Differential Addition on Twisted Edwards Curves

Reza Rezaeian Farashahi[1,2(✉)] and Seyed Gholamhossein Hosseini[1]

[1] Department of Mathematical Sciences, Isfahan University of Technology, 84156-83111, Isfahan, Iran
farashahi@cc.iut.ac.ir, g.hoseini@math.iut.ac.ir
[2] School of Mathematics, Institute for Research in Fundamental Sciences (IPM), P.O. Box 19395-5746, Tehran, Iran

Abstract. This paper presents new differential addition (i.e., the addition of two points with the known difference) and doubling formulas, as the core step in Montgomery scalar multiplication, for twisted Edwards curves. The formulas are provided with cost of $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$, $3\mathbf{M} + 7\mathbf{S} + 1\mathbf{D}$ and $3\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$ when the given difference point is in affine form. Here, $\mathbf{M}, \mathbf{S}, \mathbf{D}$ denote the costs of a field multiplication, a field squaring and a field multiplication by a constant, respectively.

Keywords: Elliptic curves · Twisted Edwards curves · Montgomery ladder · Differential addition

1 Introduction

An elliptic curve E over a field $\mathbb{F}$ is given by the Weiersrasß equation

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

where coefficients a_1, a_2, a_3, a_4 and a_6 are in $\mathbb{F}$. Elliptic curves are represented in other forms such as Legendre equation, cubic equations, quartic equations and intersection of two quadratic surfaces [16,17]. Koblitz [13] and Miler [14] independently proposed the use of elliptic curves over finite fields in cryptography. Since the introduction of elliptic curve cryptography (ECC) elliptic curves over finite fields have been studied intensively and in particular, many proposals have been made to speed up their group arithmetic. ECC is one of the attractive asymmetric key cryptosystems with the main advantage of achieving smaller key sizes under the same security level compare to that of other existing asymmetric systems such as RSA. This makes ECC suitable for software and hardware implementation in constrained environments including RFID tags, mobiles, sensors, and smart cards.

The scalar multiplication is the main important operation of ECC which is implemented based on the basic operations in finite fields. That is to compute kP for a given point P on elliptic curve E defined over a finite field $\mathbb{F}_q$ and a given

J. Pieprzyk and S. Suriadi (Eds.): ACISP 2017, Part II, LNCS 10343, pp. 366–378, 2017.
DOI: 10.1007/978-3-319-59870-3_21

integer k. The scalar multiplication is performed recursively by point addition and point doubling operations. One of the key factor in implementation of these basic curve operations is to reduce the number of field operations. This is why different forms of elliptic curves with several coordinates systems have been studied to improve the efficiency and to speed up the point multiplication. The well known recent form is Edwards curves [7] and their variants (see [1–3,12]) with great impact to ECC.

Side channel attacks use the time or power differences between implementing point addition and point doubling to reveal information about the bits of the secret k. Montgomery [15] introduced a technique for scalar multiplication of points for a special type of curves in large characteristic that is known as Montgomery ladder. In each step of the Montgomery scalar multiplication algorithm both the addition and the doubling are used which makes this method resistant against simple side-channel attacks. For Montgomery curves, the basic formulas in each step of the Montgomery ladder is differential addition and doubling expressed only by the x-coordinates of the points. For the fixed point P on the curve, this method computes the x-coordinate of the point kP recursively by computing the x-coordinates of the points $P + 2Q$ and $2Q$ from the x-coordinates of the points $P + Q$, Q. To avoid the costly field inversion operation, the computations are performed where points are represented in projective coordinates and the cost of projective x-coordinate formulas for Montgomery curves is $6\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$. Here a multiplication in $\mathbb{F}_q$ costs one $\mathbf{M}$, a squaring costs one $\mathbf{S}$ and the cost of field multiplication by a parameter (as a constant) is denoted by $\mathbf{D}$. The x-coordinate of the fixed base point P can be represented in affine form, then the differential mixed addition and doubling formulas are computed using $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$.

The Montgomery method is extended to other forms of elliptic curves, where the basic operation in each step of the ladder is differential addition and doubling expressed only by suitable w-coordinates of the points. That is to compute the w-coordinates of the addition and doubling from the w-coordinates of given points and their difference. The Montgomery-like formulas for Edwards and binary Edwards curves are presented in [3,6,8]. Gaudry and Lubicz [9] presents a very efficient Montgomery-like formulas for Kummer line the cost of $4\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$, and $3\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$ if the base point is affine. Bernstein and Lange [5] extends the Kummer-line formulas for incomplete Edwards curves with the same costs.

From the literature, the mixed differential addition and doubling formulas with the cost of $3\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$ are only given for elliptic curves with 3 points of order 2. Notice, complete twisted Edwards are suitable for cryptographic applications because of their fast complete addition law. A complete twisted Edwards curve has two points of order 4 and one single point of order 2. The main contribution of this paper is to provide faster Montgomery-like formulas for complete twisted Edwards curves, which covers all elliptic curves over finite fields with a point of order 4 and a single point of order 2. This paper presents new differential addition and doubling formulas for twisted Edwards curves with cost of $5\mathbf{M}+4\mathbf{S}+1\mathbf{D}$, $3\mathbf{M}+7\mathbf{S}+1\mathbf{D}$ and $3\mathbf{M}+6\mathbf{S}+3\mathbf{D}$ when the given difference point is in affine form.

The rest of the paper is organized as follows. In Sect. 2 we review twisted Edwards curves, and in Sect. 3 we briefly describe differential addition on elliptic curves. The proposed new differential addition and doubling formulas are provided in Sect. 4 and finally, Sect. 5 concludes the paper with a comparison between our work and other previously related work.

Throughout the paper, the letter p always denotes an odd prime number and q denotes a prime power of p. A field is denoted by $\mathbb{F}$ and a finite field of size q is denoted by $\mathbb{F}_q$. Let χ denote the quadratic character in $\mathbb{F}_q$, where $p \geq 3$. Then, for any q where $p \geq 3$, we have $u = w^2$ for some $w \in \mathbb{F}_q^*$ if and only if $\chi(u) = 1$.

2 Twisted Edwards Curve

In 2007, Edwards introduced a new normal form for elliptic curves [7]. An original *Edwards curve*, defined over a field $\mathbb{F}$ with characteristic $p \neq 2$, by the equation

$$\mathbf{E}_{\mathrm{E},c}: \quad X^2 + Y^2 = c^2(1 + X^2Y^2),$$

with $c \in \mathbb{F}$ and $c^5 \neq c$. Bernstein and Lange [2] considered the use of Edwards curves over finite fields for elliptic curve cryptography. They extended the original curves to the family of so called *Edwards curves*

$$\mathbf{E}_{\mathrm{BL},d}: \quad X^2 + Y^2 = 1 + dX^2Y^2,$$

where $d \in \mathbb{F}$ with $d \neq 0, 1$. The family of Edwards curves over a finite field $\mathbb{F}_q$ with odd characteristic is equivalent (up to $\mathbb{F}_q$ isomorphism) to the family of all elliptic curves over $\mathbb{F}_q$ with a $\mathbb{F}_q$-rational point of order 4 [1]. In other words, $\mathbf{E}_{\mathrm{BL},d}(\mathbb{F}_q)$, the group of $\mathbb{F}_q$-rational points of the Edwards curve $\mathbf{E}_{\mathrm{BL},d}$, has a $\mathbb{F}_q$-rational point of order 4 and in the other way around, every elliptic curve E over $\mathbb{F}_q$ with a point of order 4 can be represented as an Edwards curve. In addition, $\mathbf{E}_{\mathrm{BL},d}(\mathbb{F}_q)$ has a single point of order 2 if and only if $\chi(d) = -1$, i.e., the group $\mathbf{E}_{\mathrm{BL},d}(\mathbb{F}_q)$ has three points of order 2 if and only if $\chi(d) = 1$.

Edwards curves and their extensions have attracted great interest in elliptic curve cryptography (see [1–3,12]). Bernstein et al. proposed the family of so-called *twisted Edwards*, [1], given by

$$\mathbf{E}_{\mathrm{TE},a,d}: \quad aX^2 + Y^2 = 1 + dX^2Y^2,$$

where a, d are distinct nonzero elements of $\mathbb{F}_q$. The addition and doubling law for $\mathbf{E}_{\mathrm{TE},a,d}$ are given by

$$\begin{aligned}(x_1, y_1),\ (x_2, y_2) &\mapsto \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right),\\ (x_1, y_1) &\mapsto \left(\frac{2x_1y_1}{1 + dx_1^2y_1^2}, \frac{y_1^2 - ax_1^2}{1 - dx_1^2y_1^2}\right).\end{aligned} \tag{1}$$

The identity point of the addition law is $(0, 1)$ and the additive negation of a point (x, y) is $(-x, y)$. The point $(0, -1)$ is a point of order 2. If $\chi(a) = 1$ then the points $(\pm 1/\sqrt{a}, 0)$ are of order 4.

The projective closure of the twisted Edwards curve $\mathbf{E}_{\mathrm{TE},a,d}$ in $\mathbb{P}^2$ includes the projective points $(X : Y : Z)$ in $\mathbb{P}^2(\mathbb{F}_q)$ satisfying the curve equation

$$aX^2Z^2 + Y^2Z^2 = Z^4 + dX^2Y^2,$$

with the points at infinity $\infty_1 = (1 : 0 : 0)$ and $\infty_2 = (0 : 1 : 0)$. These points are singular. In the nonsingular model of $\mathbf{E}_{\mathrm{TE},a,d}$ the point ∞_1 splits into two distinct $\mathbb{F}_q$-rational points if $\chi(ad) = 1$ and is removed if $\chi(ad) = -1$. Similarly, above the point ∞_2 there exists exactly two distinct points if $\chi(d) = 1$ and no point if $\chi(d) = -1$. So, if $\chi(d) = \chi(ad) = -1$ then the set of $\mathbb{F}_q$-rational projective points of $\mathbf{E}_{\mathrm{TE},a,d}$ is the set of $\mathbb{F}_q$-rational affine points which form a group. To represent the points above the points at infinity, the projective closures of $\mathbf{E}_{\mathrm{TE},a,d}$ in $\mathbb{P}^3$ or in $\mathbb{P} \times \mathbb{P}$ are considered [4,12]. The twisted Edwards curve $\mathbf{E}_{\mathrm{TE},a,d}$ over $\mathbb{F}_q$ is represented by the set of points $(X : Y : T : Z)$ in $\mathbb{P}^3(\mathbb{F}_q)$ satisfying the equations

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

Here, the $\mathbb{F}_q$-rational points above ∞_1 are $(1 : 0 : \pm\sqrt{a/d} : 0)$ if $\chi(ad) = 1$, and the points above ∞_2 are $(0 : \pm\sqrt{d} : 1 : 0)$ if $\chi(d) = 1$. Hisil et al. [12] gave the addition laws for the projective closure of $\mathbf{E}_{\mathrm{TE},a,d}$ embedded in $\mathbb{P}^3$ as follows.

$$\begin{aligned}&(X_1 : Y_1 : T_1 : Z_1) + (X_2 : Y_2 : T_2 : Z_2)\\ = \;&\begin{array}{l}((X_1Y_2 + Y_1X_2)(Z_1Z_2 - dT_1T_2) : (Y_1Y_2 - aX_1X_2)(Z_1Z_2 + dT_1T_2)\\ : (Y_1Y_2 - aX_1X_2)(X_1Y_2 + Y_1X_2) : (Z_1Z_2 - dT_1T_2)(Z_1Z_2 + dT_1T_2)).\end{array}\end{aligned} \tag{2}$$

Here the identity point is $(0 : 1 : 0 : 1)$ and the additive negation of a point $(X : Y : T : Z)$ is $(-X : Y : -T : Z))$. The point $(0 : -1 : 0 : 1)$ is a point of order 2 and the points $(1 : 0 : \pm\sqrt{a/d} : 1)$ are the points of order 2 if $\chi(ad) = 1$. The points $(\pm 1/\sqrt{a} : 0 : 0 : 1)$ and $(0 : \pm\sqrt{d} : 1 : 0)$ are of order 4 if $\chi(a) = 1$ and $\chi(d) = 1$, respectively. Other points of order 4 are $(\alpha : \beta : \alpha\beta : 1)$ where $\alpha^4 = 1/ad$ and $\beta^4 = a/d$.

Notice, that the family of twisted Edwards curves is the extension of the family of Edwards curves. Clearly, every Edwards curve $\mathbf{E}_{\mathrm{BL},d}$ is the twisted Edwards $\mathbf{E}_{\mathrm{TE},1,d}$. Furthermore, a twisted Edwards curve $\mathbf{E}_{\mathrm{TE},a,d}$ is a twist of the Edwards curve $\mathbf{E}_{\mathrm{BL},\frac{d}{a}}$. Therefore, the family of twisted Edwards includes Edwards curves and their twists.

The addition law in twisted Edwards curve $\mathbf{E}_{\mathrm{TE},a,d}$ is complete if $\chi(d) = \chi(ad) = -1$. In other words, the projective formulas (2) have no exceptional cases if $\chi(a) = 1$ and $\chi(d) = -1$ [1,12]. Here, we show that the addition law in twisted Edwards curve $\mathbf{E}_{\mathrm{TE},a,d}$ is also complete if $\chi(a) = \chi(ad) = -1$.

Theorem 1. *Let a, d be elements of $\mathbb{F}_q$ such that $ad(a - d) \neq 0$. Let $\mathbf{E}_{\mathrm{TE},a,d}$ be a twisted Edwards curve over $\mathbb{F}_q$. Then, $\mathbf{E}_{\mathrm{TE},a,d}$ has a complete projective formulas over $\mathbb{F}_q$ if $\chi(ad) = -1$.*

Proof. If $\chi(d) = \chi(ad) = -1$, then the projective formulas (2) are complete formulas for $\mathbf{E}_{\mathrm{TE},a,d}$ [1,12]. If $\chi(a) = \chi(ad) = -1$, then the twisted Edwards

curve $\mathbf{E}_{\mathrm{TE},a,d}$ is birationally equivalent to $\mathbf{E}_{\mathrm{TE},d,a}$ via the map $(x,y) \to (x,1/y)$. In other words, the projective points of the projective closures of $\mathbf{E}_{\mathrm{TE},a,d}$ and $\mathbf{E}_{\mathrm{TE},d,a}$ in $\mathbb{P}^3(\mathbb{F}_q)$ are corresponded to each other via the map $(X:Y:T:Z) \to (T:Z:X:Y)$. From (2) and using the exchange of variables, we obtain the projective formulas for the curve $\mathbf{E}_{\mathrm{TE},a,d}$ as follows.

$$\begin{aligned}&(X_1:Y_1:T_1:Z_1)+(X_2:Y_2:T_2:Z_2)\\ =\ &\begin{array}{l}((Z_1Z_2-dT_1T_2)(T_1Z_2+Z_1T_2)\ :(Y_1Y_2-aX_1X_2)(Y_1Y_2+aX_1X_2)\\ :(T_1Z_2+Z_1T_2)(Y_1Y_2-aX_1X_2):(Z_1Z_2-dT_1T_2)(Y_1Y_2+aX_1X_2)).\end{array}\end{aligned} \tag{3}$$

Therefore, the projective formulas (3) are complete formulas for $\mathbf{E}_{\mathrm{TE},a,d}$ over $\mathbb{F}_q$ where $\chi(a) = -1$ and $\chi(d) = 1$ which concludes the proof.

It is shown in [1], that a twisted Edwards curve $\mathbf{E}_{\mathrm{TE},a,d}$ over a field $\mathbb{F}$ is birationally equivalent to a *Montgomery curve* [15] given by the equation

$$\mathbf{E}_{\mathbf{M},A,B}: \quad BY^2 = X^3 + AX^2 + X, \tag{4}$$

where $A, B \in \mathbb{F}$ with $A \neq \pm 2$ and $B \neq 0$. In more details a twisted Edwards curve $\mathbf{E}_{\mathrm{TE},a,d}$ is birationally equivalent to the Montgomery curve $\mathbf{E}_{\mathbf{M},A,B}$ by the map $\psi : \mathbf{E}_{\mathrm{TE},a,d} \to \mathbf{E}_{\mathbf{M},A,B}$

$$\psi(x,y) = \Big(\frac{1+y}{1-y}, \frac{1+y}{x(1-y)}\Big). \tag{5}$$

where $A = 2(a+d)/(a-d)$, $B = 4/(a-d)$. Also, the Montgomery curve $\mathbf{E}_{\mathbf{M},A,B}$ is birationally equivalent to the twisted Edwards curve $\mathbf{E}_{\mathrm{TE},a,d}$ by the inverse map

$$\psi^{-1}(x,y) = \Big(\frac{x}{y}, \frac{x-1}{x+1}\Big),$$

where $a = (A+2)/B$, $d = (A-2)/B$.

3 Differential Addition

The main computational core for elliptic curve cryptography is performing scalar multiplication in an efficient and secure way. The computation of kP, for a given point P on elliptic curve E defined over a finite field $\mathbb{F}_q$ and a given integer k, is performed recursively by point addition (PA) and point doubling (PD) formulas. The time or power differences between implementing point addition (PA) and point doubling (PD) can reveal information about the bits of the secret k which makes the system insecure against side channel attacks.

In Montgomery curves [15], the special formulas for addition and doubling is done with the X and Z coordinates of a point in projective form. In each step of Montgomery ladder both addition and doubling are performed, which makes this method resistant against simple side-channel attacks. Recovering the

Algorithm 1. Projective x-coordinate dADD for Montgomery curves

Input : $\mathbf{E}_{\mathbf{M},A,B}/\mathbb{F}_q : BY^2 = X^3 + AX^2 + X$ ▷ The Montgomery curve $\mathbf{E}_{\mathbf{M},A,B}$
$(X_i : Z_i) = x(P_i),\ i = 0, 1, 2.$ ▷ $x(P_0) = x(P_1 - P_2)$
Output : $(X_i : Z_i) = x(P_i),\ i = 3, 4.$ ▷ $x(P_3) = x(P_1 + P_2),\ x(P_4) = x(2P_1)$

function DADD$((X_0 : Z_0),\ (X_1 : Z_1),\ (X_2 : Z_2))$
  $X_3 = Z_0\ (X_1X_2 - Z_1Z_2)^2$
  $Z_3 = X_0\ (X_1Z_2 - X_2Z_1)^2$
  $X_4 = (X_1^2 - Z_1^2)^2$
  $Z_4 = 4X_1Z_1(\ (X_1 + Z_1)^2 + (A - 2)X_1Z_1\ )$
  return $((X_4 : Z_4),\ (X_3 : Z_3))$ ▷ The differential addition and doubling
end function

Y coordinate of the output point is done in the last step from the X and Z coordinates. Algorithm 1 provides the differential x-coordinate formulas for Montgomery curves $\mathbf{E}_{\mathbf{M},A,B}$ over $\mathbb{F}_q$ [15].

We note, that $\mathcal{O} = (0 : 1 : 0)$ is the point at infinity on the Montgomery curve $\mathbf{E}_{\mathbf{M},A,B}$ over $\mathbb{F}_q$ and $x(\mathcal{O})$ in $\mathbb{P}(\mathbb{F}_q)$ is represented by $(1 : 0)$. Also, $x((0, 0))$ is given by $(0 : 1)$. We can easily check, that the projective x-coordinate differential addition formulas in Algorithm 1 work for all inputs except for the case where $x(P_0)$ equals $(1 : 0)$ or $(0 : 1)$, i.e., where the point P_0 equals $\mathcal{O}$ or $(0, 0)$. In other words, the Montgomery ladder works for all inputs if the base point is not a point at infinity or the point $(0, 0)$. The Montgomery ladder is given by the Algorithm 2, that for any integer k and any point P (not equal $\mathcal{O}$ and $(0, 0)$) computes $x(kP)$ correctly. In particular, the ladder works properly even if the integer k is bigger than the order of the base point P. Therefore, one can use random scalar k as a countermeasure to protect against differential power analysis attack.

Algorithm 2. The modified Montgomery scalar multiplication

Input : $\mathbf{E}_{\mathbf{M},A,B}/\mathbb{F}_q : BY^2 = X^3 + AX^2 + X$ ▷ The Montgomery curve $\mathbf{E}_{\mathbf{M},A,B}$
$P = (x : y : z) \in \mathbf{E}_{\mathbf{M},A,B}(\mathbb{F}_q)$ ▷ $P \neq \mathcal{O} = (0 : 1 : 0), P \neq (0 : 0 : 1)$
$k = (k_{m-1}, \cdots, k_1, k_0)$ ▷ $0 \leq k \in \mathbb{Z}$
$(X_0 : Z_0) := (x : z),\ (X_1 : Z_1) := (1 : 0),\ (X_2 : Z_2) := (x : z).$
Output : $x(kP)$

for $i := m - 1$ **down to** 0 **do**
  if $k_i = 0$ **then**
    $((X_1 : Z_1), (X_2 : Z_2)) := \mathrm{dADD}((X_0 : Z_0), (X_1 : Z_1), (X_2 : Z_2))$
  else
    $((X_2 : Z_2), (X_1 : Z_1)) := \mathrm{dADD}((X_0 : Z_0), (X_2 : Z_2), (X_1 : Z_1))$
  end if
end for
return $(X_1 : Z_1),\ (X_2 : Z_2)$ ▷ The differential addition and doubling

The Montgomery method is extended to other forms of elliptic curves with a suitable rational function. Let w be a rational function in the coordinate ring of the elliptic curve E over $\mathbb{F}_q$ where $w(P) = w(-P)$ for every point P in $E(\mathbb{F}_q)$. The w-coordinate *differential addition* and *doubling* means to compute $w(P+Q)$ and $w(2Q)$ from given values $w(P)$, $w(Q)$ and $w(P-Q)$, where P, Q are points on $E(\mathbb{F}_q)$. If w is regular at the point P then $w(P)$ is represented by $(w(P) : 1)$ in the projective line $\mathbb{P}(\mathbb{F}_q)$. Otherwise, it is represented by $(1 : 0)$. For the fixed point P on the curve and a positive integer k, the w-coordinate of the point kP is performed recursively by differential addition and doubling formulas expressed only by w-coordinates of the points.

A projective w-coordinate differential addition is *complete* if it works for all inputs. Also, it is *almost complete* if the w-coordinate differential formulas work for all inputs except for the case where $w(P_0)$ equals $w(\mathcal{O})$, where $\mathcal{O}$ is the neutral element of the group of points $E(\mathbb{F}_q)$. Note that, the projective x-coordinate differential addition for Montgomery curves given in Algorithm 1 works for all inputs except for the case where $w(P_0)$ equals $(1 : 0)$ or $(0 : 1)$. The fast and complete differential addition formulas are very interesting for implementations. But, if the base point P_0 has large prime order then with suitable w-function $w(P_0) \neq w(\mathcal{O})$ and $w(P_0) \neq (1 : 0), (0 : 1)$. Therefore, the almost complete and Montgomery-like formulas are usable for cryptographic applications.

The cost of projective x-coordinate differential addition and doubling formulas for Montgomery curves $\mathbf{E}_{\mathbf{M},A,B}$ over $\mathbb{F}_q$ given by Algorithm 1 is $6\mathbf{M}+4\mathbf{S}+1\mathbf{D}$. The x-coordinate of the fixed base point P can be represented by $x(P) = (X_0 : Z_0)$, where $Z_0 = 1$, then the differential addition and doubling formulas are computed using $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$.

Castryck, Galbraith and Farashahi [6] give the y-coordinate differential addition Montgomery-like formulas for Edwards curves. They use the quasi free projective map between twisted Edwards and Montgomery curves which provides the Montgomery formulas for twisted Edwards curves with the cost of $6\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$, and $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ if the base point is affine. They also give a doubling formulas with cost of $1\mathbf{M} + 3\mathbf{S} + 3\mathbf{D}$ assuming d is a square element. Gaudry and Lubicz [9] obtained a very efficient differential addition Montgomery-like formulas for Kummer line with the cost of $4\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$, and $3\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$ if the base point is affine. The Kummer line behaves very similar to the Montgomery form. Compare to the Montgomery form, the Kummer line formulas saves $2\mathbf{M} - 2\mathbf{S}$, but have extra 2 multiplication by constants. The Kummer line is linked to the Legendre curve $\mathbf{E}_\lambda : Y^2 = X(X-1)(X-\lambda)$, where $\lambda = a^4/(a^4 - b^4)$ and $(a : b)$ defines the Kummer line. The group order of the corresponding curve E_λ over $\mathbb{F}_q$ is divisible by 4, and in particular it has 3 points of order 2. Bernstein and Lange [5] provides a Kummer-line formulas for Edwards curves $\mathbf{E}_{\mathrm{BL},d}$ where $d = r^2$ is a square element. They give the cost of w-coordinates mixed differential addition and doubling formulas for $w = ry$ and $w = ry^2$ by $3\mathbf{M} + 6\mathbf{S} + 5\mathbf{D}$ and $3\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$ respectively. Here, the Edwards curve $\mathbf{E}_{\mathrm{BL},d}$ over $\mathbb{F}_q$ with $\chi(d) = 1$ has 3 points of order 2 and the addition law

is not complete. In the next section, we provide new Montgomery-like formulas for complete twisted Edwards curves.

4 New Differential Additions

In this section, we provide new differential addition and doubling formulas for twisted Edwards. The mixed formulas have the cost $5\mathbf{M}+4\mathbf{S}+1\mathbf{D}$, $3\mathbf{M}+7\mathbf{S}+1\mathbf{D}$. In addition, we give mixed formulas with cost of $3\mathbf{M}+6\mathbf{S}+3\mathbf{D}$ for subfamily of twisted Edwards curves. These efficient and fast formulas are applicable for complete twisted Edwards in this subfamily. From the birational map between the twisted Edwards and Montgomery curve, we can use similar formulas for Montgomery curves.

4.1 Twisted Edwards

Here, we consider *twisted Edwards curves* $\mathbf{E}_{\mathrm{TE},a,d}$ and present new w-coordinates differential formulas.

We define the rational function w by $w(x,y) = d(xy)^2$. This function is well computed for all affine points on a twisted Edwards curves. Since $-(x,y) = (-x,y)$, for all points P on the curve, we have $w(P) = w(-P)$. Also, we have $w(\mathcal{O}) = 0$. For $i = 0,1,2,3,4$, let $w_i = w(P_i)$, where $P_i \in E_{a,d}$ with $w_0 = w(P_1 - P_2)$, $w_3 = w(P_1 + P_2)$ and $w_4 = w(2P_1)$. From the addition and doubling formulas for $\mathbf{E}_{\mathrm{TE},a,d}$ (1) with a straightforward calculation, we obtain the following differential addition formulas.

$$w_4 = \frac{4w_1((w_1+1)^2 - ew_1)}{(w_1^2-1)^2},\ w_3w_0 = \frac{(w_1-w_2)^2}{(w_1w_2-1)^2}. \tag{6}$$

where $e = 4a/d$.

Assume that w_0 is given as a field element, and the inputs w_1, w_2 are given as fractions W_1/Z_1, W_2/Z_2 and the outputs w_4, w_3 are given as fraction W_4/Z_4 and W_3/Z_3. From Eq. (6) the explicit projective formulas are given by

$$\begin{aligned} \frac{W_4}{Z_4} &= \frac{4W_1Z_1(\ (W_1+Z_1)^2 - eW_1Z_1)}{(W_1-Z_1)^2(W_1+Z_1)^2}, \\ \frac{W_3}{Z_3} &= \frac{Z_0\ (W_1Z_2 - W_2Z_1)^2}{W_0\ (W_1W_2 - Z_1Z_2)^2}. \end{aligned} \tag{7}$$

From the Eqs. (7), the cost of projective w-coordinates addition and doubling formulas is $6\mathbf{M}+4\mathbf{S}+1\mathbf{D}$. If we set $Z_0 = 1$, then the mixed projective w-coordinates differential addition and doubling formulas have the total cost $5\mathbf{M}+4\mathbf{S}+1\mathbf{D}$ as follows:

$$\begin{gathered} A_1 = (W_1+Z_1),\ B_1 = (W_1-Z_1),\ A_2 = (W_2+Z_2),\ B_2 = (W_2-Z_2), \\ C = A_1B_2,\ D = A_2B_1,\ \ E = A_1^2 - B_1^2, \\ W_4 = E(A_1^2 - (e/4)\ E),\ Z_4 = A_1^2B_1^2, \\ W_3 = (C-D)^2,\ Z_3 = w_0(C+D)^2. \end{gathered} \tag{8}$$

From (8), the costs of differential addition and doubling formulas are $3\mathbf{M}+2\mathbf{S}$ and $2\mathbf{M}+2\mathbf{S}+1\mathbf{D}$, respectively. And, the total cost of the mixed differential addition and doubling is $5\mathbf{M}+4\mathbf{S}+1\mathbf{D}$. In addition, the cost of following mixed differential addition and doubling formulas is $3\mathbf{M}+7\mathbf{S}+1\mathbf{D}$.

$$\begin{gathered} A_1=(W_1+Z_1),\ B_1=(W_1-Z_1),\ A_2=(W_2+Z_2),\ B_2=(W_2-Z_2),\\ C=A_1B_2,\ \ D=A_2B_1,\ \ E=A_1^2-B_1^2,\ F=(A_1^4+B_1^4)-E^2,\\ W_4=2(A_1^4-(e/4)E^2)-F,\ Z_4=F,\\ W_3=(C-D)^2,\ Z_3=w_0(C+D)^2. \end{gathered} \tag{9}$$

Furthermore, for the twisted Edwards curves $\mathbf{E}_{\mathrm{TE},a,d}$ with $\chi(e(e-4))=\chi(a(a-d))=1$, the cost of the following mixed differential addition and doubling formulas is $3\mathbf{M}+6\mathbf{S}+3\mathbf{D}$. Here we let $r^2=(e-4)/e$.

$$\begin{gathered} A_1=(W_1+Z_1),\ B_1=(W_1-Z_1),\ A_2=(W_2+Z_2), B_2=(W_2-Z_2),\\ C=A_1\ B_2,\ D=A_2\ B_1,\ H_1=(rA_1^2+B_1^2)^2,\ H_2=(rA_1^2-B_1^2)^2,\\ G=(H_1+H_2),\ K=(H_1-H_2),\ S=\tfrac{1}{r}K,\ T=rK,\\ W_4=2G-S-T,\ Z_4=T-S,\\ W_3=(C-D)^2,\ Z_3=w_0(C+D)^2. \end{gathered} \tag{10}$$

From differential addition and doubling formulas (10), the costs of differential addition and doubling are $3\mathbf{M}+2\mathbf{S}$, $4\mathbf{S}+3\mathbf{D}$ respectively. And, the total cost of the mixed differential addition and doubling formulas is $3\mathbf{M}+6\mathbf{S}+3\mathbf{D}$, where $2\mathbf{D}$ is the multiplication by the parameter r and one $\mathbf{D}$ is the multiplication by 1/r. So, if the parameter r is chosen to be small then the cost of mixed differential formulas is $3\mathbf{M}+6\mathbf{S}+1\mathbf{D}$.

Example 1. Let $p=2^{255}-19$. Let $a=1$ and $d=-204347024$. The twisted Edwards curve $\mathbf{E}_{\mathrm{TE},a,d}$ is a complete Edwards curve over $\mathbb{F}_p$ of order 8ℓ, where ℓ is the prime

$$\begin{aligned} \ell\ =\ & 723700557733226221397318656304299424082\\ & 231628998147646229476670936168466530 01. \end{aligned}$$

The cost of the mixed differential addition and doubling formulas (10) is $3\mathbf{M}+6\mathbf{S}+3\mathbf{D}$, where $2\mathbf{D}$ is the multiplication by the small constant $r=14295$ and one $\mathbf{D}$ is the multiplication by 1/r.

Remark 1. Let $\mathbf{E}_{\mathrm{TE},a,d}$ be a complete twisted Edwards curve over $\mathbb{F}_q$ with $\chi(d)=\chi(ad)=-1$. Then, $\mathbf{E}_{\mathrm{TE},a,d}$ has the four torsion subgroup as

$$\mathbf{E}_{\mathrm{TE},a,d}(\mathbb{F}_q)[4]=\{(0,1),(0,-1),(1/\sqrt{a},0),(-1/\sqrt{a},0)\}.$$

Then the coset of the point $P=(x,y)$ on the curve up to this subgroup equals

$$P+\mathbf{E}_{\mathrm{TE},a,d}(\mathbb{F}_q)[4]=\{(x,y),(-x,-y),(y\sqrt{a},-x\sqrt{a}),(-y/\sqrt{a},x\sqrt{a})\}.$$

We note that the proposed w-function has the property that $w(Q)=w(P)$ for all points Q in the coset of P.

As an alternative w-coordinate differential addition formulas, we define the rational function w by $w(x,y) = a(x/y)^2$. From the addition and doubling formulas for $\mathbf{E}_{\mathrm{TE},a,d}$ (1), we obtain the following differential addition formulas.

$$w_4 = \frac{4w_1((w_1+1)^2 - ew_1)}{(w_1^2-1)^2},\ w_3w_0 = \frac{(w_1-w_2)^2}{(w_1w_2-1)^2},$$

where $e = 4d/a$. Similarly, we obtain the same projective and mixed $w-$coordinates formulas as (7), (8), (9) and (10). This w-function is also invariant for the coset of a point up to the 4-torsion subgroup of the complete twisted Edwards curve $\mathbf{E}_{\mathrm{TE},a,d}$ over $\mathbb{F}_q$ with $\chi(a) = \chi(ad) = -1$.

Furthermore, for twisted Edwards curves where $\chi(ad) = 1$, we define another differential formulas by the rational function w by $w(x,y) = \sqrt{ad}\left(\frac{2xy}{ax^2+y^2}\right)^2$. Similarly, we obtain the following differential addition formulas.

$$w_4 = \frac{4w_1((w_1+1)^2 - ew_1)}{(w_1^2-1)^2},\ w_3w_0 = \frac{(w_1-w_2)^2}{(w_1w_2-1)^2},$$

where $e = 2 + (a+d)/\sqrt{ad}$. So, we have the same results for this w-coordinates by formulas (7), (8), (9) and (10). Note that, this w-function is invariant for the coset of a point up to the full 2-torsion subgroup of the incomplete twisted Edwards curve $\mathbf{E}_{\mathrm{TE},a,d}$ over $\mathbb{F}_q$ with $\chi(ad) = 1$.

4.2 Montgomery Curves

Now, we consider the Montgomery curves. Note that above w-coordinates differential addition and doubling formulas for twisted Edwards curves can be applied for Montgomery curve using the birational maps between these two curves (5). Furthermore, from formulas (9) and (10), we give the mixed x-coordinates differential addition and doubling formulas for Montgomery curves with cost of $3\mathbf{M} + 7\mathbf{S} + 1\mathbf{D}$ and $3\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$.

We recall [15], that for the Montgomery curve $\mathbf{E}_{\mathbf{M},A,B}$ with the rational function $w(x,y) = x$, we have the following differential addition formulas.

$$w_4 = \frac{(w_1^2-1)^2}{4w_1((w_1+1)^2 - ew_1)},\ w_3w_0 = \frac{(w_1w_2-1)^2}{(w_1-w_2)^2},$$

where $e = 2 - A$. In other words, the x-coordinates formulas for Montgomery curves and above w coordinates formulas (6) for twisted Edwards curves are inverse of each other. It means the projective formulas for Montgomery curves is obtained by the projective formulas (7) only by swapping the role of W and Z. Therefore, from formulas (9) we have the following formulas with cost of $3\mathbf{M} + 7\mathbf{S} + 1\mathbf{D}$

$$\begin{array}{c} A_1 = (W_1+Z_1),\ B_1 = (W_1-Z_1),\ A_2 = (W_2+Z_2),\ B_2 = (W_2-Z_2), \\ C = A_1B_2,\ \ D = A_2B_1,\ \ E = A_1^2 - B_1^2,\ F = (A_1^4 + B_1^4) - E^2, \\ W_4 = F,\ Z_4 = 2(A_1^4 - (e/4)E^2) - F, \\ W_3 = w_0(C+D)^2,\ Z_3 = (C-D)^2. \end{array} \tag{11}$$

and from formulas (10), we obtain the formulas with cost of $3\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$ as follows.

$$\begin{gathered} A_1 = (W_1 + Z_1),\ B_1 = (W_1 - Z_1),\ A_2 = (W_2 + Z_2), B_2 = (W_2 - Z_2), \\ C = A_1\ B_2,\ D = A_2\ B_1,\ H_1 = (rA_1^2 + B_1^2)^2,\ H_2 = (rA_1^2 - B_1^2)^2, \\ G = (H_1 + H_2),\ K = (H_1 - H_2),\ S = \tfrac{1}{r}K,\ T = rK, \\ W_4 = T - S,\ Z_4 = 2G - S - T, \\ W_3 = w_0(C + D)^2,\ Z_3 = (C - D)^2. \end{gathered} \tag{12}$$

5 Concluding Remarks

The known Montgomery ladder differential addition formulas for elliptic curves over a finite field are not complete; they work for all input points P except for the case where $w(P)$ equals $(1 : 0)$ or $(0 : 1)$. However, the Montgomery ladder algorithm works perfectly in cryptographic applications, since the order of base point P should be a large prime number. The cost of the Montgomery-like formulas is $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ if the base point P is affine. We believe, this record can be obtained for any form of elliptic curve with group order divisible by 4 by a suitable rational function. This includes the family of Jacobi curves.

Our proposed Montgomery-like formulas for twisted Edwards curves are improved in terms of efficiency and speed. They are almost complete formulas if the curve parameters are chosen carefully. The mixed formulas are provided for twisted Edwards curves with the cost of $3\mathbf{M} + 7\mathbf{S} + 1\mathbf{D}$. Also, faster mixed formulas are presented for a subfamily of twisted Edwards curves with the cost of $3\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$ which gives further speedup if the parameters are chosen to be small.

In Table 1, we compare our new differential addition formulas with the known formulas for other forms of elliptic curves. Notice, the fast and efficient presented

Table 1. Cost of differential addition and doubling for families of elliptic curves in odd characteristic

Model	Projective differential	Mixed differential
Montgomery [15]	$6\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$	$5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$
This work (11)	$4\mathbf{M} + 7\mathbf{S} + 1\mathbf{D}$	$3\mathbf{M} + 7\mathbf{S} + 1\mathbf{D}$
This work (12)	$4\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$	$3\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$
Kummer curve [9]	$4\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$	$3\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$
Edwards curve $\mathbf{E}_{\mathrm{BL},d}$		
$(d = r^2, w = ry)$ [5]	$4\mathbf{M} + 6\mathbf{S} + 5\mathbf{D}$	$3\mathbf{M} + 6\mathbf{S} + 5\mathbf{D}$
$(d = r^2, w = ry^2)$ [5]	$4\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$	$3\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$
Jacobi quartic [10]	$6\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$	$5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$
Twisted edwards		
This work (8)	$6\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$	$5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$
This work (9)	$4\mathbf{M} + 7\mathbf{S} + 1\mathbf{D}$	$3\mathbf{M} + 7\mathbf{S} + 1\mathbf{D}$
This work (10)	$4\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$	$3\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$

formulas by Gaudry-Lubicz [9] and Bernstein-Lange [5] are given with the cost of $4\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$, and $3\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$ if the base point is affine, only for subfamily of elliptic curves with 3 points of order 2. Our formulas have the same costs and presented for a subfamily of twisted Edwards with a point of order 4 which includes the complete twisted Edwards curves therein.

For complete twisted Edwards curves, the proposed w functions are invariant in the coset of a point P with respect to the subgroup of $\mathbb{F}_q$-rational points with order 4. And, for incomplete twisted Edwards curves the suggested w function is invariant in the coset of a point P up to the subgroup of full 2-torsion points. For future works, we are going to investigate the use of these differential addition formulas along with the eliminating cofactors technique through point compression [11]. Computing the full point representation at the end of Montgomery ladder is an alternative question which is useful for cryptographic applications that need the full version of the scalar multiplication algorithm.

Acknowledgment. The authors would like to thank anonymous reviewers for their useful comments. This research was in part supported by a grant from IPM (No. 95050416).

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). doi:10.1007/978-3-540-68164-9_26
2. 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). doi:10.1007/978-3-540-76900-2_3
3. Bernstein, D.J., Lange, T., Rezaeian Farashahi, R.: Binary edwards curves. In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 244–265. Springer, Heidelberg (2008). doi:10.1007/978-3-540-85053-3_16
4. Bernstein, D., Lange, T.: A complete set of addition laws for incomplete Edwards curves. J. Number Theory **131**, 858–872 (2011)
5. Bernstein, D., Lange, T.: Explicit-formulas database. http://www.hyperelliptic.org/EFD/
6. Castryck, W., Galbraith, S., Farashahi, R.: Efficient arithmetic on elliptic curves using a mixed Edwards Montgomery representation. https://eprint.iacr.org/2008/218.pdf
7. Edwards, H.M.: A normal form for elliptic curves. Bull. Amer. Math. Soc. **44**, 393–422 (2007)
8. Rezaeian Farashahi, R., Hosseini, S.G.: Differential addition on binary elliptic curves. In: Duquesne, S., Petkova-Nikova, S. (eds.) WAIFI 2016. LNCS, vol. 10064, pp. 21–35. Springer, Cham (2016). doi:10.1007/978-3-319-55227-9_2
9. Gaudry P. and Lubicz D.: The arithmetic of characteristic 2 Kummer surface. Finite Fields Appl. 15, 246–260 (2009)
10. Gu, H., Gu, D., Xie, W.: Differential addition on Jacobi quartic curves Conference: ICT and Energy Efficiency and Workshop on Information Theory and Security (CIICT 2012)

11. Hamburg, M.: Decaf: eliminating cofactors through point compression. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 705–723. Springer, Heidelberg (2015). doi:10.1007/978-3-662-47989-6_34
12. 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). doi:10.1007/978-3-540-89255-7_20
13. Koblitz, N.: Elliptic curve cryptosystems. Math. Comp. **48**(177), 203–209 (1987)
14. Miller, V.S.: Use of elliptic curves in cryptography. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 417–426. Springer, Heidelberg (1986). doi:10.1007/3-540-39799-X_31
15. Montgomery, P.L.: Speeding the Pollard and elliptic curve methods of factorization. Math. Comp. **48**(177), 243–264 (1987)
16. Silverman, J.H.: The Arithmetic of Elliptic Curves. Springer, Berlin (1995)
17. Washington, D.C.: Elliptic Curves: Number Theory and Cryptography, 2nd edn. CRC Press, Boca Raton (2008)