Differential Addition on Binary Elliptic Curves

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

[1] Department of Mathematical Sciences, Isfahan University of Technology, Isfahan 84156-83111, 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 extremely fast 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 various forms of elliptic curves over binary fields. The formulas are provided for *binary Edwards*, *binary Hessian* and *binary Huff* elliptic curves with cost of $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ 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. This paper also presents, new *complete* differential addition formulas for *binary Edwards* curves with cost of $5\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$.

Keywords: Elliptic curves · Binary Edwards curves · Hessian curves · Binary Huff curves · Differential addition

1 Introduction

An elliptic curve E over a field $\mathbb{F}$ can be 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 $\mathbb{F}$. There are many other ways to represent elliptic curves such as Legendre equation, cubic equations, quartic equations and intersection of two quadratic surfaces [18]. The use of elliptic curves over finite fields based on their finite groups in cryptography (ECC) was independently proposed in the mid 1980s by Koblitz [11] and Miler [14]. Since the introduction of elliptic curve cryptography many proposals have been made to speed up the group arithmetic. Efficient arithmetic (addition, doubling, tripling and scalar multiplication) on elliptic curves over finite fields is the core requirement of elliptic curve cryptography. Several forms of elliptic curves over finite fields with several coordinate systems have been studied to improve the efficiency and the speed of the arithmetic on the group law.

S. Duquesne and S. Petkova-Nikova (Eds.): WAIFI 2016, LNCS 10064, pp. 21–35, 2016.
DOI: 10.1007/978-3-319-55227-9_2

Elliptic curves over binary finite fields are interesting particularly for hardware implementations. Every ordinary elliptic curve over the binary finite filed $\mathbb{F}_{2^m}$ can be represented in the Weierstraß form

$$y^2 + xy = x^3 + ax^2 + b,$$

where $a, b \in \mathbb{F}_{2^m}$ and $b \neq 0$. There are alternative ways to represent binary elliptic curves such as binary Hessian [1,5,6,17], binary Edwards [3], binary Huff curves [9] and binary μ_4-normal forms [12].

The scalar multiplication is the most important operation of elliptic curve cryptography. 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 integer k. The scalar multiplication can be performed by a sequence of point additions and point doublings. Speed and efficiency are the main factors to be considered in the correct implementing of scalar multiplication. Moreover, the implementations should be performed in a way to be resistant against passive and active side channel attacks. There are several mathematical countermeasures proposed for preventing these attacks. Simple side-channel attacks get information from a single scalar multiplication when the power trace reveal distinctive key dependent patterns. The main idea of the countermeasure against simple side-channel attacks is to make the computation uniform. And the main solutions are making indistinguishable point addition and point doubling, using double and add always method, using window method or applying the Montgomery technique.

The Montgomery method [15,16] is introduced for scalar multiplication of points for a special type of curve in large characteristic. This method has been extended to other form of elliptic curves and to binary elliptic curves [8]. The Montgomery scalar multiplication is known also as Montgomery ladder. In the Montgomery ladder, for each bit of the scalar both doubling and addition are performed, so this prevents the computation secure against simple power analysis. Also this method is not subject to fault attacks.

The countermeasures for some other passive or active attacks are to insert suitable randomness to the key and also to the base point of the scalar multiplication. Therefore, here the scalar key may be larger than the order of the base point, which makes some exceptional cases like the point at infinity in the computation of the Montgomery ladder. Thus, obtaining *complete* or *almost complete* formulas for addition and doubling makes the ladder performs completely.

In this paper we present fast explicit formulas for differential additions and doublings on well known binary elliptic curves such as binary Edwards, binary Hessian and binary Huff curves.

2 Differential Addition

A Montgomery curve over a field $\mathbb{F}$ of characteristic different from 2 is given by the equation

$$bY^2Z = X^3 + aX^2Z + XZ^2,$$

where $a,\ b$ are elements of $\mathbb{F}$ with $b(a^2-4) \neq 0$. The Montgomery ladder for scalar multiplication is performed by a sequence of simultaneous point addition and doubling, which makes this method interesting against side-channel attacks. In Montgomery curves, the basic computation in a each step is done without the Y coordinate, i.e., the technique involves special formulas for addition and doubling that relies on only the X and Z coordinates of a point in projective form. Also, the Y coordinate of the output point can be derived from the X and Z coordinates.

In general, the basic computation in a each step of the Montgomery ladder is differential addition and doubling. That is for given points P_1, P_2 and $P_1 - P_2$ on elliptic curve E over $\mathbb{F}_q$ to compute $P_1 + P_2$ and $2P_1$. The idea is extended by a suitable rational function on the elliptic curve. Suppose w is a rational function defined over an elliptic curve E over a finite field $\mathbb{F}_q$. The function w is given by fraction of polynomials in the coordinate ring of E over $\mathbb{F}_q$. Let $w(P) = w(-P)$ for any point P on $E(\mathbb{F}_q)$. Then the w-coordinate *differential addition* and *doubling* means to compute $w(2P_1)$ and $w(P_1+P_2)$ from given values $w(P_1)$, $w(P_2)$ and $w(P_1-P_2)$, where $P_1,\ P_2$ are points on $E(\mathbb{F}_q)$. For Montgomery curves the function w is x, where $w(P)$ equals the x-coordinate of the point P. Since field inversion is costly, practically computations are performed where points are represented in projective coordinates. Therefore, when 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 $(1 : 0)$. The projective w-coordinate differential addition and doubling (dADD) algorithm is given in Algorithm 1. Notice, in Algorithm 1, the given input values $w(P_1)$, $w(P_2)$ and $w(P_0) = w(P_1 - P_2)$ are represented by W_i/Z_i where $i = 1, 2, 0$ respectively. Then $w(P_1 + P_2)$, i.e. the w-coordinate differential addition, is given by $\frac{f_a}{g_a}$ with some homogenous polynomials f_a and g_a in variables $W_i,\ Z_i$, where $i = 0, 1, 2$. Also, $w(2P_1)$ is given by $\frac{f_d}{g_d}$, where f_d and g_d are homogenous polynomials with variables $W_1,\ Z_1$.

Algorithm 1. Projective w-coordinate dADD

Input : $E/F_q,\ w : E(\mathbb{F}_q) \to \mathbb{P}(\mathbb{F}_q)$, ▷ The elliptic curve E over $\mathbb{F}_q$
$(W_i : Z_i) = w(P_i),\ i = 0, 1, 2.$ ▷ $w(P_0) = w(P_1 - P_2)$
Output : $(W_i : Z_i) = w(P_i),\ i = 3, 4.$ ▷ $w(P_3) = w(P_1 + P_2),\ w(P_4) = w(2P_1)$

function DADD($(W_0 : Z_0),\ (W_1 : Z_1),\ (W_2 : Z_2)$)
  $W_3 = f_a(W_0, Z_0, W_1, Z_1, W_2, Z_2)$ ▷ Differential addition computation
  $Z_3 = g_a(W_0, Z_0, W_1, Z_1, W_2, Z_2)$
  $W_4 = f_d(W_1, Z_1)$ ▷ Doubling computation
  $Z_4 = g_d(W_1, Z_1)$
  return $((W_4 : Z_4),\ (W_3 : Z_3))$ ▷ The differential addition and doubling
end function

The Montgomery scalar multiplication based on a projective w-coordinate dADD is given in Algorithm 2. Notice, the base point P can be considered such that one of the coordinates of $w(P)$ equals 1, which makes less field operation computation in each step of the ladder.

Algorithm 2. The Montgomery scalar multiplication

Input : $E/F_q,\ w : E(\mathbb{F}_q) \to \mathbb{P}(\mathbb{F}_q)$, ▷ The elliptic curve E over $\mathbb{F}_q$
Projective w-coordinate dADD funtion,
$P \in E(\mathbb{F}_q),\ k = (k_{m-1}, \cdots, k_1, k_0)$ ▷ k is a positive integer, $k_{m-1} = 1$
$(W_0 : Z_0) := w(P),\ (W_1 : Z_1) := w(P),\ (W_2 : Z_2) := w(2P)$.
Output : $w(kP)$

1: **for** $i := m - 2$ **down to** 0 **do**
2: **if** $k_i = 0$ **then**
3: $((W_1 : Z_1), (W_2 : Z_2)) := dADD((W_0 : Z_0), (W_1 : Z_1), (W_2 : Z_2))$
4: **else**
5: $((W_2 : Z_2), (W_1 : Z_1)) := dADD((W_0 : Z_0), (W_2 : Z_2), (W_1 : Z_1))$
6: **end if**
7: **end for**
8: **return** $(W_1 : Z_1),\ (W_2 : Z_2)$ ▷ The differential addition and doubling

Note that if there are some exceptional points where the function dADD is not computed correctly, then the Montgomery ladder does not work properly. We say that the differential w-coordinate is *complete* if the Algorithm 1 works for any input without any exception. We also say that the function dADD is *almost complete* if the Algorithm 1 works 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 $E(\mathbb{F}_q)$. Therefore, for the complete function dADD the Montgomery ladder is performed without any problem for any input. Moreover, for the almost complete function dADD the Montgomery ladder works for any base point P except for the points where $w(P)$ equals $w(\mathcal{O})$. Notice, the almost complete function is also suitable for cryptographic application.

In this paper, we concentrate on differential addition on binary elliptic curves. Let E be a binary elliptic curve over $\mathbb{F}_{2^m}$ in Weiersrasß form

$$y^2 + xy = x^3 + ax^2 + b,$$

where $a,\ b$ are in $\mathbb{F}_{2^m}$. Lopez and Dahab [13] presented the projective formulas for the addition and doubling of points on E. And, they generalized the Montgomery's idea to binary curves. Algorithm 3 provides the Lopez and Dahab differential x-coordinate on elliptic curve E over $\mathbb{F}_{2^m}$.

If we assume $Z_0 = 1$, then the Lopez and Dahab formulas are computed using $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$. Here, a multiplication in $\mathbb{F}_q$ costs one $\mathbf{M}$ and a squaring costs one $\mathbf{S}$. Also the cost of field multiplication by a parameter (as a constant) is denoted by $\mathbf{D}$.

We note, that the point at infinity on the binary elliptic curve E over $\mathbb{F}_{2^m}$ is $\mathcal{O} = (0 : 1 : 0)$ and $x(\mathcal{O})$ is represented by $(1 : 0)$. One can easily check that the projective x-coordinate formulas work for all inputs if $Z_0 \neq 0$, that is where $P_0 \neq \mathcal{O}$. In other words the formulas are almost complete and the Montgomery ladder works for all inputs if the base point is not the point at infinity. So, the

Algorithm 3. Lopez and Dahab projective x-coordinate dADD

Input : $E/F_q : y^2 + xy = x^3 + ax^2 + b$ ▷ The elliptic curve E over $\mathbb{F}_{2^m}$
$(X_i : Z_i) = x(P_i),\ i = 0, 1, 2.$ ▷ $x(P_0) = x(P_1 - P_2)$
Output : $(X_i : Z_i) = x(P_i),\ i = 3, 4.$ ▷ $x(P_3) = x(P_1 + P_2),\ x(P_4) = x(2P_1)$

1: **function** DADD($(X_0 : Z_0)$, $(X_1 : Z_1)$, $(X_2 : Z_2)$)
2: $X_3 = X_0\ (X_1Z_2 + X_2Z_1)^2 + Z_0\ (X_1Z_1X_2Z_2)$
3: $Z_3 = Z_0\ (X_1Z_2 + X_2Z_1)^2$
4: $X_4 = (X_1^4 + bZ_1^4)$
5: $Z_4 = X_1^2\ Z_1^2$
6: **return** $((X_4 : Z_4),\ (X_3 : Z_3))$ ▷ The differential addition and doubling
7: **end function**

Montgomery ladder can be modified as Algorithm 4. Here there is no need to assume that the bit k_{m-1} of the integer k is equal to '1'. Also, there is no need to precompute $2P$ from the base point P. Moreover, the ladder works properly even if the integer k is bigger than the order of the base point P. So, for Lopez and Dahab formulas, one can use random scalar k as a countermeasure to protect against differential power analysis attack.

Algorithm 4. The modified Montgomery scalar multiplication

Input : $E/F_q : y^2 + xy = x^3 + ax^2 + b$ ▷ The elliptic curve E over $\mathbb{F}_q$
$P = (x : y : z) \in E(\mathbb{F}_q)$ ▷ $P \neq \mathcal{O} = (0 : 1 : 0)$
$k = (k_{m-1}, \cdots, k_1, k_0)$ ▷ $0 \leq k \in \mathbb{Z}$
$(X_0 : Z_0) := (x : z),\ (X_1 : Z_1) := (1 : 0),\ (X_2 : Z_2) := (x : z).$
Output : $w(kP)$

1: **for** $i := m - 1$ **down to** 0 **do**
2: **if** $k_i = 0$ **then**
3: $((X_1 : Z_1), (X_2 : Z_2)) := dADD((X_0 : Z_0), (X_1 : Z_1), (X_2 : Z_2))$
4: **else**
5: $((X_2 : Z_2), (X_1 : Z_1)) := dADD((X_0 : Z_0), (X_2 : Z_2), (X_1 : Z_1))$
6: **end if**
7: **end for**
8: **return** $(X_1 : Z_1),\ (X_2 : Z_2)$ ▷ The differential addition and doubling

3 Binary Edwards Curves

In this section we review the *Binary Edwards curve* [3] and propose new differential addition and doubling formulas.

Let d_1, d_2 be elements of $\mathbb{F}_{2^m}$ such that $d_1 \neq 0$ and $d_2 \neq d_1(d_1 + 1)$. The binary Edwards curve with parameters d_1 and d_2 is given by the equation

$$E_{B,d_1,d_2} : d_1(x + y) + d_2(x + y)^2 = xy(x + 1)(y + 1). \quad (1)$$

The curve is symmetric in $x,\ y$ and the negation of (x, y) is (y, x). This curve has two points $(0, 0)$ and $(1, 1)$ which are invariant under the negation law. The point $(0, 0)$ is the neutral element of the addition law and the point $(1, 1)$ has order 2. We denote the point $(0, 0)$ by $\mathcal{O}$.

The binary Edwards curve E_{B,d_1,d_2} is birationally equivalent to the ordinary elliptic curve in Weierstraß form

$$v^2 + uv = u^3 + au^2 + b,$$

where a, b are in $\mathbb{F}_{2^m}$ with $b \neq 0$. The map $(x, y) \longmapsto (u, v)$ defined by

$$u = ((d_1^3 + d_1^2 + d_1d_2)(x + y))/(xy + d_1(x + y))$$

$$v = (d_1^3 + d_1^2 + d_1d_2)(d_1 + 1 + x/(xy + d_1(x + y))$$

is a birational equivalence form E_{B,d_1,d_2} to the elliptic curve

$$v^2 + uv = u^3 + (d_1^2 + d_2)u^2 + d_1^4(d_1^4 + d1^2 + d_2).$$

Affine Addition. The sum of two points (x_1, y_1) and (x_2, y_2) on E_{B,d_1,d_2} is the point (x_3, y_3) defined as follows:

$$x_3 = \frac{d_1(x_1 + x_2) + d_2(x_1 + y_1)(x_2 + y_2) + (x_1 + x_1^2)(x_2(y_1 + y_2 + 1) + y_1y_2)}{d_1 + (x_1 + x_1^2)(x_2 + y_2)}, \tag{2}$$

$$y_3 = \frac{d_1(y_1 + y_2) + d_2(x_1 + y_1)(x_2 + y_2) + (y_1 + y_1^2)(y_2(x_1 + x_2 + 1) + x_1x_2)}{d_1 + (y_1 + y_1^2)(x_2 + y_2)}.$$

Affine Doubling. The doubling of point (x_1, y_1) is the point (x_4, y_4) defined as follows:

$$x_4 = 1 + \frac{d_1 + d_2(x_1^2 + y_1^2) + y_1^2 + y_1^4}{d_1 + (x_1^2 + y_1^2) + d_2/d_1(x_1^4 + y_1^4)}, \tag{3}$$

$$y_4 = 1 + \frac{d_1 + d_2(x_1^2 + y_1^2) + x_1^2 + x_1^4}{d_1 + (x_1^2 + y_1^2) + d_2/d_1(x_1^4 + y_1^4)}.$$

Differential Addition. Bernstein, Lange and Farashahi in [3] proposed the differential addition and doubling formulas for binary Edwards curve. Assume that $P = (x_1, y_1),\ Q = (x_2, y_2)$ are points on E_{B,d_1,d_2} and $Q - P = (x_0, y_0),\ Q + P = (x_3, y_3)$ and $2P = (x_4, y_4)$. They considered w-function as $w(x_i, y_i) = x_i + y_i$ and obtained the following complete formulas for differential addition:

$$w_4 = \frac{w_1^2 + w_1^4}{d_1 + w_1^2 + (d_2/d_1)w_1^4},$$

$$w_3 + w_0 = \frac{d_1w_1w_2(1 + w_1)(1 + w_2)}{d_1^2 + w_1w_2(d_1(1 + w_1 + w_2) + d_2(w_1w_2))},$$

$$w_3w_0 = \frac{d_1^2(w_1^2 + w_2^2)}{d_1^2 + w_1w_2(d_1(1 + w_1 + w_2) + d_2(w_1w_2))}.$$

Assume that w_0 is given as a field element, and $w_1,\ w_2$ are given as fractions W_1/Z_1, W_2/Z_2 and $w_4,\ w_3$ are outputs as fractions W_4/Z_4 and W_3/Z_3. Then, the mixed projective w-coordinate differential addition and doubling formulas are given as follows.

$$A = W_1(W_1 + Z_1), \quad B = W_2(W_2 + Z_2), \quad C = Z_1Z_2, \quad D = W_1W_2, \quad E = AB,$$
$$F = E + (\sqrt{d_1}C + \sqrt{d_2/d_1 + 1}D)^2,$$
$$W_4 = A^2, \quad Z_4 = W_4 + ((\sqrt[4]{d_1}Z_1 + \sqrt[4]{d_2/d_1 + 1}W_1)^2)^2,$$
$$Z_3 = F,\ W_3 = E + w_0F.$$

From above formulas, for the general case $d_1 \neq d_2$, the cost of differential addition is $6\mathbf{M}+1\mathbf{S}+2\mathbf{D}$ and the cost of doubling is $1\mathbf{M}+3\mathbf{S}+2\mathbf{D}$. And the total cost is $6\mathbf{M} + 4\mathbf{S} + 4\mathbf{D}$. If $d_1 = d_2$ the total cost is $5\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$. Recently Kim, Lee and Negre [10] for the case $d_1 = d_2$, by using the co-Z trick improved the differential addition formulas by $1\mathbf{D}$ and obtained almost complete differential addition formulas with cost of $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$.

New Differential Addition. In this section, we consider *binary Edwards curves* in general form and present two new w-coordinates differential formulas where one of this formulas is complete and the other is almost complete.

Let define the rational function w by $w(x, y) = (x + y)/(d_1(x + y + 1))$. The function is well computed for all affine points on a binary Edwards curve except for the points (x, y) where $x + y = 1$. Since $-(x, y) = (y, x)$, for all points P on the curve, we have $w(P) = w(-P)$. Also, we have $w(\mathcal{O}) = 0$. As before, for $i = 0, 1, 2, 3, 4$, let $w_i = w(P_i)$, where $P_i \in E_{B,d_1,d_2}(\mathbb{F}_{2^m})$ with $w(P_0) = w(P_1 - P_2)$, $w(P_3) = w(P_1 + P_2)$ and $w(P_4) = w(2P_1)$. From the addition formula (2), with a straightforward calculation, we obtain the following differential addition formulas.

$$w_3 + w_0 = \frac{w_1w_2}{d_1^2(d_1^2 + d_1 + d_2)w_1^2w_2^2 + 1}, \tag{4}$$

$$w_3w_0 = \frac{w_1^2 + w_2^2}{d_1^2(d_1^2 + d_1 + d_2)w_1^2w_2^2 + 1}. \tag{5}$$

Also, from the doubling formula (3) and some calculations we obtain

$$w_4 = \frac{w_1^2}{d_1^2(d_1^2 + d_1 + d_2)w_1^4 + 1}. \tag{6}$$

We recall [3] that the binary Edwards curve E_{B,d_1,d_2} over $\mathbb{F}_{2^m}$ is complete if $\mathrm{Tr}(d_2) = 1$. Here Tr is the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. Moreover, if $\mathrm{Tr}(d_1) = 0$ then there is no point (x, y) on the curve with $x + y + 1 = 0$. Since, if there is a point (x, y) with $x + y + 1 = 0$ on the curve E_{B,d_1,d_2} with $\mathrm{Tr}(d_2) = 1$ and $\mathrm{Tr}(d_1) = 0$, then by the curve Eq. (1), we have $x^4 + x^2 + d_1 + d_2 = 0$. Then,

$$\begin{aligned}\mathrm{Tr}(0) &= \mathrm{Tr}(x^4 + x^2 + d_1 + d_2)\\ &= \mathrm{Tr}(x^4) + \mathrm{Tr}(x^2) + \mathrm{Tr}(d_1) + \mathrm{Tr}(d_2)\\ &= \mathrm{Tr}(x^2) + \mathrm{Tr}(x^2) + 0 + 1 = 1,\end{aligned}$$

which is a contradiction. Therefore, the function w is well defined for all affine points on the complete binary Edwards curve E_{B,d_1,d_2} with $\mathrm{Tr}(d_1) = 0$.

Notice, the set of affine $\mathbb{F}_{2^m}$-rational points of the complete binary Edwards curve E_{B,d_1,d_2} is an abelian group. And, with the condition $\mathrm{Tr}(d_1) = 0$, for any point $P = (x, y)$ on the curve, the value $w(P)$ is well computed and belongs to $\mathbb{F}_{2^m}$. By the Eqs. (4) and (6) we have

$$(w_3 + w_0)(d_1^2(d_1^2 + d_1 + d_2)w_1^2w_2^2 + 1) = w_1w_2 \ ,$$
$$w_4(d_1^2(d_1^2 + d_1 + d_2)w_1^4 + 1) = w_1^2.$$

So, we see that if $\mathrm{Tr}(d_1) = 0$ then the denominators of Eqs. (4) and (6) never equal zero. In other words, above w-coordinates differential addition and doubling formulas for complete binary Edwards curve are complete where $\mathrm{Tr}(d_1) = 0$.

For further speedup, we can divide the Eq. (4) by Eq. (5) and obtain the following faster formula.

$$\frac{1}{w_3} + \frac{1}{w_0} = \frac{w_1w_2}{(w_1 + w_2)^2}. \tag{7}$$

Cost of Projective w-Coordinates. Using Eqs. (4) and (6), we obtained new and complete differential addition formulas for general *binary Edwards curves* with the total cost of $5\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$ where the difference of input points is affine. Then, by using the Eqs. (6) and (7) we obtain, new and fast, but almost complete, differential addition formulas in mixed projective coordinates with the total cost of $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$. Thus, the total cost of differential addition and doubling in general binary Edwards curves is reduced from $6\mathbf{M} + 4\mathbf{S} + 4\mathbf{D}$ to $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$.

As before assume that w_0 is given as a field element, and $w_1,\ w_2$ are given as fractions W_1/Z_1, W_2/Z_2 and $w_4,\ w_3$ are to be output as fraction W_4/Z_4 and W_3/Z_3. From Eq. (6) the explicit doubling formula is given by

$$\frac{W_4}{Z_4} = \frac{W_1^2Z_1^2}{(d_1^4 + d_1^3 + d_1^2d_2)W_1^4 + Z_1^4} \tag{8}$$

and from Eq. (4) the explicit addition formula is given by

$$\frac{W_3}{Z_3} = \frac{W_0((d_1^4 + d_1^3 + d_1^2d_2)\ W_1^2W_2^2 + Z_1^2Z_2^2) + Z_0(W_1W_2Z_1Z_2)}{Z_0((d_1^4 + d_1^3 + d_1^2d_2)\ W_1^2W_2^2 + Z_1^2Z_2^2))}. \tag{9}$$

So, from the Eqs. (8) and (9), the cost of projective w-coordinates is $7\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$. If we set $Z_0 = 1$, then the mixed projective w-coordinates differential addition and doubling formulas have the total cost $5\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$ as follows.

$$\begin{aligned} &A = W_1Z_1, \quad B = W_1W_2, \quad C = Z_1Z_2, \\ &W_4 = A^2, \quad Z_4 = (\sqrt[4]{(d_1^4 + d_1^3 + d_1^2d_2)}W_1 + Z_1)^4, \\ &Z_3 = (\sqrt{(d_1^4 + d_1^3 + d_1^2d_2)}B + C)^2, \quad W_3 = BC + w_0Z_3. \end{aligned} \tag{10}$$

From Eq. (7), we also obtain the following explicit projective differential addition formulas.

$$\frac{Z_3}{W_3} = \frac{Z_0(W_1Z_2 + W_2Z_1)^2 + W_0(W_1Z_2W_2Z_1)}{W_0(W_1Z_2 + W_2Z_1)^2}. \tag{11}$$

Thus, by Eqs. (8) and (11), the cost of projective w-coordinates is $7\mathbf{M}+4\mathbf{S}+2\mathbf{D}$. If we set $W_0 = 1$ and using the mixed projective coordinates we have the following formulas for computing differential addition.

$$\begin{aligned} &A = W_1Z_1, \quad B = W_1Z_2, \quad C = W_2Z_1, \\ &W_4 = A^2, \quad Z_4 = (\sqrt[4]{(d_1^4 + d_1^3 + d_1^2d_2)}W_1 + Z_1)^4, \\ &W_3 = (B + C)^2, \quad Z_3 = BC + z_0W_3. \end{aligned} \tag{12}$$

From differential addition and doubling formulas (12), the costs of differential addition and doubling are $4\mathbf{M} + 1\mathbf{S}$, $1\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$ respectively. And, the total cost is $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$.

The binary Edwards curve E_{B,d_1,d_2}, has the neutral element $\mathcal{O}$ represented by w-coordinate as $(0 : 1)$. For the complete binary Edwards curve E_{B,d_1,d_2} with $\mathrm{Tr}(d_1) = 0$, any point P on the curve can be represented by $(w(P) : 1)$. In other words, for any w-coordinate representation of the point P by $(W : Z)$ we have $Z \neq 0$. So, from the completeness of the affine w-coordinates differential addition and doubling formulas for complete binary Edwards curve with $\mathrm{Tr}(d_1) = 0$, we deduce that the projective w-coordinates differential addition and doubling formulas (8) and (9) are also complete. The mixed projective formulas (10) have the cost of $5\mathbf{M}+4\mathbf{S}+2\mathbf{D}$. Furthermore, the projective w-coordinates differential addition and doubling formulas (8) and (11) are almost complete; the exceptional cases are points P_0 where $w(P_0) = w(\mathcal{O})$. The mixed projective formulas (12) have the cost of $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$.

4 Binary Hessian Curve

A *Hessian curve* over a field $\mathbb{F}_{2^m}$ is given by the cubic equation

$$\mathrm{H}_d : \; x^3 + y^3 + 1 + dxy = 0\,,$$

for some $d \in \mathbb{F}_{2^m}$ with $d^3 \neq 27$ [5]. The family is extended to the family of generalized Hessian [5] or twisted Hessian curves [1]. A generalized Hessian curve $\mathrm{H}_{c,d}$ over $\mathbb{F}_{2^m}$ is defined by the equation

$$\mathrm{H}_{c,d} : x^3 + y^3 + c + dxy = 0,$$

where c, d are elements of $\mathbb{F}_{2^m}$ such that $c \neq 0$ and $d^3 \neq 27c$. The projective closure of the curve $\mathrm{H}_{c,d}$ is

$$\mathbf{H}_{c,d} : \; X^3 + Y^3 + cZ^3 = dXYZ.$$

It has the points $(1 : \omega : 0)$ with $\omega^3 = 1$ at infinity. The neutral element of the group of $\mathbb{F}_{2^m}$-rational points of $\mathbf{H}_{c,d}$ is the point at infinity $(1 : 1 : 0)$ that is denoted by $\mathcal{O}$. And, the negation of point $(X : Y : Z)$ is $(Y : X : Z)$.

Affine Addition. The sum of two different points (x_1, y_1), (x_2, y_2) on $\mathrm{H}_{c,d}$ is the point (x_3, y_3) given by

$$x_3 = \frac{{y_1}^2 x_2 + {y_2}^2 x_1}{x_2 y_2 + x_1 y_1} \quad \text{and} \quad y_3 = \frac{{x_1}^2 y_2 + {x_2}^2 y_1}{x_2 y_2 + x_1 y_1}.$$

Affine Doubling. The doubling of the point (x_1, y_1) on $\mathrm{H}_{c,d}$ is the point (x_4, y_4) given by

$$x_4 = \frac{y_1(c + {x_1}^3)}{{x_1}^3 + {y_1}^3} \quad \text{and} \quad y_4 = \frac{x_1(c + {y_1}^3)}{{x_1}^3 + {y_1}^3}.$$

Differential Addition. Farashahi and Joye in [5] adapted differential addition formulas for the binary curve $\mathbf{H}_{c,d}$. They defined the rational function $w(x, y) = x^3 + y^3$. As before, for $i = 0, 1, 2, 3, 4$, let $w_i = w(P_i)$, where P_i are points of $\mathrm{H}_{c,d}(\mathbb{F}_{2^m})$ with $w(P_0) = w(P_1 - P_2), w(P_3) = w(P_1 + P_2)$ and $w(P_4) = w(2P_1)$. From [5], we have

$$w_4 = \frac{{w_1}^4 + c^3(d^3 + c)}{d^3 {w_1}^2}, \tag{13}$$

$$w_0 + w_3 = \frac{d^3 w_1 w_2}{(w_1 + w_2)^2} \quad \text{and} \quad w_0 w_3 = \frac{{w_1}^2 {w_2}^2 + c^3(d^3 + c)}{(w_1 + w_2)^2}. \tag{14}$$

To have mixed projective formulas, w_i are given by the fractions W_i/Z_i for $i = 0, 1, 2, 3$ where $Z_0 = 1$. The following explicit formulas give the output w_3 defined by W_3/Z_3:

$$A = W_1 Z_2,\ B = W_2 Z_1,\ C = AB,\ U = d^3 C,\ V = (A + B)^2,$$
$$Z_3 = V,\ W_3 = U + w_0 V.$$

Moreover, we write w_4 by the fraction W_4/Z_4. Then, the explicit doubling formulas is

$$A = {W_1}^2,\ B = {Z_1}^2,\ C = A + \sqrt{c^3(d^3 + c)}B,\ D = d^3 B,$$
$$W_4 = C^2,\ Z_4 = AD.$$

The cost of these mixed w-coordinates is $4\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for addition and $1\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$ for doubling and the total cost is $5\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$.

New Differential Addition. In this section we present two new differential addition formulas for *generalized Hessian* curve over binary field $\mathbb{F}_{2^m}$ with total cost of $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ for both doubling and addition.

We modify the definition of the above rational function w, [5], and consider $w(x, y) = \frac{x^3 + y^3}{d^3}$. Using the differential addition formulas (14), by a straightforward calculations, we obtain the following formulas in affine coordinates.

$$w_3 + w_0 = \frac{w_1 w_2}{w_1^2 + w_2^2}, \tag{15}$$

$$w_3 w_0 = \frac{w_1^2 w_2^2 + (c^4 + c^3 d^3)/(d^{12})}{w_1^2 + w_2^2}. \tag{16}$$

Also, from the doubling formula (13), the following doubling formula is obtained.

$$w_4 = \frac{w_1^4 + (c^4 + c^3 d^3)/(d^{12})}{w_1^2}. \tag{17}$$

Cost of Projective w-Coordinates. To obtain the projective formulas, assume that w_i are given by the fractions W_i/Z_i for $i = 0, 1, 2, 3, 4$. From Eq. (15) the following explicit formulas give W_3/Z_3 by

$$\frac{W_3}{Z_3} = \frac{W_0(W_1 Z_2 + W_2 Z_1)^2 + Z_0(W_1 Z_2 W_2 Z_1)}{Z_0(W_1 Z_2 + W_2 Z_1)^2}. \tag{18}$$

Also, from Eq. (17), the doubling is given by

$$\frac{W_4}{Z_4} = \frac{W_1^4 + (c^4 + c^3 d^3)/(d^{12})\ Z_1^4}{W_1^2 Z_1^2}. \tag{19}$$

The cost of projective w-coordinates differential addition and doubling is $7\mathbf{M}+4\mathbf{S}+1\mathbf{D}$; see Eqs. (18) and (19). If we set $Z_0 = 1$ then we have the following mixed projective coordinates formulas with the total cost $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$.

$$\begin{aligned} &A = W_1 Z_1, \quad B = W_1 Z_2, \quad C = W_2 Z_1 \\ &W_4 = (W_1 + \sqrt[4]{(c^4 + c^3 d^3)/d^{12}}\ Z_1)^4, \quad Z_4 = A^2, \\ &Z_3 = (B + C)^2, \quad W_3 = BC + w_0 Z_3. \end{aligned}$$

Here, the differential addition formulas use $4\mathbf{M} + 1\mathbf{S}$ and doubling formulas use $1\mathbf{M}+3\mathbf{S}+1\mathbf{D}$ and the total cost is $5\mathbf{M}+4\mathbf{S}+1\mathbf{D}$. So the computation of $1\mathbf{D}$ is saved. Notice, the projective w-coordinate differential addition and doubling formulas (18) and (19) are almost complete; the exceptional points are 3 torsion points P_0 where $w(P_0) = w(\mathcal{O}) = (1 : 0)$.

5 Binary Huff Curves

Huff model at first introduced by Huff [7] in 1948 to study a diophantine problem. Huff model are extended over fields of odd characteristic. Joye et al. [9], extended the Huff model and also introduced the binary partner for Huff curve. In 2011 Devigen and Joye [4] described the addition law for *Binary Huff* curve and compute formulas for addition, doubling and differential addition which the cost of their differential addition and doubling is $5\mathbf{M}+5\mathbf{S}+1\mathbf{D}$. Here, we improve their results to the cost of $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$.

The *binary Huff* curve is given by the equation

$$HF_{a,b} \ : \ ax(y^2 + y + 1) = by(x^2 + x + 1), \tag{20}$$

where a, b are in $\mathbb{F}_{2^m}$ such that $a, b \neq 0$ and $a \neq b$. This curve have three points at infinity, namely $(a : b : 0)$, $(1 : 0 : 0)$ and $(0 : 1 : 0)$. Binary Huff curve is birationally equivalent to the Weierstraß elliptic curve

$$v^2 + uv = u^3 + (a^2 + b^2)u^2 + a^2b^2u$$

via the map $(x, y) \longmapsto (u, v)$ defined by

$$u = \frac{ab}{xy}, \qquad v = \frac{ab(axy + b)}{x^2y}$$

with the inverse map

$$x = \frac{b(u + a^2)}{v}, \qquad y = \frac{a(u + b^2)}{v + (a + b)u}.$$

The neutral element of binary Huff curve is the point $(0, 0)$. The negation of the point (x, y) is $(\tilde{x}, \tilde{y})$ where

$$\tilde{x} = \frac{y(b + axy)}{a + bxy}, \qquad \tilde{y} = \frac{x(a + bxy)}{b + axy}.$$

Affine Addition. The sum of two points (x_1, y_1) and (x_2, y_2) on $HF_{a,b}$ is the point (x_3, y_3) defined as follows:

$$x_3 = \frac{(x_1y_1 + x_2y_2)(1 + y_1y_2)}{(y_1 + y_2)(1 + x_1x_2y_1y_2)}, \qquad y_3 = \frac{(x_1y_1 + x_2y_2)(1 + x_1x_2)}{(x_1 + x_2)(1 + x_1x_2y_1y_2)}. \tag{21}$$

Affine Doubling. The doubling of point (x_1, y_1) is the point (x_4, y_4) defined as follows:

$$x_4 = \frac{(a + b)x_1^2(1 + y_1^2)}{b(1 + x_1^2)(1 + x_1^2y_1^2)}, \qquad y_4 = \frac{(a + b)y_1^2(1 + x_1^2)}{a(1 + y_1^2)(1 + x_1^2y_1^2)}. \tag{22}$$

As $b \neq 0$ we can divide the Eq. (20) by b and for simplicity we can assume $b = 1$. So, we consider the binary Huff curve with the equation

$$ax(y^2 + y + 1) = y(x^2 + x + 1)$$

where $a \neq 0, 1$.

Differential Addition. Devigen and Joye, [4], proposed the rational function $w(x, y) = xy$ for the binary Huff curves. They obtained the following affine w-coordinates formulas

$$w_4 = \frac{(a^2 + 1)/aw_1^2}{1 + w_1^4}, \qquad w_3 = \frac{(w_1 + w_2)^2}{w_0(1 + w_1w_2)^2}.$$

The projective coordinates of the formulas are

$$W_4 = (a^2 + 1)/a(W_1Z_1)^2, \quad Z_4 = (W_1 + Z_1)^4,$$
$$W_3 = w_0(W_1Z_2 + W_2Z_1)^2, \quad Z_3 = (W_1W_2 + Z_1Z_2)^2.$$

The cost of this w-coordinates in one step of the Montgomery ladder is $5\mathbf{M}+5\mathbf{S}+1\mathbf{D}$.

New Differential Addition. Here, we modify the rational function $w(x,y)=xy$ on binary Huff curve by scaling to $w(x,y)=\frac{(a^2+1)}{a}xy$. This new rational function reduces the cost of differential addition by $1\mathbf{S}$. As before, we use the same notation for differential addition and doubling. From addition formulas (21), we obtain the following formulas in affine coordinates.

$$w_3+w_0=\frac{w_1w_2}{(a/(a^2+1))^4w_1^2w_2^2+1}, \tag{23}$$

$$w_3w_0=\frac{w_1^2+w_2^2}{(a/(a^2+1))^4w_1^2w_2^2+1}. \tag{24}$$

The doubling formula (22) provides the following affine doubling formula.

$$w_4=\frac{w_1^2}{(a/(a^2+1))^4w_1^4+1}. \tag{25}$$

Then, by Eqs. (23) and (24) we have

$$\frac{1}{w_3}+\frac{1}{w_0}=\frac{w_1w_2}{(w_1+w_2)^2}. \tag{26}$$

Cost of Projective w-Coordinates. Assume that w_i are given by the fractions W_i/Z_i for $i=0,1,2,3,4$. By Eq. (26) the following explicit formulas give the output W_3/Z_3 by

$$\frac{Z_3}{W_3}=\frac{Z_0(W_1Z_2+W_2Z_1)^2+W_0(W_1Z_2W_2Z_1)}{W_0(W_1Z_2+W_2Z_1)^2}. \tag{27}$$

Also, from Eq. (25) the explicit doubling formulas is obtained.

$$\frac{W_4}{Z_4}=\frac{W_1^2Z_1^2}{W_1^4+(a/(a^2+1))^4\ Z_1^4}. \tag{28}$$

So, the cost of projective w-coordinates differential addition and doubling is $7\mathbf{M}+4\mathbf{S}+1\mathbf{D}$; see Eqs. (27) and (28). Let assume $W_0=1$. Then using the mixed projective coordinates, we have the following formulas for differential addition:

$$\begin{aligned} A&=W_1Z_1,\quad B=W_1Z_2,\quad C=W_2Z_1,\\ Z_4&=(W_1+(a/(a^2+1))Z_1)^4,\quad W_4=A^2,\\ W_3&=(B+C)^2,\qquad Z_3=BC+z_0Z_3. \end{aligned}$$

Here, the addition formulas use $4\mathbf{M}+1\mathbf{S}$ and doubling formulas use $1\mathbf{M}+3\mathbf{S}+1\mathbf{D}$. The total cost is $5\mathbf{M}+4\mathbf{S}+1\mathbf{D}$ and one S is saved. Moreover the projective w-coordinates differential addition and doubling formulas (27) and (28) are almost complete.

6 Comparison with Previous Works

In Table 1, we compare our new differential addition formulas with other models of binary elliptic curves. The addition formulas for all binary elliptic are complete or almost complete which makes the Montgomery ladder work perfectly in cryptographic applications. The cost of almost complete formulas is $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ that is the best known record. We believe this record may be obtained for any form of binary elliptic curve by a suitable rational function. The proposed formulas for general binary Edwards are improved in terms of efficiency and speed. The complete formulas for binary Edwards curves are the only known complete formulas for binary elliptic curves with the cost of $5\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$.

Table 1. Cost of differential addition and doubling for families of binary elliptic curves

Model	Projective differential	Mixed differential	Completeness
Short Weierstraß [2]	$7\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$	$5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$	Almost
Binary Edwards (*general*) [3]	$8\mathbf{M} + 4\mathbf{S} + 4\mathbf{D}$	$6\mathbf{M} + 4\mathbf{S} + 4\mathbf{D}$	Yes
$(d_1 = d_2)$ [3]	$7\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$	$5\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$	Yes
$(d_1 = d_2)$ [10]	$7\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$	$5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$	Almost
(general) this work	$7\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$	$5\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$	Yes
(general) this work	$7\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$	$5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$	Almost
Binary Hessian [5]	$7\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$	$5\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$	Almost
This work	$7\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$	$5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$	Almost
Binary Huff [4]	$6\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$	$5\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$	Almost
This work	$7\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$	$5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$	Almost

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. 93050416).

References

1. Bernstein, D.J., Chuengsatiansup, C., Kohel, D., Lange, T.: Twisted Hessian curves. In: Lauter, K., Rodríguez-Henríquez, F. (eds.) LATINCRYPT 2015. LNCS, vol. 9230, pp. 269–294. Springer, Heidelberg (2015). doi:10.1007/978-3-319-22174-8_15
2. Bernstein, D., Lange, T.: Explicit-formulas database. http://www.hyperelliptic.org/EFD/
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. Devigne, J., Joye, M.: Binary Huff curves. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 340–355. Springer, Heidelberg (2011). doi:10.1007/978-3-642-19074-2_22
5. Farashahi, R.R., Joye, M.: Efficient arithmetic on Hessian curves. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 243–260. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13013-7_15
6. Gaudry, P., Lubicz, D.: The arithmetic of characteristic 2 Kummer surface. Finite Fields Appl. 246–260 (2009)
7. Huff, G.B.: Diophantine problems in geometryand elliptic ternary forms. Duke Math. J. **15**, 246–260 (1948)
8. Joye, M., Quisquater, J.-J.: Hessian elliptic curves and side-channel attacks. In: Koç, Ç.K., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 402–410. Springer, Heidelberg (2001). doi:10.1007/3-540-44709-1_33
9. Joye, M., Tibouchi, M., Vergnaud, D.: Huff's model for elliptic curves. In: Hanrot, G., Morain, F., Thomé, E. (eds.) ANTS 2010. LNCS, vol. 6197, pp. 234–250. Springer, Heidelberg (2010). doi:10.1007/978-3-642-14518-6_20
10. Kim, K.H., Lee, C.O., Negre, C.: Binary Edwards curves revisited. In: Meier, W., Mukhopadhyay, D. (eds.) INDOCRYPT 2014. LNCS, vol. 8885, pp. 393–408. Springer, Heidelberg (2014). doi:10.1007/978-3-319-13039-2_23
11. Koblitz, N.: Elliptic curves cryptosystem. Math. Comput. **48**, 203–209 (1987)
12. Kohel, D.: Efficient arithmetic on elliptic curves in characteristic 2. In: Galbraith, S., Nandi, M. (eds.) INDOCRYPT 2012. LNCS, vol. 7668, pp. 378–398. Springer, Heidelberg (2012). doi:10.1007/978-3-642-34931-7_22
13. Lopez, J., Dahab, R.: Improved algorithms for elliptic curve arithmetic in GF(2^n) without precomputation. CHES, 220–254 (1999)
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 polard and elliptic curves methods of factorization. Math. Comput. **48**, 243–264 (1987)
16. Montgomery, P.L.: Modular multiplication without trial division. Math. Comput. **48**, 243–264 (1987)
17. Smart, N.P.: The Hessian form of an elliptic curve. In: Koç, Ç.K., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 118–125. Springer, Heidelberg (2001). doi:10.1007/3-540-44709-1_11
18. Washington, L.C.: Elliptic Curves Number Theory and Cryptography. CRC Press, Boca Raton (2008)