\sqrt{\frac{a}{d}}$ in the equation of $E_{a,d,p}$, we get $ax^2 + \frac{a}{d} = 1 + ax^2$ and $\frac{a}{d} = 1$. Since $a \neq d$, then this is impossible. Therefore the points $(u,v) = \left(-\frac{1}{3}\left(a + d \pm 6\sqrt{ad}\right), 0\right) \in W_{a,d,p}$ are not mapped in $E_{a,d,p}$.

Second, for $3u + a - 5d \equiv 0 \pmod 0$ we have $u \equiv -\frac{1}{3}(a - 5d) \pmod p$. Suppose that there exists v such that $(u,v) = \left(-\frac{1}{3}(a-5d), v\right) \in W_{a,d,p}$. Then v satisfies

$$v^2 \equiv 4d(a-d)^2 \pmod p.$$

Hence, if d is a square in $\mathbb{Z}/p\mathbb{Z}$, then $v \equiv \pm 2\sqrt{d}(a-d) \pmod p$. Plugging $(u,v) = \left(-\frac{1}{3}(a-5d), \pm 2\sqrt{d}(a-d)\right)$ in the first coordinate of (4), we get $x = \mp\frac{\sqrt{d}}{d}$. Plugging this in the equation of $W_{a,d,p}$, we get $\frac{a}{d} + y^2 = 1 + y^2$ and $\frac{a}{d} = 1$, which is impossible since $a \neq d$. Consequently, the points $(u,v) = \left(-\frac{1}{3}(a-5d), \pm 2\sqrt{d}(a-d)\right) \in W_{a,d,p}$ are not mapped on the twisted Edwards curve $E_{a,d,p}$.