Fast and Simple Point Operations on Edwards448 and E448

Luying Li[1,2], Wei Yu[2,3(✉)], and Peng Xu[1,4(✉)]

[1] JinYinHu Laboratory, Wuhan 430040, China
liluying@pku.org.cn
[2] State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, China
[3] Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
yuwei@iie.ac.cn, yuwei_1_yw@163.com
[4] Hubei Key Laboratory of Distributed System Security, School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074, China
xupeng@mail.hust.edu.cn

Abstract. Since Edwards curves were introduced in elliptic curve cryptography, they have attracted a lot of attention. The twisted Edwards curves are defined by the equation $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$. Twisted Edwards curve is the state-of-the-art for $a = -1$, and even for $a \neq -1$. E448 and Edwards448 are NIST standard curve in 2023 and TLS 1.3 standard curve in 2018. They both can be converted to $d = -1$, but can not be converted to $a = -1$ through isomorphism. The motivation of using a curve with $d = -1$ is that we want to improve the efficiency of E448, and Edwards448, especially to achieve a great saving in terms of the number of field multiplications (**M**) and field squarings (**S**). We propose new explicit formulas for point operations on these curves. Our full point addition only requires 8**M**, and mixed addition requires 7**M**. Our results applied on the Edward448 and E448 yield a clean and simple implementation and achieve a brand new speed record. The scalar multiplication on Edwards448 and E448 have the same cost of **M** and **S** as that on Edwards25519 per bit.

Keywords: Scalar multiplication · Addition · Doubling · Explicit formulas · Twisted Edwards curves · E448 · Edwards448

1 Introduction

Elliptic curve cryptography is one of the most popular cryptosystems. Because elliptic curve cryptography's shorter key length offers the same level of security as other public key cryptosystems with longer key lengths, it has been widely used in modern life since 2005. It is particularly well-liked in applications for mobile devices such as wireless and the internet of things.

The elliptic curves are the curves of genus one with a specified base point. In cryptography, the interest in elliptic curves is focused on their group structure.

Q. Tang and V. Teague (Eds.): PKC 2024, LNCS 14604, pp. 389–411, 2024.
https://doi.org/10.1007/978-3-031-57728-4_13

The points on the elliptic curve form an additive Abelian group. The scalar multiplication is an operation that continually adds the same point to itself repeatedly. In other words, scalar multiplication computes

$$nP = \underbrace{P + P + \cdots + P}_{n \text{ times}},$$

where n is a large positive integer known as the *scalar* and P is a point on an elliptic curve over the finite field. Elliptic curve cryptography is usually based on scalar multiplication on prime order cyclic subgroups of the elliptic curve point groups. Scalar multiplication is considered as the core operation in elliptic-curve cryptography. It is also the costliest part of some wildly used elliptic curve cryptography protocols, e.g. elliptic curve Diffie-Hellman key exchange and elliptic curve digital signature algorithm.

Compared to other elliptic curves, the Edwards curve in elliptic curve cryptography does not have such a long history. It was not until 2007 that this elliptic curve form was first explicitly proposed by Edwards [10]. In the same year, Bernstein and Lange introduced the Edwards curve into cryptography [3]. The importance of Edwards curves and their generalizations, especially the twisted Edwards curves, is beyond doubt. The twisted Edwards form is one of the three forms of curves recommended by NIST Special Publication 800-186 [7] over the finite field of large prime. The twisted Edwards curves Edwards25519 and Edwards448, also referred to as Ed25519 and Ed448, were recommended to be used in digital signature by NIST FIPS 186-5 [22], and Internet Engineering Task Force Request for Comments (IETF RFC) 8032 [19]; and were recommended to be employed in secure shell (SSH) protocol by IETF RFC 8709 [21]. The twisted Edwards curves are also employed in the Elliptic Curve Method (ECM) [2,6].

Ever since it was proposed, the scalar multiplication on the Edwards curve has become the leader in multi-scalar multiplication. Speeding up the scalar multiplications is one of the major challenges of elliptic curve cryptography. There are three main ways to improve the efficiency of scalar multiplication:

- Improving the point operations [18,25].
- Using efficient endomorphisms [13,14].
- Reducing the Hamming weight of the scalar, for example, non-adjacent form, window non-adjacent form, and double base chains [24].

In this paper, we investigate elliptic curve point arithmetic formulas on twisted Edwards curves for $d = -1$ to bridge the gap of previous works which focus on the general and $a = -1$ cases.

We provide two addition formulas on twisted Edwards curves in extended twisted Edwards coordinates. The *unified* addition formula, i.e., the point addition formula remains valid when two input points are equal, offers better side-channel resistance. The *unified* addition formula costs 8 field multiplications and one field multiplication with constant a, and the fast addition formula takes only 8 field multiplications, as fast as the addition formula for $a = -1$ on twisted Edwards curves [18].

The table below illustrates the state-of-the-art theoretical time costs of the unified addition, the mixed unified addition (where one coordinate is fixed as one in the unified addition formula), the fast addition ($P = Q$ may cause an exception), and the mixed addition of the fast addition. The **M**, **S**, and **D** denote field multiplication, field squaring, and field multiplication with a constant respectively (Table 1).

Table 1. The theoretical time cost of twisted Edwards curves

parameter	unified add	mixed unified add	fast add	mixed add
$a = -1$ [18]	$8\mathbf{M} + 1\mathbf{D}$	$7\mathbf{M} + 1\mathbf{D}$	$8\mathbf{M}$	$7\mathbf{M}$
$a \neq -1$ [18]	$9\mathbf{M} + 2\mathbf{D}$	$8\mathbf{M} + 2\mathbf{D}$	$9\mathbf{M} + 1\mathbf{D}$	$8\mathbf{M} + 1\mathbf{D}$
$d = -1$	$8\mathbf{M} + 1\mathbf{D}$	$7\mathbf{M} + 1\mathbf{D}$	$8\mathbf{M}$	$7\mathbf{M}$

The following problem is that the efficient doubling and tripling equations on $a = -1$ do not immediately yield good efficiency when $d = -1$. In order to solve this problem, we consider another set of projections of the extended twisted Edwards coordinates on $\mathbb{P}^2$ other than projective coordinates.

The remainder of this paper is organized as follows: in Sect. 2, we review twisted Edwards curves. Section 3 provides the unified addition formula. In Sect. 4, we provide the unified addition formulae with clearing denominators. In Sect. 5, we provide fast addition, doubling, and tripling formulae for further speedup. In Sect. 6, we analyze the exceptional cases of $2q$ and $4q$ order subgroups. In Sect. 7, we show the benefit of clearing denominators addition formulas in parallel environments and adapt the strategy of mixing different coordinates to obtain better efficiency for fast addition formulas. We draw our conclusions in Sect. 8.

2 Twisted Edwards Curve

The history of the Edwards curve family goes back to Euler's time. Euler studied an interesting curve $x^2 + y^2 + x^2y^2 = 1$. In his paper [11], Euler hinted at the explicit addition formula for this curve. Gauss explicitly stated this addition formula decades later.

In 2007, Edwards generalized the special curve $x^2 + y^2 + x^2y^2 = 1$ into the form

$$x^2 + y^2 = a^2 + a^2x^2y^2$$

and believed that this curve form deserves more attention than it had received at that time [10]. Edwards demonstrated that elliptic curves of this equation have the following addition law:

$$X = \frac{1}{a} \cdot \frac{xy' + yx'}{1 + xyx'y'}, \qquad Y = \frac{1}{a} \cdot \frac{yy' - xx'}{1 - xyx'y'}.$$

Edwards illustrated that it is a normal form of elliptic curves, i.e., every elliptic curve over algebraically closed field k is equivalent to $x^2 + y^2 = a^2 + a^2x^2y^2$ for some a. Thus, in a sense, this addition law can be employed for any elliptic curve.

Bernstein and Lange introduced this model and its addition law into elliptic curve cryptography, and proposed fast explicit formulas for addition, mixed addition, and doubling in projective coordinates [3]. Additionally, Bernstein and Lange expanded the addition law to a generalization form of the Edwards curve: $x^2 + y^2 = c^2(1 + dx^2y^2)$, and showed all the elliptic curves in the generalization form are isomorphic to curves $x^2 + y^2 = 1 + dx^2y^2$. When $c = 1$, they provided a $3\mathbf{M} + 4\mathbf{S}$ algorithm for the doubling formula and a $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ algorithm for the addition formula.

Bernstein and Lange later introduced inverted Edwards coordinates [4] to further lower down the cost of performing group operations on Edwards curves. The doubling costs $3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$, requires one more field multiplication with constant $2d$ when compared with [3]; and the addition costs $9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$, saving one field multiplication.

In order to cover more curves over finite fields, Bernstein, Birkner, Joye, Lange, and Peters generalized the Edwards curves into twisted Edwards curves with a new parameter a

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

A twisted Edwards curve with $a = 1$ is an Edwards curve. Each twisted Edwards curve $E_{a,d}$ is a quadratic twist of the Edwards curve $E_{1,d/a}$. Meanwhile, every quadratic twist of a twisted Edwards curve is isomorphic to a twisted Edwards curve. Scalar multiplications on twisted Edwards curves cost almost as much as they do on Edwards curves. More specifically, the doubling costs $3\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$ and the addition costs $9\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$. They proved that their addition law on the twisted Edwards curve is complete when a is a square and d is a non-square [1]. In addition, the twisted Edwards model can save time for many curves that were already expressible as Edwards curves by clearing denominators i.e. computing the scalar multiplication on $E_{a,d}$ rather than $E_{1,d/a}$. They also employ the clearing denominators technique in the curve $E_{1,d/a}$.

Hisil, Wong, Carter, and Dawson proposed extended twisted Edwards coordinates on the twisted Edwards curve to obtain a more efficient addition formula [18]. They found that there are four addition laws on twisted Edwards curves. They discovered that the twisted Edwards curves with $a = -1$ have an $8\mathbf{M}$ addition formula and $8\mathbf{M} + 1\mathbf{D}$ unified addition formula. The corresponding mixed addition formulae save one multiplication each. As a corresponding cost, the doubling formula in extended twisted Edwards coordinates required $4\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$, one multiplication slower than the doubling formula in projective coordinates. In order to solve this problem, Hisil et al. introduced a strategy of mixing different coordinates [18]. Therefore, the majority of the doubling could be computed in projective coordinates.

Bernstein and Lange studied the twisted Edwards curves as curves in $\mathbb{P}^1 \times \mathbb{P}^1$ [5]. They showed that the curve

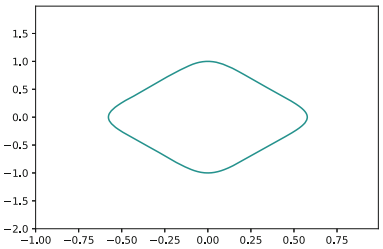
$$aX^2W^2 + Y^2Z^2 = Z^2W^2 + dX^2Y^2,$$

is nonsingular, where $(X : Z)$ and $(Y : W)$ are the representation of affine coordinates x and y in $\mathbb{P}^1$. They provided a set of two addition laws that can accept any pair of input points P_1, P_2 as input.

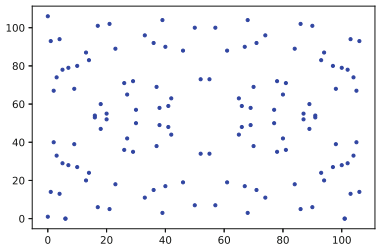
In [20], Kohel studied the symmetric model of twisted Edwards curves, including the extended twisted Edwards coordinates and $\mathbb{P}^1 \times \mathbb{P}^1$ model given by Bernstein and Lange. Kohel showed that a twisted Edwards curve using the extended twisted Edwards coordinates can be seen as the curve on $\mathbb{P}^3$, i.e., the curve is

$$E : dT^2 + Z^2 = aX^2 + Y^2, \qquad ZT = XY.$$

Kohel showed that the twisted Edwards curve on $\mathbb{P}^3$ can be regarded as the intersection of two symmetric surfaces. It follows that parameter d should have properties as parameter a, which inspired us to look for efficient point operations for special d. Meanwhile, when a is a non-square and d is a square, Kohel implied another complete addition law.



(a) Twisted Edwards curve $3x^2 + y^2 = 1 - 11x^2y^2$



(b) Rational points on twisted Edwards curve $3x^2 + y^2 = 1 - 11x^2y^2$ over finite field $\mathbb{F}_{107}$

2.1 Ed448 and E448

The most famous curves in the twisted Edwards curves are the Edwards25519 (Ed25519), Edwards448 (Ed448), and E448. The curve Edwards25519 is a twisted Edwards curve that is isomorphic to the Montgomery curve Curve25519. The curve Edwards448 is designed by Hamburg [16] and has been favored by the Internet Research Task Force Crypto Forum Research Group (IETF CFRG) ever since. The curve E448 is a twisted Edwards curve. It is birationally equivalent to the Montgomery curve Curve448, and is 4-isogenous to the curve Edwards448.

The curve Edwards25519 has parameter $a = -1$, Edwards448 and E448 have parameter $a = 1$ instead of $a = -1$. In the following paragraphs, we will describe how to convert Edwards448 and E448 to the relative curves with $d = -1$.

Let $E_{a,d}$ be a twisted Edwards curve. If there exists an element c in the finite field that satisfies $d = -c^2$, in other words, $-d$ is a square in the finite field, then there is an isomorphism between $E_{a,d}$ and the following curve:

$$E_{-a/d,-1} : -\frac{a}{d}x^2 + y^2 = 1 - x^2y^2.$$

The map from $E_{a,d}$ to $E_{-a/d,-1}$ is given by $(x, y) \mapsto (cx, y)$.

The parameters d in both Edwards448 and E448 satisfy the condition that $-d$ is a square in the finite field. Thus, they are isomorphic to $E_{-a/d,-1}$. The isomorphism between $E_{a,d}$ and $E_{-a/d,-1}$ allow us to use the curve $E_{-a/d,-1}$ to compute the scalar multiplication rather than $E_{a,d}$. More specifically, the parameters for Edwards448 are given as follows:

$$\begin{aligned} p &= 2^{448} - 2^{224} - 1, \\ a &= 1, \\ d &= -39081. \end{aligned}$$

It satisfies $-d = 39081$ is a square in $\mathbb{F}_p$. One of the square roots of $-d$ is

$$\begin{aligned} c = \sqrt{-d} = 0x22d962fbeb24f7683bf68d722fa26aa0a1f1a7b8a5b8d54b64a2d78\backslash \\ 0968c14ba839a66f4fd6eded260337bf6aa20ce529642ef0f45572736. \end{aligned}$$

And the parameters for E448 are given as follows:

$$\begin{aligned} p &= 2^{448} - 2^{224} - 1, \\ a &= 1, \\ d &= 39082/39081, \end{aligned}$$

The curve E448 satisfies $-d = -39082/39081$ is a square in $\mathbb{F}_p$. One of the square roots of $-d$ is

$$\begin{aligned} c = \sqrt{-d} = 0x54457070fb7967d346710750c9f632c2792bd08a0d9bc3791700015\backslash \\ fcada1acc74ce0dd46445d2d8b81c730cd43d844a7e20c44e4b9a266c. \end{aligned}$$

2.2 Affine Addition and Doubling Laws on Twisted Edwards Curves

We recalled the addition laws given by Hisil, Wong, Carter, and Dawson [18]. Let (x_3, y_3) be the point $(x_1, y_1) + (x_2, y_2)$. x_3 has two representations:

$$\mathfrak{x}_0 = \frac{x_2y_1 + x_1y_2}{1 + dx_1x_2y_1y_2} \qquad \text{and} \qquad \mathfrak{x}_1 = \frac{x_1y_1 + x_2y_2}{y_1y_2 + ax_1x_2},$$

y_3 has two representations, too:

$$\mathfrak{y}_0 = \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \qquad \text{and} \qquad \mathfrak{y}_1 = \frac{x_1y_1 - x_2y_2}{x_1y_2 - x_2y_1}.$$

Thus, there are four different affine addition laws for twisted Edwards curves. They are respectively presented as follows:

$$(x_3, y_3) = (x_1, y_1)+(x_2, y_2) = \left(\frac{x_2y_1 + x_1y_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right) = (\mathfrak{x}_0, \mathfrak{y}_0), \quad (1)$$

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2) = \left(\frac{x_2y_1 + x_1y_2}{1 + dx_1x_2y_1y_2}, \frac{x_1y_1 - x_2y_2}{x_1y_2 - x_2y_1}\right) = (\mathfrak{x}_0, \mathfrak{y}_1), \quad (2)$$

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_1 + x_2y_2}{y_1y_2 + ax_1x_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right) = (\mathfrak{x}_1, \mathfrak{y}_0), \quad (3)$$

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_1 + x_2y_2}{y_1y_2 + ax_1x_2}, \frac{x_1y_1 - x_2y_2}{x_1y_2 - x_2y_1}\right) = (\mathfrak{x}_1, \mathfrak{y}_1). \quad (4)$$

The point $(0, 1)$ on $E_{a,d}$ is the identity element and $(0, -1)$ is a point of order 2. The negative of a point (x, y) is $(-x, y)$.

The addition law (1) is the first one found on twisted Edwards curves which was proposed by Bernstein, Birkner, Joey, Lange, and Peters in [1]. They pointed out that when a is a square and d is not a square, this addition law is complete. In [18], Hisil et al. studied the addition law (1) and (4) in detail.

In this paper, we study the addition laws (2) and (3). Since the expression of the addition law (2) is independent of a, (2) can perform efficiently even if a is large. The addition law (3) is another complete addition law implied by Kohel [20] and explicitly stated by Farashahi and Hosseini [12]. This addition law is complete if and only if d is a square and a is a nonsquare. But when the finite field $\mathbb{F}_p$ satisfies $p \equiv 3 \pmod 4$, $d = -1$ is a nonsquare. Thus, this addition law on Edwards448 is not complete. Later in Sect. 3, we will show this addition formula is unified when $d = -1$ is a nonsquare and a is a square.

Similar to (4), the addition law (2) has some exceptional cases even if a and d are carefully selected.

The following lemmas show that the exceptional cases would not occur when the scalar multiplication performs on the odd order subgroup.

Lemma 1 (Lemma 2 in [23]). *Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ be a pair of non-trivial exceptional points ($P \neq \pm Q$ and P, Q are points of odd prime order) on $E_{a,d}$. Then the following holds:*

$$\begin{aligned} x_1x_2y_1y_2 &\neq 0, \\ dx_1x_2y_1y_2 \pm 1 &\neq 0, \\ ax_1x_2 \pm y_1y_2 &\neq 0, \\ x_1y_2 \pm x_2y_1 &\neq 0, \\ x_1y_1 \pm x_2y_2 &\neq 0. \end{aligned}$$

Lemma 1 shows that when the elliptic curve scalar multiplication is performed on the subgroup of points of prime order, the addition law (3) and (2) are exception-free for distinct input points. By [1], the doubling law is

$$2(x_1, y_1) = \left(\frac{2x_1y_1}{1 + dx_1^2y_1^2}, \frac{y_1^2 - ax_1^2}{1 - dx_1^2y_1^2}\right) = (x_3, y_3). \quad (5)$$

2.3 Extended Twisted Edwards Coordinates

Recall the homogenous projective equation for twisted Edwards curves:

$$(aX^2 + Y^2)Z^2 = Z^4 + dX^2Y^2.$$

Hisil et al. introduced an auxiliary coordinate $T = XY/Z$ to represent a point (x, y) on twisted Edwards curves [18]. For all nonzero $\lambda \in K$, $(T : X : Y : Z) = (\lambda T : \lambda X : \lambda Y : \lambda Z)$ represents the affine point $(x, y) = (X/Z, Y/Z)$ in affine coordinates. Following the notation in [18], $\mathcal{E}^e$ was employed to denote the extended twisted Edwards coordinates.

However, under this definition, the points $(0 : 1 : 0)$ and $(1 : 0 : 0)$ will be invalid when they are extended to points in extended twisted Edwards coordinates. This problem can be fixed by another model of extended twisted Edwards coordinates proposed by Kohel [20]. Recall that Kohel revisited the twisted Edwards curve with the extended twisted Edwards coordinates by the projective closure.

$$Z^2 + dT^2 = aX^2 + Y^2, \qquad ZT = XY.$$

In this model, the twisted Edwards curve was considered as the intersection of two surfaces in $\mathbb{P}^3$.

The points $(0 : 1 : 0)$ and $(1 : 0 : 0)$ can be extended to $(\pm 1/\sqrt{d} : 0 : 1 : 0)$ and $(\pm\sqrt{a/d} : 1 : 0 : 0)$.

Specifically, in an algebraically closed field $\bar{k}$, each twisted Edwards curve has eight points that contain zero value coordinates. There are four points of order 4: $(\pm 1/\sqrt{d} : 0 : 1 : 0)$, $(0 : 1 : 0 : \pm\sqrt{a})$; three points of order 2: $(\pm\sqrt{a}/\sqrt{d} : 1 : 0 : 0)$ and $(0 : 0 : -1 : 1)$, and an identity point $(0 : 0 : 1 : 1)$. The point $(0 : 0 : 0 : 0)$ satisfies the equation in $\mathbb{P}^3$ but not satisfies that in $\mathbb{P}^2$. It should be ignored.

3 Unified Addition in $\mathcal{E}^e$ for $d = -1$

To prevent the protocols from simple power analysis, unified addition formulae are more favorable [23]. Let K be a finite field of odd characteristic. This section proposes a unified addition formula for $d = -1$ on the prime order subgroup of twisted Edwards curves over K.

3.1 The Unified Addition Law

The addition formulas are designed for $d = -1$ to obtain the speeding up on Edwards448, E448, and other twisted Edwards curves that satisfy $-d$ is a square. For the state-of-the-art formulas for other situations, please refer to [18].

In the following, we recall the addition law (3)

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_1 + x_2y_2}{y_1y_2 + ax_1x_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right).$$

When a is a non-square and d is a square, this addition law has been proved as a complete addition law [12,20]. In the following parts, we will demonstrate that this formula is unified on the prime order subgroup for arbitrary a and d.

Lemma 2. *Let K be a finite field of odd characteristic. Let $E_{a,d}$ be a twisted Edwards curve defined over K. Let $P = (x_1, y_1)$ be a fixed point on $E_{a,d}$ and $Q = (x_2, y_2)$ be another point on $E_{a,d}$.*

- $1 - dx_1x_2y_1y_2 = 0$ *if and only if*

$$Q \in S_{P,1} = \left\{ \left(\frac{-1}{\sqrt{d}y_1}, \frac{-1}{\sqrt{d}x_1} \right), \left(\frac{1}{\sqrt{d}y_1}, \frac{1}{\sqrt{d}x_1} \right), \left(\frac{-1}{\sqrt{ad}x_1}, \frac{-\sqrt{a}}{y_1\sqrt{d}} \right), \left(\frac{1}{\sqrt{ad}x_1}, \frac{\sqrt{a}}{y_1\sqrt{d}} \right) \right\}$$

  and $Q \in K^2$ is well-defined.
- $y_1y_2 + ax_1x_2 = 0$ *if and only if*

$$Q \in S_{P,2} = \left\{ \left(\frac{y_1}{\sqrt{a}}, -\sqrt{a}x_1 \right), \left(\frac{-y_1}{\sqrt{a}}, \sqrt{a}x_1 \right), \left(\frac{-1}{\sqrt{ad}x_1}, \frac{\sqrt{a}}{y_1\sqrt{d}} \right), \left(\frac{1}{\sqrt{ad}x_1}, \frac{-\sqrt{a}}{y_1\sqrt{d}} \right) \right\}$$

  and $Q \in K^2$ is well-defined.

Proof. Since P and Q are points on $E_{a,d}$, x_1, y_1, x_2, and y_2 satisfy the equations $ax_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ and $ax_2^2 + y_2^2 = 1 + dx_2^2y_2^2$. If $1 - dx_1x_2y_1y_2 = 0$ (resp. $y_1y_2 + ax_1x_2 = 0$), then combining these functions we have $Q \in S_{P,1}$ (resp. $Q \in S_{P,2}$).

Corollary 1. *Any points P and Q of odd order q would not induce the exceptional cases of the addition law (3). (3) is a unified addition law on prime order subgroup.*

Proof. If both P and Q are points of odd prime order q, then $P \pm Q$ are either 0 or of odd prime order too. Let $S_{1,P}$ and $S_{2,P}$ be defined as in Lemma 2. Then for any point P and point $Q \in S_{1,P} \bigcup S_{2,P}$, it can be computed that one of $Q + P$ and $Q - P$ is a point of order two or order four (in the extension of K where they exist). In contrast to earlier assumptions.

The projective form of it can be obtained as

$$\begin{aligned}(x_3, y_3) &= (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) \\ &= \left(\frac{X_1Y_1Z_2^2 + X_2Y_2Z_1^2}{(Y_1Y_2 + aX_1X_2)Z_1Z_2}, \frac{(Y_1Y_2 - aX_1X_2)Z_1Z_2}{Z_1^2Z_2^2 - dX_1X_2Y_1Y_2} \right).\end{aligned}$$

When $Z_1Z_2 \neq 0$, the addition law can be rewritten in extended twisted Edwards coordinates as

$$\begin{aligned}(x_3, y_3) &= (T_1 : X_1 : Y_1 : Z_1) + (T_2 : X_2 : Y_2 : Z_2) \\ &= \left(\frac{\frac{X_1Y_1}{Z_1}Z_2 + \frac{X_2Y_2}{Z_2}Z_1}{Y_1Y_2 + aX_1X_2}, \frac{Y_1Y_2 - aX_1X_2}{Z_1Z_2 - d\frac{X_1Y_1}{Z_1}\frac{X_2Y_2}{Z_2}} \right).\end{aligned}$$

When $Z_i \neq 0$, we have $T_i = X_i Y_i / Z_i$. It turns to be

$$\begin{aligned}(x_3, y_3) &= (T_1 : X_1 : Y_1 : Z_1) + (T_2 : X_2 : Y_2 : Z_2) \\ &= \left(\frac{T_1 Z_2 + T_2 Z_1}{Y_1 Y_2 + a X_1 X_2}, \frac{Y_1 Y_2 - a X_1 X_2}{Z_1 Z_2 - d T_1 T_2} \right).\end{aligned}$$

All the points on twisted Edwards curves satisfying the Z-coordinates of it is zero have even order. In particular, for Edwards448 and E448, there are no points that have coordinate $Z = 0$ in $\mathcal{E}^e$ or $\mathcal{E}$. According to Lemma 1, when P and Q is a pair of non-trivial exceptional points on $E_{a,d}$, we have $T_1 Z_2 + T_2 Z_1 \neq 0$, $Y_1 Y_2 + a X_1 X_2 \neq 0$, $Y_1 Y_2 - a X_1 X_2 \neq 0$, and $Z_1 Z_2 - d T_1 T_2 \neq 0$. When $P = Q$ and P, Q have odd prime order, according to Corollary 1, the exceptional cases also would not happen when $Z_1 Z_2 \neq 0$.

Then the unified addition formulae with $d = -1$ on extended twisted Edwards coordinates can be obtained as follows. Given two points $(T_1 : X_1 : Y_1 : Z_1)$ and $(T_2 : X_2 : Y_2 : Z_2)$ with $Z_1 Z_2 \neq 0$, the point addition on $E_{a,-1}$ can be performed as $(T_1 : X_1 : Y_1 : Z_1) + (T_2 : X_2 : Y_2 : Z_2) = (T_3 : X_3 : Y_3 : Z_3)$, where

$$\begin{aligned}T_3 &= (T_1 Z_2 + T_2 Z_1)(Y_1 Y_2 - a X_1 X_2), \\ X_3 &= (T_1 Z_2 + T_2 Z_1)(Z_1 Z_2 + T_1 T_2), \\ Y_3 &= (Y_1 Y_2 + a X_1 X_2)(Y_1 Y_2 - a X_1 X_2), \\ Z_3 &= (Y_1 Y_2 + a X_1 X_2)(Z_1 Z_2 + T_1 T_2).\end{aligned} \tag{6}$$

3.2 The Unified Addition Formula

The addition formula can be performed with a $8\mathbf{M} + 1\mathbf{D}$ algorithm given by

$$\begin{gathered}m_1 \leftarrow 2Y_1 \cdot Y_2, \quad m_2 \leftarrow 2X_1 \cdot X_2, m_3 \leftarrow (T_1 + Z_1) \cdot (T_2 + Z_2), \\ m_4 \leftarrow (T_1 - Z_1) \cdot (T_2 - Z_2), \quad d_1 = a \cdot m_2, \quad a_1 = m_1 + d_1,\end{gathered}$$

$$\begin{gathered}a_2 = m_1 - d_1, \quad a_3 = m_3 + m_4, \quad a_4 = m_3 - m_4, \\ X_3 = a_3 \cdot a_4, \quad Y_3 = a_1 \cdot a_2, \quad Z_3 = a_1 \cdot a_3, \quad T_3 = a_2 \cdot a_4.\end{gathered}$$

The $\mathbf{D}$ in this algorithm is a field multiplication with the constant value a.

A $7\mathbf{M} + 1\mathbf{D}$ mixed addition algorithm can be derived by setting $X_2 = 1$ or $Y_2 = 1$. If one of the input points is fixed, for example, assuming $(X_2 : Y_2 : T_2 : Z_2)$ is fixed, then the multiplication m_2 and the multiplication with constant d_1 can be combined in a single multiplication $2aX_2 \cdot X_1$ if $2a \cdot X_2$ is pre-computed. Then the cost of the addition becomes $8\mathbf{M}$ and the cost of the mixed addition becomes $7\mathbf{M}$. Since $1/39081$ is a large number in the finite field of Edwards448, this pre-computation is recommended when the formula is employed to compute the scalar multiplication on Edwards448.

Since this addition formula is unified on the prime order subgroup, it can be employed in protocols that require SPA protection.

4 Clearing Denominators and Scalar Multiplication in Parallel Environments

When Bernstein et al. [1] introduced the twisted Edwards curves, they used the clearing denominators technique to speed up the scalar multiplication of the Edwards curves

$$x^2 + y^2 = 1 + dx^2y^2$$

with parameters $d = \bar{d}/\bar{a}$, where $\bar{d}$ and $\bar{a}$ are small in K and $\bar{d}/\bar{a}$ is large. In projective coordinates, they proposed $10\mathbf{M} + 1\mathbf{S} + 3\mathbf{D}$ clearing denominators addition formula, where the $3\mathbf{D}$ are two multiplications by $\bar{a}$ and one by $\bar{d}$. As a comparison, the previous addition formula costs $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$, where the $\mathbf{D}$ is one multiplication by d. In inverted projective coordinates, they proposed $9\mathbf{M} + 1\mathbf{S} + 3\mathbf{D}$ clearing denominators addition formula, where the $3\mathbf{D}$ are two multiplications by $\bar{a}$ and one by $\bar{d}$. As a comparison, the previous addition formula costs $9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$, where the $\mathbf{D}$ is one by d.

In the implementations, the ratio $\mathbf{D}/\mathbf{M}$ varies for different constants, different libraries, and different implement environments. For example, the multiplication with 10, and the multiplication with $1/10$ are both denoted by $\mathbf{D}$, but in the former case, the ratio $\mathbf{D}/\mathbf{M}$ may close to 0, while in the latter case, this ratio may close to 1. When d and a are small in K, several field multiplications with a and d might be faster than one field multiplication with d/a.

Later in Sect. 7, we will show that clearing denominators formulae in particular suit the parallel environments.

4.1 Clearing Denominators for $d = -1$

For a twisted Edwards curve $E_{\bar{a}/\bar{d},-1}$, the addition formula can also be performed with a $8\mathbf{M} + 4\mathbf{D}$ algorithm given by

$$\begin{gathered}
m_1 \leftarrow Y_1 \cdot Y_2, \quad m_2 \leftarrow X_1 \cdot X_2, \quad m_3 \leftarrow (T_1 + Z_1) \cdot (T_2 + Z_2), \\
m_4 \leftarrow (T_1 - Z_1) \cdot (T_2 - Z_2), \quad d_1 = 2\bar{d} \cdot m_1, \quad d_2 = 2\bar{a} \cdot m_2, \\
d_3 = \bar{d} \cdot m_3, \quad d_4 = \bar{d} \cdot m_4, \quad a_1 = d_1 + d_2, \\
a_2 = d_1 - d_2, \quad a_3 = d_3 + d_4, \quad a_4 = d_3 - d_4, \\
X_3 = a_3 \cdot a_4, \quad Y_3 = a_1 \cdot a_2, \quad Z_3 = a_1 \cdot a_3, \quad T_3 = a_2 \cdot a_4.
\end{gathered}$$

The $4\mathbf{D}$ in this algorithm is a field multiplication with the constant $2\bar{a}$, a field multiplication with the constant $2\bar{d}$, and two field multiplications with the constant $\bar{d}$.

4.2 Clearing Denominators for $a = -1$

For a twisted Edwards curve $E_{-1,\bar{d}/\bar{a}}$, the addition formula can also be performed with a $8\mathbf{M} + 4\mathbf{D}$ algorithm given by

$$\begin{gathered}
m_1 \leftarrow (Y_1 - X_1) \cdot (Y_2 - X_2), \quad m_2 \leftarrow (Y_1 + X_1) \cdot (Y_2 + X_2), \\
m_3 \leftarrow T_1 \cdot T_2, \quad m_4 \leftarrow Z_1 \cdot Z_2, \quad d_1 = \bar{a} \cdot m_1, \quad d_2 = \bar{a} \cdot m_2,
\end{gathered}$$

$$d_3 = 2\bar{d} \cdot m_3, \quad d_4 = 2\bar{a} \cdot m_4,$$
$$a_1 = d_2 - d_1, \quad a_2 = d_4 - d_3, \quad a_3 = d_3 + d_4, \quad a_4 = d_1 + d_2,$$
$$X_3 = a_1 \cdot a_2, \quad Y_3 = a_3 \cdot a_4, \quad Z_3 = a_1 \cdot a_4, \quad T_3 = a_2 \cdot a_3.$$

The 4**D** in this algorithm is a field multiplication with the constant $2\bar{a}$, a field multiplication with the constant $2\bar{d}$, and two field multiplications with the constant $\bar{a}$.

5 Fast Formulae in $\mathcal{E}^e$

This section shows the fast addition, doubling, and tripling formulae on twisted Edwards curves with $d = -1$. The doubling and tripling in $\mathcal{E}^e$ are doubling and tripling from $\mathcal{E}$ to $\mathcal{E}^e$. In general, only one of the parameters a and d can be set as very tiny. Since the existing doubling, addition, and tripling formulas on the twisted Edwards curves all focus on the smaller a, they cannot achieve good efficiency for the case where d is smaller and a is larger. In this paper, we proposed new addition, doubling, and tripling formulas for this situation.

5.1 Fast Addition in $\mathcal{E}^e$ for $d = -1$

Similar to the unified addition formulae, the fast addition formulae can be obtained as follows. Given two points $(T_1 : X_1 : Y_1 : Z_1)$ and $(T_2 : X_2 : Y_2 : Z_2)$ with $Z_1 Z_2 \neq 0$, the point addition can be performed as $(T_1 : X_1 : Y_1 : Z_1) + (T_2 : X_2 : Y_2 : Z_2) = (T_3 : X_3 : Y_3 : Z_3)$, where

$$\begin{aligned} T_3 &= (X_2 Y_1 + X_1 Y_2)(T_1 Z_2 - T_2 Z_1) \\ X_3 &= (X_2 Y_1 + X_1 Y_2)(X_1 Y_2 - X_2 Y_1) \\ Y_3 &= (T_1 Z_2 - T_2 Z_1)(Z_1 Z_2 + d T_1 T_2) \\ Z_3 &= (X_1 Y_2 - X_2 Y_1)(Z_1 Z_2 + d T_1 T_2) \end{aligned}. \tag{7}$$

When $d = -1$, the addition formula can be performed with a 8**M** algorithm given by

$$m_1 \leftarrow 2X_1 \cdot Y_2, \quad m_2 \leftarrow 2X_2 \cdot Y_1, \quad m_3 \leftarrow (T_1 + Z_1) \cdot (-T_2 + Z_2),$$
$$m_4 \leftarrow (-T_1 + Z_1) \cdot (T_2 + Z_2), \quad a_1 = m_1 + m_2, \quad a_2 = m_1 - m_2,$$
$$a_3 = m_3 + m_4, \quad a_4 = m_3 - m_4,$$
$$X_3 = a_1 \cdot a_2, \quad Y_3 = a_3 \cdot a_4, \quad Z_3 = a_2 \cdot a_3, \quad T_3 = a_1 \cdot a_4.$$

A 7**M** mixed addition algorithm can be derived by setting $X_2 = 1$ or $Y_2 = 1$.

5.2 Modified Projective Coordinates $\mathcal{E}$

As we mentioned in Sect. 1, only one of the parameters a and d can reasonably be assumed to be very small. All the efficient doubling and tripling point formulae are based on the case where a is very small. Meanwhile, the doubling and tripling formulae on projective coordinates are more efficient than those on extended twisted Edwards coordinates.

This section introduces new modified projective coordinates to obtain the efficient doubling and tripling point formulae. All these formulae are as efficient as the existing projective formulae on twisted Edwards curves.

Recall that the extended twisted Edwards coordinates have four components: X, Y, Z, and T. Since $ZT = XY$, every three components can determine the value of the remaining ones. The modified projective coordinates are a projection of extended Edwards coordinates on $\mathbb{P}^2$, denoted by $\mathcal{E}$. It employs the components T, Y, and Z. Then the affine coordinates (x, y) can be recovered as $(x, y) = (\frac{T}{Y}, \frac{Y}{Z})$ by a point $(Y : T : Z)$ in $\mathcal{E}$. This representation is invalid if it represents the point at infinity or y-coordinate in affine form satisfies $y = 0$, which follows that $(x, y) = (\pm 1/\sqrt{a}, 0)$. By [1], $(\pm 1/\sqrt{a}, 0)$ and points at infinity are points of even order, would not appear in prime order subgroup scalar multiplication.

Given $(T : Y : Z)$ in $\mathcal{E}$ passing to $\mathcal{E}^e$ requires $3\mathbf{M} + 1\mathbf{S}$ by computing (TY, TZ, Y^2, YZ). Given $(T : X : Y : Z)$ in $\mathcal{E}^e$ passing to $\mathcal{E}$ is cost-free by simply ignoring X.

5.3 Doubling in $\mathcal{E}^e$

For any point $(T_1 : X_1 : Y_1 : Z_1)$ on the twisted Edwards curves, we have

$$aX_1^2 + Y_1^2 = Z_1^2 + dT_1^2, \quad Z_1T_1 = X_1Y_1.$$

As a result, the doubling formula (5) can be rewritten as

$$(x_3, y_3) = 2(x_1, y_1) = \left(\frac{2X_1Y_1}{Z_1^2 + dT_1^2}, \frac{Y_1^2 - aX_1^2}{Z_1^2 - dT_1^2}\right) = \left(\frac{2Z_1T_1}{Z_1^2 + dT_1^2}, \frac{2Y_1^2 - Z_1^2 - dT_1^2}{Z_1^2 - dT_1^2}\right) \tag{8}$$

This formula is *independent of* a. The point doubling can be performed as $2(X_1 : Y_1 : T_1 : Z_1) = (X_3 : Y_3 : T_3 : Z_3)$ where

$$\begin{aligned} X_3 &= 2Z_1T_1(Z_1^2 - dT_1^2), \\ Y_3 &= (Z_1^2 + dT_1^2)(2Y_1^2 - Z_1^2 - dT_1^2), \\ Z_3 &= (Z_1^2 + dT_1^2)(Z_1^2 - dT_1^2), \\ T_3 &= 2Z_1T_1(2Y_1^2 - Z_1^2 - dT_1^2). \end{aligned}$$

This formula can be performed with a $4\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ algorithm as follows:

$$\begin{gathered} s_1 = T_1^2, \quad s_2 = Z_1^2, \quad s_3 = (T_1 + Z_1)^2 - s_1 - s_2, \quad s_4 = Y_1^2, \\ d_1 = d \cdot s_1, \quad a_1 = s_2 - d_1, \quad a_2 = s_2 + d_1, \quad a_3 = 2s_4 - a_2, \\ X_3 = s_3 \cdot a_1, \quad Y_3 = a_2 \cdot a_3, \quad Z_3 = a_1 \cdot a_2, \quad T_3 = s_3 \cdot a_3. \end{gathered}$$

5.4 Tripling in $\mathcal{E}^e$

The tripling formula can be derived by computing $3P = 2P + P$. The following formulas compute $(X_3 : Y_3 : T_3 : Z_3) = 3(X_1 : Y_1 : T_1 : Z_1)$ in $11\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$, where $\mathbf{D}$ is one multiplication by d.

$$s_1 = dT_1^2, \quad s_2 = Y_1^2, \quad s_3 = Z_1^2, \quad a_1 = s_1 + s_3,$$
$$a_2 = s_3 - s_1, \quad m_1 = a_2 \cdot s_2, \quad m_2 = a_2 \cdot (a_1 - s_2), \quad m_3 = a_1 \cdot (2s_2 - a_1),$$
$$a_3 = m_3 + m_1, \quad a_4 = m_3 + m_2, \quad a_5 = m_3 - m_1, \quad a_6 = m_2 - m_3,$$
$$m_4 = Y \cdot a_4, \quad m_5 = Y \cdot a_6, \quad , m_6 = Z \cdot a_5, \quad m_7 = T \cdot a_3,$$
$$X_3 = m_6 \cdot m_7, \quad Y_3 = m_4 \cdot m_5, \quad Z_3 = m_4 \cdot m_6, \quad T_3 = m_5 \cdot m_7.$$

5.5 Doubling in $\mathcal{E}$

The point doubling on $\mathcal{E}$ formula can be performed with a $4\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$ algorithm as follows:

$$s_1 = T_1^2, \quad s_2 = Z_1^2, \quad s_3 = (T_1 + Z_1)^2 - s_1 - s_2, \quad s_4 = Y_1^2,$$
$$d_1 = d \cdot s_1, \quad a_1 = s_2 - d_1, \quad a_2 = s_2 + d_1, \quad a_3 = 2s_4 - a_2,$$
$$T_3 = s_3 \cdot a_3 \quad Y_3 = a_2 \cdot a_3, \quad Z_3 = a_1 \cdot a_2.$$

5.6 Tripling in $\mathcal{E}$

The tripling formula can be performed with a $9\mathbf{M}+3\mathbf{S}+1\mathbf{D}$ algorithm as follows:

$$s_1 = dT_1^2, \quad s_2 = Y_1^2, \quad s_3 = Z_1^2, \quad a_1 = s_1 + s_3,$$
$$a_2 = s_3 - s_1, \quad m_1 = a_2 \cdot s_2, \quad m_2 = a_2 \cdot (a_1 - s_2), \quad m_3 = a_1 \cdot (2s_2 - a_1),$$
$$a_3 = m_3 + m_1, \quad a_4 = m_3 + m_2, \quad a_5 = m_3 - m_1, \quad a_6 = m_2 - m_3,$$
$$T_3 = T_1 \cdot a_3 \cdot a_6 \quad Y_3 = Y_1 \cdot a_4 \cdot a_6, \quad Z_3 = Z_1 \cdot a_4 \cdot a_5.$$

These formulae of addition, doubling, and tripling in this section cost the same as $a = -1$. And the formulae of addition save a few field operations compared with unified addition formulae.

6 Exceptional Case Analysis and Handling Strategies

In this section, we explore scalar multiplication on $2q$-order and $4q$-order subgroups, in addition to q-order subgroups, motivated by three factors.

Firstly, while q-order subgroups are known for their favorable properties and high completeness, ensuring that a point precisely lies on a subgroup of order q is challenging. In contrast, on Edwards448 curves, points must belong to the $4q$-order group. This forms the primary motivation for our investigation.

Secondly, the structure of the (twisted) Edwards curve inherently includes small-order points, which may expose it to attacks exploiting small cofactors. These attacks manipulate the scalar multiplication from q-order subgroups to 2q-order or 4q-order subgroups. If scalar multiplication fails on the $2q$-order and $4q$-order subgroups, an attacker could gather information about the secret key. Therefore, studying scalar multiplication in these cases becomes essential for protecting sensitive information.

Thirdly, Hamburg proposed the decaf technique to address the small cofactor trap on the Edwards448 curve using point compression and decompression [15] (CRYPTO 2015). Decaf technology eliminates the requirement for scalar multiplications to operate solely on subgroups of prime order. Instead, scalar multiplications over $2q$-order and $4q$-order subgroups are permitted. These subgroups are treated as a prime order group. The differences are handled during compression and decompression. Cremers and Jackson thought decaf is an exciting proposal [9]. Achieving exceptional-free scalar multiplication on $2q$-order and $4q$-order subgroups holds significance for decaf. It is the final motivation for our investigation.

A straightforward solution for scalar multiplication on both the $2q$-order and $4q$-order subgroups is to utilize the $9\mathbf{M} + 2\mathbf{D}$ unified point addition formula proposed by Hisil et al. [18]. Here, one $\mathbf{D}$ corresponds to multiplication with a, while the other corresponds to multiplication with d.

It is worth noting that our isomorphism mapping preserves the fact that a is a square element and d is a non-square element. Consequently, the elliptic curve obtained through the isomorphism remains a complete Edwards curve. The unified point addition formula proposed by Hisil et al. [18] is complete in this case. This is also why we propose the $d = -1$ point operation algorithms instead of obtaining the elliptic curve with $a = -1$ by birational mapping or isogeny as in [15] and run the point operations on that curve.

In this section, we analyze the exceptional cases in our new point addition algorithm. We propose corresponding solutions to enhance efficiency on the $2q$-order and $4q$-order subgroups.

We detail the exceptional cases of $2q$-order and $4q$-order subgroups on $\mathcal{E}^e$ in the following lemma.

Lemma 3. *Let K be a finite field of odd characteristic. Let $E_{a,d}$ be a twisted Edwards curve defined over K. Let $P = (T_1 : X_1 : Y_1 : Z_1)$ be a fixed point on $E_{a,d}$. Let $Q = (T_2 : X_2 : Y_2 : Z_2)$ be another point on $E_{a,d}$. Let $R_1 = (0 : 1 : 0 : \sqrt{a})$. Assume that a is a square and $d = -1$ is a non-square.*

For the unified addition formula, we have

- $Y_1Y_2 + aX_1X_2 = 0$ *if and only if*

$$(T_2 : X_2 : Y_2 : Z_2) \in \{(-T_1 : Y_1/\sqrt{a} : -\sqrt{a}X_1 : Z_1), (-T_1 : -Y_1/\sqrt{a} : \sqrt{a}X_1 : Z_1)\} = \{P + R_1, P + 3R_1\}$$

- $Y_1Y_2 - aX_1X_2 = 0$ *if and only if*

$$(T_2 : X_2 : Y_2 : Z_2) \in \{(T_1 : -Y_1/\sqrt{a} : -\sqrt{a}X_1 : Z_1), (T_1 : Y_1/\sqrt{a} : \sqrt{a}X_1 : Z_1)\} = \{-P + R_1, -P + 3R_1\}$$

- $T_1Z_2 + Z_1T_2 = 0$ *if and only if*

$$\begin{aligned}(T_2 : X_2 : Y_2 : Z_2) \in &\{(-T_1 : Y_1/\sqrt{a} : -\sqrt{a}X_1 : Z_1), (-T_1 : -Y_1/\sqrt{a} : \sqrt{a}X_1 : \\ &Z_1), (-T_1 : -X_1 : Y_1 : Z_1), (-T_1 : X_1 : -Y_1 : Z_1)\} \\ =&\{P + R_1, P + 3R_1, -P, -P + 2R_1\}\end{aligned}$$

- $T_1T_2 + Z_1Z_2 = 0$ *would not occur.*

For the fast addition formula, we have

- $Y_1X_2 + X_1Y_2 = 0$ *if and only if*

$$\begin{aligned}(T_2 : X_2 : Y_2 : Z_2) \in &\{(-T_1 : -X_1 : Y_1 : Z_1), (-T_1 : X_1 : -Y_1 : Z_1)\} \\ =&\{-P, -P + 2R_1\}\end{aligned}$$

- $Y_1X_2 - X_1Y_2 = 0$ *if and only if*

$$\begin{aligned}(T_2 : X_2 : Y_2 : Z_2) \in &\{(T_1 : -X_1 : -Y_1 : Z_1), (T_1 : X_1 : Y_1 : Z_1)\} \\ =&\{P, P + 2R_1\}\end{aligned}$$

- $T_1Z_2 - Z_1T_2 = 0$ *if and only if*

$$\begin{aligned}(T_2 : X_2 : Y_2 : Z_2) \in &\{(T_1 : -Y_1/\sqrt{a} : -\sqrt{a}X_1 : Z_1), (T_1 : Y_1/\sqrt{a} : \sqrt{a}X_1 : \\ &Z_1), (T_1 : X_1 : Y_1 : Z_1), (T_1 : -X_1 : -Y_1 : Z_1)\} \\ =&\{-P + R_1, -P + 3R_1, P, P + 2R_1\}\end{aligned}$$

- $T_1T_2 - Z_1Z_2 = 0$ *would not occur.*

Proof. Similar to Lemma 1, these equivalences are derived from combing the equations. For example, when obtain the exceptional cases of $Y_1Y_2 + aX_1X_2 = 0$, we combine $Y_1Y_2 + aX_1X_2 = 0$ with $aX_1^2 + Y_1^2 = Z_1^2 + dT_1^2, aX_2^2 + Y_2^2 = Z_2^2 + dT_2^2$, $X_1Y_1 = Z_1T_1$, and $X_2Y_2 = Z_2T_2$. And we ignore the solution $(T_2 : X_2 : Y_2 : Z_2) = (0 : 0 : 0 : 0)$.

6.1 Unified Addition Formula on $2q$-Order Subgroup

We first handle the easier but crucial case, the unified addition formula performs on the subgroup of order $2q$. For curve Edwards448, we have the following corollary of Lemma 3:

Corollary 2. *For the cases that a is a square element and $d = -1$ is a non-square element, points P and Q in the subgroup of order $2q$ would not induce the exceptional cases of our unified addition formula. In particular, the finite field of Edwards448 and E448 satisfy this condition.*

Proof. If both $P = (T_1 : X_1 : Y_1 : Z_1)$ and $Q = (T_2 : X_2 : Y_2 : Z_2)$ are points in the subgroup of order $2q$. According to Lemma 3, if zero occurs in $P + Q$, then $Q = -P$ or $Q = -P + 2R_1$. In addition, since $Q = -P$ or $-P + 2R_1$, we have $Q \neq \pm P + \pm R_1$. Thus, $Y_1Y_2 \pm aX_1X_2 \neq 0$. If $Q = -P$, $P + Q$ is computed as

$$P + Q = (0, 0, (Y_1^2 - aX_1^2)(Y_1^2 + aX_1^2), (Y_1Y_2 - aX_1X_2)(Z_1^2 - T_1^2))$$

by our unified addition formula. Combined with the fact that $Y_1^2 + aX_1^2 = Z_1^2 - T_1^2$ and $(Y_1^2 - aX_1^2)(Y_1^2 + aX_1^2) = (Y_1Y_2 + aX_1X_2)(Y_1Y_2 - aX_1X_2) \neq 0$. We have

$$P + Q = (0, 0, 1, 1).$$

The result is equal to what it should be. Thus, $Q = -P$ will not induce an exceptional case. Similarly, $Q = -P + 2R_1$ will not induce exceptional cases.

Corollary 2 shows that our unified addition formula is complete on the $2q$-order subgroup.

6.2 Strategy for Single-Scalar Multiplication

The single-scalar multiplication computes kP for a scalar k and a fixed point P. Since our unified addition formula is complete on the $2q$-order subgroup, it is exceptional free when computing single-scalar multiplication on the $2q$-order subgroup. However, Lemma 3 shows that our unified addition formula is not complete on the $4q$-order subgroup.

As for our fast point addition formula, it yields exceptions on subgroups of order $2q$ and $4q$ on Edwards448. Even if the exception to doubling ($P = Q$) is ignored, still some cases need to be handled on Edwards448.

We handle these exceptional cases by reducing the scalar k modulo q first, limiting the scalar in $\{0, 1, \cdots, q-1\}$. And then eliminate the difference through equivalence classes, as the way decaf did. The justification for this operation is supported by two reasons. Firstly, this modulus operation is common in elliptic curve cryptography. For example, the EdDSA signature generation operation in IETF RFC 8032 reduced the scalar modulo q for efficiency reasons [19]. Secondly, we will show that the differences between points calculated with and without the modulus fall within the 4-torsion subgroup of E later. Therefore, when integrated with decaf's Edwards-only strategy, these two outcomes effectively represent the

same point. The equivalence testing of $P = (T_1 : X_1 : Y_1 : Z_1)$ and $Q = (T_2 : X_2 : Y_2 : Z_2)$ can be made by checking whether

$$X_1Y_2 = Y_1X_2 \qquad \text{or} \qquad Y_1Y_2 = -aX_1X_2$$

as in ristretto [17]. Another solution is to test whether $4P = 4Q$ as mentioned in RFC 8032 [19].

If P is a point of order $4q$ or $2q$ on Edwards448 or E448, then we have $R_1 = mqP,\ m = 1, 3$, or $qP = 2R_1 = (0, -1),\ R_1 \notin \{kP, k \in \mathbb{N}\}$. Assuming Q is an exceptional point of P in Lemma 3, then

$$Q = kP, \quad k \equiv 1, q-1 \mod q, \qquad \text{or} \qquad Q \notin \{kP, k \in \mathbb{N}\}$$

In single-scalar multiplication with scalar smaller than $q-1$, the case $(q-1)P+P$ would not occur; the case $P+P$ is not the exceptional case of the unified addition formula and performed by the doubling formula when employing the fast addition formula; and the case $Q \notin \{kP, k \in \mathbb{N}\}$ can be disregarded.

The modular equivalence $k' = k \mod q$ yields that $k - k' = mq$ with $m \in \mathbb{N}$. Since each of Edwards448 and E448 only contains one 4-torsion subgroup, and the size of it is 4. We have $kP - k'P = mqP \in E[4]$, where $E[4] = \{(0, \pm 1), (\pm 1/\sqrt{a}, 0)\}$ is the 4-torsion subgroup of E.

6.3 Strategy for Multi-scalar Multiplication

Since the scalars between the adding points are blinding, our strategy for single-scalar multiplication is invalid for multi-scalar multiplication.

We propose a new algorithm that combines our unified addition formula and the unified addition formula proposed by Hisil et al. [18] to speed up the point addition on multi-scalar multiplication on Edwards448 and E448.

Assuming that $P = (T_1 : X_1 : Y_1 : Z_1)$ and $Q = (T_2 : X_2 : Y_2 : Z_2)$ are the two inputs of our unified addition formula. The addition can be performed by the following algorithm:

In Algorithm 1, we first compute the value of X_1X_2, Y_1Y_2, and aX_1X_2. In Lemma 3, we analyzed the exceptional cases of our unified addition formula. Similar to $Q = -P$ or $-P+2R_1$, our unified addition formula runs correct when $Q = -P + R_1$ or $-P + 3R_1$ with $Q \neq P + R_1$ or $P + 3R_1$. The exceptional cases that remained to be concerned are $Q = P+R_1, P+3R_1$ with P in the subgroup of order $4q$ or 4. No matter what the order of P is, the exceptional cases $Q = P+R_1$ or $P+3R_1$ yield $Y_1Y_2+aX_1X_2 = 0$ by Lemma 3. Algorithm 1 compute the result by the unified addition formula proposed by Hisil et al. [18] in these cases. Since this addition formula has been proved to be complete [20], Algorithm 1 returns the correct answer in these cases. As for the case $Y_1Y_2+aX_1X_2 \neq 0$, the output of our unified addition formula is correct. Algorithm 1 employs our unified addition formula in this situation.

When $Y_1Y_2 + aX_1X_2 = 0$, our algorithm costs $9\mathbf{M} + 1\mathbf{D} + 1\mathbf{V}$, where $\mathbf{V}$ denotes the time cost of verifying whether $Y_1Y_2 + aX_1X_2 = 0$ or not. And when $Y_1Y_2 + aX_1X_2 \neq 0$, our algorithm costs $8\mathbf{M} + 1\mathbf{D} + 1\mathbf{V}$. Since $d = -1$, Hisil

Algorithm 1: Addition algorithm for multi-scalar multiplication

Data: $P = (T_1 : X_1 : Y_1 : Z_1)$ and $Q = (T_2 : X_2 : Y_2 : Z_2)$
Result: $(T_3 : X_3 : Y_3 : Z_3) = P + Q$
$m_1 \to Y_1 \cdot Y_2$; $m_2 \to X_1 \cdot X_2$; $d_1 \to a \cdot m_2$;
if $m_1 + d_1 \neq 0$ **then**
    $m_3 \to (T_1 + Z_1) \cdot (T_2 + Z_2)$; $m_3 \to (T_1 - Z_1) \cdot (T_2 - Z_2)$; $a_1 \to 2m_1 + 2d_1$;
    $a_2 \to 2m_1 - 2d_1$; $a_3 \to m_3 + m_4$; $a_4 \to m_3 - m_4$; $X_3 \to a_3 \cdot a_4$; $Y_3 \to a_1 \cdot a_2$;
    $Z_3 \to a_1 \cdot a_3$; $T_3 \to a_2 \cdot a_4$;
else
    $m_3 \to -T_1 \cdot T_2$; $m_4 \to Z_1 \cdot Z_2$; $m_5 \to (X_1 + Y_1) \cdot (X_2 + Y_2) - m_1 - m_2$;
    $a_2 \to m_4 - m_3$; $a_3 \to m_4 + m_3$; $a_4 \to m_1 - d_1$; $X_3 \to m_5 \cdot a_2$; $Y_3 \to a_3 \cdot a_4$;
    $Z_3 \to a_2 \cdot a_3$; $T_3 \to m_5 \cdot a_4$;
return $(T_3 : X_3 : Y_3 : Z_3)$

et al.'s unified addition formula costs $9\mathbf{M} + 1\mathbf{D}$. Thus, our algorithm costs one more $\mathbf{V}$ when $Y_1Y_2 + aX_1X_2 = 0$, and saves $1\mathbf{M} - 1\mathbf{V}$ when $Y_1Y_2 + aX_1X_2 \neq 0$. Since $Y_1Y_2 + aX_1X_2 = 0$ rarely occurs, our algorithm is competitive with Hisil et al.'s unified addition formula when there are no constant time requirements.

However, our new algorithm contains an if-else judgment, and the time cost varies in different conditional branches. Thus, the unified addition formula proposed by Hisil et al. [18] is a better choice for multi-scalar multiplication that requires side-channel assistance.

7 Fast Scalar Multiplication

7.1 Parallelization for Unified Addition Formulae

In [18], Hisil et al. noticed that their unified addition formula is highly parallelizable. Our unified addition formulae also maintain this good property.

In particular, when there are 4 processors can be employed, both of the $8\mathbf{M}+1\mathbf{D}$ unified addition formula and the $8\mathbf{M}+4\mathbf{D}$ clearing denominators unified addition formulas can be performed with effective 5-steps $2\mathbf{M} + 1\mathbf{D}$ algorithm as in Table 2.

As in Table 2, although both of the $8\mathbf{M}+1\mathbf{D}$ unified addition formula and the $8\mathbf{M} + 4\mathbf{D}$ unified addition formulae require $2\mathbf{M} + 1\mathbf{D}$ in a 4-processor parallel point operation, the latter may be faster than the former. For example, the parameter d in Edwards25519 is $d = 121665/121666$. It implies that $d = \bar{d}/\bar{a}$ where $\bar{d} = 121665$ and $\bar{a} = 121666$. Thus, the D in 4-processor parallel of Edwards25519 is a field multiplication by $d = 121665/121666$, and the D in 4-processor parallel of Edwards25519 with clearing denominator is about field multiplication by $2\bar{d} = 2 \cdot 121666 = 243332$.

Table 2. 4-Processor unified addition formulae

cost	step	**Processor 1**	**Processor 2**	**Processor 3**	**Processor 4**
	1	$a_1 \leftarrow T_1 + Z_1$	$a_2 \leftarrow T_2 + Z_2$	$a_3 \leftarrow T_1 - Z_1$	$a_4 \leftarrow T_2 - Z_2$
1M	2	$m_1 \leftarrow X_1 \cdot X_2$	$m_2 \leftarrow Y_1 \cdot Y_2$	$m_3 \leftarrow a_1 \cdot a_2$	$m_4 \leftarrow a_3 \cdot a_4$
1D	3	$d_1 \leftarrow 2m_1$	$d_2 \leftarrow 2a \cdot m_2$	idle	idle
	4	$a_1 \leftarrow d_1 + d_2$	$a_2 \leftarrow d_1 - d_2$	$a_3 \leftarrow m_3 + m_4$	$a_4 \leftarrow m_3 - m_4$
1M	5	$X_3 \leftarrow a_3 \cdot a_4$	$Y_3 \leftarrow a_1 \cdot a_2$	$Z_3 \leftarrow a_1 \cdot a_3$	$T_3 \leftarrow a_2 \cdot a_4$

(a) $d = -1$

cost	step	**Processor 1**	**Processor 2**	**Processor 3**	**Processor 4**
	1	$a_1 \leftarrow T_1 + Z_1$	$a_2 \leftarrow T_2 + Z_2$	$a_3 \leftarrow T_1 - Z_1$	$a_4 \leftarrow T_2 - Z_2$
1M	2	$m_1 \leftarrow X_1 \cdot X_2$	$m_2 \leftarrow Y_1 \cdot Y_2$	$m_3 \leftarrow a_1 \cdot a_2$	$m_4 \leftarrow a_3 \cdot a_4$
1D	3	$d_1 \leftarrow 2\bar{d}m_1$	$d_2 \leftarrow 2\bar{a} \cdot m_2$	$d_3 \leftarrow 2\bar{d}m_4$	$d_4 \leftarrow 2\bar{d}m_4$
	4	$a_1 \leftarrow d_1 + d_2$	$a_2 \leftarrow d_1 - d_2$	$a_3 \leftarrow d_3 + d_4$	$a_4 \leftarrow d_3 - d_4$
1M	5	$X_3 \leftarrow a_3 \cdot a_4$	$Y_3 \leftarrow a_1 \cdot a_2$	$Z_3 \leftarrow a_1 \cdot a_3$	$T_3 \leftarrow a_2 \cdot a_4$

(b) $d = -1$ with clearing denominators

cost	step	**Processor 1**	**Processor 2**	**Processor 3**	**Processor 4**
	1	$a_1 \leftarrow X_1 + Y_1$	$a_2 \leftarrow X_2 + Y_2$	$a_3 \leftarrow X_1 - Y_1$	$a_4 \leftarrow X_2 - Y_2$
1M	2	$m_1 \leftarrow a_3 \cdot a_4$	$m_2 \leftarrow a_1 \cdot a_2$	$m_3 \leftarrow T_1 \cdot T_2$	$m_4 \leftarrow Z_1 \cdot Z_2$
1D	3	$d_1 \leftarrow \bar{a}m_1$	$d_2 \leftarrow \bar{a} \cdot m_2$	$d_3 \leftarrow 2\bar{d}m_4$	$d_4 \leftarrow 2\bar{a}m_4$
	4	$a_1 \leftarrow d_2 - d_1$	$a_2 \leftarrow d_4 - d_3$	$a_3 \leftarrow d_3 + d_4$	$a_4 \leftarrow d_1 + d_2$
1M	5	$X_3 \leftarrow a_1 \cdot a_2$	$Y_3 \leftarrow a_3 \cdot a_4$	$Z_3 \leftarrow a_1 \cdot a_4$	$T_3 \leftarrow a_2 \cdot a_3$

(c) $a = -1$ with clearing denominators

7.2 Speedup by Mixing Different Coordinates

The mixing different coordinates technique in elliptic curve cryptography was first proposed by Cohen, Miyaji, and Ono to speed up the scalar multiplication on short Weierstrass curves [8]. Hisil et al. used this technique on twisted Edwards curves [18]. We also take this technique for the case $d = -1$.

Recall that given $(T : Y : Z)$ in $\mathcal{E}$ passing to $\mathcal{E}^e$ requires $3\mathbf{M} + 1\mathbf{S}$ by computing (TY, TZ, Y^2, YZ), and given $(T : X : Y : Z)$ in $\mathcal{E}^e$ passing to $\mathcal{E}$ is cost-free by simply ignoring X. When performing a scalar multiplication, the scalar multiplication can be speedup by employing the following strategies:

(1) If a point doubling or tripling is followed by another point doubling or tripling, one should employ the corresponding formula on $\mathcal{E}$.
(2) After each addition, the tripling scalar multiplication *should* be performed as early as possible.
(3) If a point doubling or tripling is followed by a point addition, please use $\mathcal{E}^e \leftarrow k\mathcal{E}, k = 2, 3$ and $\mathcal{E} \leftarrow \mathcal{E}^e + \mathcal{E}^e$ for the point doubling or tripling and the point addition.

The core idea is cutting down the number of computations of the coordinate X. Then, when $d = -1$, the cost of the doubling formula can be considered as $4\mathbf{M} + 3\mathbf{S}$; and the cost of the addition formula can be considered as $8\mathbf{M}$ (with one $\mathbf{M}$ more from the doubling formula to obtain X-coordinate for the input point of the addition and one $\mathbf{M}$ less since the X-coordinate output point can be ignored). For more details, please see [18] §4.

8 Conclusion

In this paper, we proposed efficient point operations on twisted Edwards curves $d = -1$. Two addition formulas are introduced, one of them is unified. Two unified addition formulas with clearing denominators are introduced to gain new speed records in the parallel environments.

The unified addition formula with $d = -1$ saves $1\mathbf{M}+1\mathbf{D}$ compared with the general case in [18]. It is approximately 11.1% and 18.2% faster than the results in [18] under the assumptions $\mathbf{D}/\mathbf{M} \approx 0$ and $\mathbf{D}/\mathbf{M} \approx 1$, respectively. The faster addition formula costs only $8\mathbf{M}$, saving an additional $\mathbf{D}$ compared to our unified addition formula. Moreover, special doubling and tripling formulas are proposed. All of these formulae are as fast as the best-known results for $a = -1$.

Acknowledgments. The authors would like to thank the anonymous reviewers for many helpful comments and their helpful suggestions. This work was supported by the National Key R&D Program of China (Grant No. 2023YFB4503203), the National Natural Science Foundation of China (Grant No. 62272453 and 62272186), the Key Research Program of the Chinese Academy of Sciences (Grant No. ZDRW-XX-2022-1), and the Innovation Project of Jinyinhu Laboratory (Grant No. 2023JYH010103).

References

1. Bernstein, D.J., Birkner, P., Joye, M., Lange, T., Peters, C.: Twisted Edwards curves. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 389–405. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-68164-9_26
2. Bernstein, D.J., Birkner, P., Lange, T., Peters, C.: ECM using Edwards curves. Math. Comput. **82**, 1139–1179 (2013)
3. Bernstein, D.J., Lange, T.: Faster addition and doubling on elliptic curves. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 29–50. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-76900-2_3
4. Bernstein, D.J., Lange, T.: Inverted Edwards coordinates. In: Boztaş, S., Lu, H.-F.F. (eds.) AAECC 2007. LNCS, vol. 4851, pp. 20–27. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-77224-8_4
5. Bernstein, D.J., Lange, T.: A complete set of addition laws for incomplete Edwards curves. J. Number Theory **131**(5), 858–872 (2011). https://doi.org/10.1016/j.jnt.2010.06.015, https://www.sciencedirect.com/science/article/pii/S0022314X10002155. Elliptic Curve Cryptography
6. Bouvier, C., Imbert, L.: Faster cofactorization with ECM using mixed representations. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020. LNCS, vol. 12111, pp. 483–504. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45388-6_17

7. Chen, L., Moody, D., Regenscheid, A., Randall, K.: NIST special publication 800-186, recommendations for discrete logarithm-based cryptography: elliptic curve domain parameters. Technical report (2023). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-186.pdf
8. Cohen, H., Miyaji, A., Ono, T.: Efficient elliptic curve exponentiation using mixed coordinates. In: Ohta, K., Pei, D. (eds.) ASIACRYPT 1998. LNCS, vol. 1514, pp. 51–65. Springer, Heidelberg (1998). https://doi.org/10.1007/3-540-49649-1_6
9. Cremers, C., Jackson, D.: Prime, order please! Revisiting small subgroup and invalid curve attacks on protocols using Diffie-Hellman. In: 2019 IEEE 32nd Computer Security Foundations Symposium (CSF), pp. 78–7815. IEEE (2019)
10. Edwards, H.M.: A normal form for elliptic curves. Bull. Am. Math. Soc. **44**, 393–423 (2007). https://doi.org/10.1090/S0273-0979-07-01153-6
11. Euler, L.: Observationes de comparatione arcuum curvarum irrectificibilium. Novi commentarii academiae scientiarum Petropolitanae 58–84 (1761)
12. Farashahi, R.R., Hosseini, S.G.: Differential addition on twisted Edwards curves. In: Pieprzyk, J., Suriadi, S. (eds.) ACISP 2017. LNCS, vol. 10343, pp. 366–378. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-59870-3_21
13. Galbraith, S.D., Lin, X., Scott, M.: Endomorphisms for faster elliptic curve cryptography on a large class of curves. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 518–535. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01001-9_30
14. Gallant, R.P., Lambert, R.J., Vanstone, S.A.: Faster point multiplication on elliptic curves with efficient endomorphisms. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 190–200. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_11
15. Hamburg, M.: Decaf: eliminating cofactors through point compression. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015, Part I. LNCS, vol. 9215, pp. 705–723. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47989-6_34
16. Hamburg, M.: Ed448-goldilocks, a new elliptic curve. Cryptology ePrint Archive, Report 2015/625 (2015). https://eprint.iacr.org/2015/625
17. de Valence, H., Grigg, J., Tankersley, G., Valsorda, F., Lovecruft, I.: The ristretto255 group. Technical report, IETF CFRG Internet Draft (2019)
18. Hisil, H., Wong, K.K.-H., Carter, G., Dawson, E.: Twisted Edwards curves revisited. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 326–343. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-89255-7_20
19. Josefsson, S., Liusvaara, I.: Edwards-curve digital signature algorithm (EdDSA). RFC 8032 (2017). https://doi.org/10.17487/RFC8032, https://www.rfc-editor.org/info/rfc8032
20. Kohel, D.: Addition law structure of elliptic curves. J. Number Theory **131**(5), 894–919 (2011). https://doi.org/10.1016/j.jnt.2010.12.001
21. Miniero, L., Murillo, S.G., Pascual, V.: Guidelines for end-to-end support of the RTP control protocol (RTCP) in back-to-back user agents (B2BUAs). RFC 8079 (2017). https://doi.org/10.17487/RFC8079, https://www.rfc-editor.org/info/rfc8079
22. National Institute of Standards and Technology (NIST): Federal information processing standard (FIPS) 186-5, digital signature standard (DSS)
23. Sedlacek, V., Chi-Domínguez, J.-J., Jancar, J., Brumley, B.B.: A formula for disaster: a unified approach to elliptic curve special-point-based attacks. In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021. LNCS, vol. 13090, pp. 130–159. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-92062-3_5

24. Yu, W., Musa, S.A., Li, B.: Double-base chains for scalar multiplications on elliptic curves. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020. LNCS, vol. 12107, pp. 538–565. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45727-3_18
25. Yu, W., Xu, G.: Pre-computation scheme of window τNAF for koblitz curves revisited. In: Canteaut, A., Standaert, F.-X. (eds.) EUROCRYPT 2021. LNCS, vol. 12697, pp. 187–218. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-77886-6_7