On the Alternate Models of Elliptic Curves

Muhammad Ashraf[1] and Barış Bülent Kırlar[1,2]

[1]Institute of Applied Mathematics, Middle East Technical University, 06531, Ankara, Turkey
[2]Department of Mathematics, Süleyman Demirel University, 32260, Isparta, Turkey
e-mails: ashraf6061@gmail.com, bariskirlar@sdu.edu.tr

Abstract—In the recent years, alternate models of elliptic curves have been studied. Such well-known models are Edwards curves, Jacobi intersections and Jacobi quartics, Hessian curves, Huff curves, and their variants to the more common Weierstrass curve. These models sometimes allow for more efficient computation on elliptic curves or provide other features of interest to cryptographers, such as resistance to side-channel attacks. In this paper, we first give the alternate models of elliptic curves emphasizing point addition and point doubling formulae with computational costs, the suggested improvements in each model and then countermeasures to side channel attacks if any. We also describe the geometric interpretation of the addition law in each model.

Keywords—alternate models of elliptic curves, side channel attack, unified addition formulae, computational cost.

1. Introduction

From the advent of elliptic curve cryptosystems, independently by Miller (1985) and Koblitz (1987), arithmetic of elliptic curves have been so much interest from cryptographic researchers. Along this period, they proposed many methods to speed up the arithmetic of elliptic curves. These methods can be divided into four different categories:

- Use optimum underlying finite field extensions,
- Use optimum coordinates for representation of group elements,
- Use efficient arithmetic methods,
- Use alternate models of elliptic curves.

In this work, we are dealing with the alternate models of elliptic curves to the more common Weierstrass curve: Edwards curves, Jacobi intersections and Jacobi quartics, Hessian curves, Huff curves, and their variants. These models allow for more efficient computation on elliptic curves such that the group structure of these curves have already been studied in [4], or provide other features of interest to cryptographers, such as resistance to side-channel attacks. These attacks reveal secret information of an elliptic curve cryptosystem based on the point multiplication operation, in which a point is multiplied by a scalar. The basic method for implementing point multiplication is the *double-and-add technique*, which uses a binary representation of the scalar and performs a sequence of point additions and point doublings depending on the bits of the scalar. In double-and-add point multiplication, a point doubling is done for every bit of the key k, but a point addition is done only when a bit of the key is 1. If, in a side-channel analysis, a point addition is distinguishable from a point doubling, then the bits of the secret key can be determined. This is done by analyzing side channel information such as power

Manuscript received June 12, 2012

consumption [27], running time [26], differential fault analysis [10], electromagnetic emissions [1] and so on. As a countermeasure of this attack, one can use the unified addition formula which means point addition formula that can be used for doublings. The unified formulae for point addition and point doubling use the same sequence of field operations and hence are indistinguishable.

Edwards introduced the normal form of elliptic curves together with an explicit addition law in [15]. He also showed that every elliptic curve over a non-binary field is birationally equivalent to a curve in Edwards form over an extension of the field, and in many cases over the original field. In [3], Bernstein and Lange introduced the notion of Edwards curves which is covering more curves than original Edwards curves when those defined on finite fields. Twisted Edwards curve was introduced by Bernstein et al. in [8] as a generalization of Edwards curves. Hisil et al. introduced the extended twisted Edwards coordinates, and obtained efficient point addition algorithm in [22] that is the fastest one in the literature. These algorithms provide a natural protection from side channel attacks based on Simple Power Analysis (SPA). Bernstein et al. [7] introduced Edwards curves over finite fields of characteristic 2, and obtained addition and doubling formulae.

Jacobi form of the elliptic curves are introduced as the intersection of two quadrics in projective space of dimension 3 by Liardet and Smart in [28]. They showed that these curves could provide a defence against Simple and Differential Power Analysis (SPA/DPA) style attacks. The twisted Jacobi intersections which contains Jacobi intersections as a special case is introduced by Feng et al. in [19]. Billet and Joye [9] reinvestigated the Jacobi Form suggested by Liardet and Smart. They showed that the addition law is directly derived from the underlying quartics.

Hessian curves are investigated as a step towards resistance against side-channel attacks by Joye and Quisquater in [24]. The efficient arithmetic on Hessian elliptic curves are studied in [29] and [20]. They proposed efficient point multiplication algorithms using the Hessian form over finite fields of characteristic 3. In 2010, the family of generalized Hessian curves are proposed by Farashahi and Joye [16]. They showed that these curves cover more isomorphism classes of elliptic curves and that have efficient unified addition formulas. In [6], Bernstein, Kohel and Lange introduced the twisted Hessian form that is similar to the generalized Hessian curves up to the order of the coordinates.

Huff model of elliptic curve is introduced by Huff [21] over rational fields $\mathbb{Q}$ in 1948. Joye et al. [25] improved these curves to the fields of characteristic different than 2. They obtained point addition and doubling formulae on Huff curves. The generalized form of Huff curve is introduced by Feng and Wu in [18]. Ciss and Sow [13] investigated the new generalized Huff curve that the addition law in projective coordinates is as fast as in the previous particular cases. In 2011, Devigne and Joye [14] obtained the unified point addition formula for Huff curves over fields of characteristic 2.

This paper is organized as follows. In section II, we give Weierstrass form of elliptic curves and its group law. In section III, Edwards curves and their variants are discussed. In section IV, Jacobi intersection and Jacobi quartic with related modifications and improvements are discussed. In section V, Hessian curves are elaborated. In section VI, Huff curves and its generalizations are described. In section VII, we compare the alternate models of elliptic curves and conclude the paper.

2. Weierstrass Curves

An elliptic curve in affine coordinates of simplified Weierstrass form over the finite field $\mathbb{F}$ with $char(\mathbb{F}) \neq 2, 3$ is defined by

$$E \ : \ y^2 = x^3 + ax + b, \tag{1}$$

where $a, b \in \mathbb{F}$. If we apply the process of homogenization with $x = X/Z$ and $y = Y/Z$ for $Z \neq 0$ to (1), we obtain the homogeneous equation in projective coordinates given by

$$E \ : \ Y^2Z = X^3 + aXZ^2 + bZ^3, \tag{2}$$

where $a, b \in \overline{\mathbb{F}}$ (the algebraic closure of $\mathbb{F}$). The curve E has exactly one point with coordinate Z equal to zero, namely $(0 : 1 : 0)$. This point is so called point at infinity and denoted by ∞. The curve E has an additive group structure together with the identity element ∞.

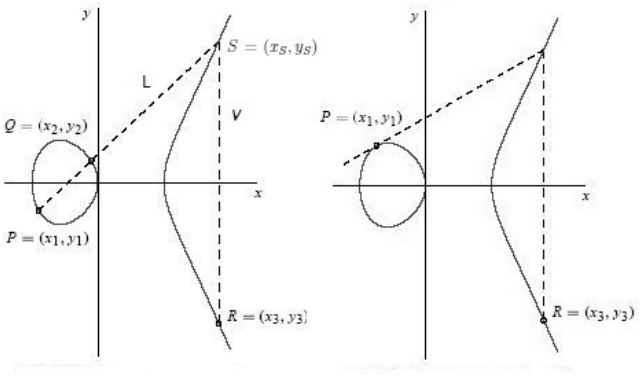

Fig. 1. Addition and doubling over $\mathbb{R}$

The geometric interpretation of the addition law is given by the following way using divisor theory from algebraic geometry [12]: Let $P, Q \in E$. Suppose the line between P and Q (tangent line if $P = Q$) has an equation $L(x, y) = 0$. By Bezout's theorem, this line L intersects E at a third point $S = (x_S, y_S)$ in the projective space. Then the divisor of L is $\text{div}(L) = (P) + (Q) + (S) - 3(\infty)$. The vertical line $V(x) = (x - x_S)$ passes through the points S and $R = P + Q$. Then $\text{div}(V) = (S) + (R) - 2(\infty)$. Therefore, the equation $R = P + Q$ corresponds to $\text{div}(L/V) = (P) + (Q) - (R) - (\infty)$.

This observation allows us to write down the explicit formula for point addition and point doubling of the curve E as follows: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be the points on E with $P, Q \neq \infty$ and $Q \neq -P$. Then

- If $P \neq Q$, then $P + Q = R = (x_3, y_3)$, where

$$\begin{cases} x_3 = (\dfrac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2 \\ y_3 = (\dfrac{y_2 - y_1}{x_2 - x_1})(x_1 - x_3) - y_1 \end{cases}$$

- If $P = Q$, then $2P = R = (x_3, y_3)$, where

$$\begin{cases} x_3 = (\dfrac{3x_1^2 - a}{2y_1})^2 - 2x_1 \\ y_3 = (\dfrac{3x_1^2 - a}{2y_1})(x_1 - x_3) - y_1 \end{cases}$$

Formulas that do not involve field inversions for adding and doubling points in projective coordinates can be derived by first converting the points to affine coordinates, then using the formulae above to add the affine points, and finally clearing denominators. The computational cost of point addition and point doubling in projective coordinates are $12\mathbf{M}+2\mathbf{S}$ and $5\mathbf{M}+6\mathbf{S}$, respectively. Until today, much more point representations were used in simplified Weierstrass form of elliptic curves for fast computations, such as Jacobian, Chudnovsky and mixed coordinates. The mixed addition formulae can also be obtained by replacing $Z_2 = 1$ in this form that reduces the total costs to $9\mathbf{M} + 2\mathbf{S}$. In 2002, Brier and Joye [11] obtained the unified point addition formulae for simplified Weierstrass curves in projective coordinates such that the computational cost is $11\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$.

For the rest of the paper, we enumerate the cost of field operations in terms of multiplication **M**,

squaring **S**, multiplication by a constant **D**, and addition/subtraction **a** in $\mathbb{F}$.

3. Normal Form of Elliptic Curves

In this section, we will discuss salient features of Edwards curves and their variants in respect of point addition and point doubling.

3.1. Edwards Curves

Edwards [15] introduced a new model of elliptic curves over $\mathbb{F}$ with char$(\mathbb{F}) \neq 2$ which is defined by

$$E_c: \ x^2 + y^2 = c^2(1 + x^2y^2), \tag{3}$$

where $c \in \mathbb{F}$. He obtained an efficient explicit formula for point addition of these curves as follows: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on E_c. Then $P + Q = R = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{x_1y_2 + x_2y_1}{c(1 + x_1x_2y_1y_2)} \\ y_3 = \dfrac{y_1y_2 - x_1x_2}{c(1 - x_1x_2y_1y_2)} \end{cases}$$

Edwards showed that all elliptic curves over non-binary finite field $\mathbb{F}$ can be transformed to Edwards curves if $\mathbb{F}$ is algebraically closed. However, over the finite field $\mathbb{F}$, only a small number of elliptic curves can be expressed in this form.

Bernstein and Lange [3] improved the notion of Edwards form defined by

$$E_d: \ x^2 + y^2 = 1 + dx^2y^2, \tag{4}$$

where $d \in \mathbb{F} \setminus \{0, 1\}$. They showed that more than 1/4 of all isomorphism classes of elliptic curves over the finite field $\mathbb{F}$ could be transformed to Edwards curve over the same field. The curve E_d has an additive group structure together with the identity (neutral) element $\mathcal{O} = (0, 1)$. The point

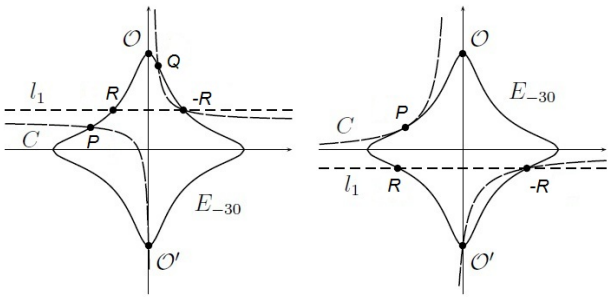

Fig. 2. Addition and doubling over $\mathbb{R}$ for $d < 0$

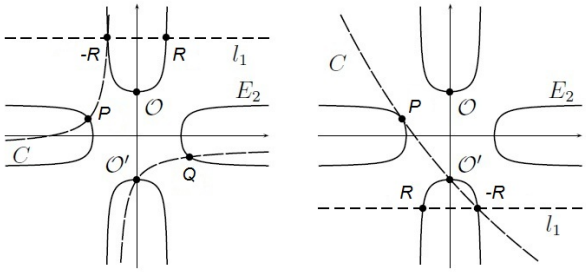

Fig. 3. Addition and doubling over $\mathbb{R}$ for $d > 1$

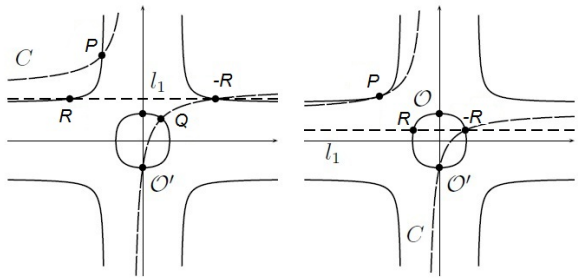

Fig. 4. Addition and doubling over $\mathbb{R}$ for $0 < d < 1$

$\mathcal{O}' = (0, -1)$ has order 2. The points $(1, 0)$ and $(-1, 0)$ have order 4.

The geometric interpretation of the addition law for Edwards curves is given by the following way [2]: We first observe that $\Omega_1 = (1 : 0 : 0)$ and $\Omega_2 = (0 : 1 : 0)$ are the points at infinity that have multiplicity 2. There is a conic C determined by passing through the 5 points $P, Q, \mathcal{O}', \Omega_1$ and Ω_2 has only one more intersection point $-R$ with the curve

E. Let h_1 be the function corresponding to C with $\text{div}(h_1) = (P)+(Q)+(\mathcal{O}')+(-R)-2(\Omega_1)-2(\Omega_2)$. In order to replace $\mathcal{O}'$ by $\mathcal{O}$ and $-R$ by R, one can use another function h_2 that is the product $h_2 = \ell_1\ell_2$ of two lines. A horizontal line ℓ_1 passing through the point R is with $\text{div}(\ell_1) = (R) + (-R) - 2(\Omega_2)$, and a vertical line ℓ_2 passing through the point $\mathcal{O}$ is with $\text{div}(\ell_2) = (\mathcal{O}) + (\mathcal{O}') - 2(\Omega_1)$. Therefore, the equation $R = P+Q$ corresponds to $\text{div}(h_1/\ell_1\ell_2) = (P) + (Q) - (R) - (\mathcal{O})$.

Using this observation, Bernstein and Lange write down the explicit formula for point addition and point doubling of the curve E_d as follows: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on E_d. Then $P + Q = R = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2} \\ y_3 = \dfrac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \end{cases}$$

These formulae are strongly unified. If d is a non-square in $\mathbb{F}$, the addition law is complete, i.e, it works for all pairs of inputs. The inverse of the point (x_1, y_1) on E_d is $(-x_1, y_1)$.

In order to avoid the inversion in addition formulae, the notion of Edwards curves in projective coordinates [3] is defined by

$$(X^2 + Y^2)Z^2 = (Z^4 + dX^2Y^2). \tag{5}$$

The point addition for (5) is obtained by the following formulae: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (5), then $P + Q = R = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = Z_1Z_2(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)[(X_1 + Y_1)(X_2 + Y_2) \\ \qquad -X_1X_2 - Y_1Y_2] \\ Y_3 = Z_1Z_2(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Y_1Y_2 - X_1X_2) \\ Z_3 = (Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2) \end{cases}$$

These formulae are also unified. The point $(0 : 1 : 1)$ is the identity element of addition law. The inverse of $(X_1 : Y_1 : Z_1)$ is $(-X_1 : Y_1 : Z_1)$. The computational cost for addition, doubling, and unified addition is $10\mathbf{M}+1\mathbf{S}+1\mathbf{D}+7\mathbf{a}$, $3\mathbf{M}+4\mathbf{S}+6\mathbf{a}$, and $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D} + 7\mathbf{a}$, respectively. The mixed addition formulae can also be obtained by replacing $Z_2 = 1$ in the above formulae that reduces the total costs to $9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D} + 7\mathbf{a}$. The presence of point of order 4 in the group of elliptic curves in equation (5), reduces the number of elliptic curves in Edwards model over $\mathbb{F}$. To overcome this problem Bernstein et al. [8] introduced further variation of Edwards curves which is so called Twisted Edwards curves.

3.2. Twisted Edwards Curves

Let $\mathbb{F}$ be a field with char($\mathbb{F}$)$\neq 2$. Then twisted Edwards curve is defined by

$$E_{a,d}: \ ax^2 + y^2 = 1 + dx^2y^2, \tag{6}$$

where $a,\ d \in \mathbb{F} \setminus \{0\}$. The twisted Edwards curve $E_{a,d}$ is a quadratic twist of the Edwards curve $E_{1,d/a}$. If a is square in $\mathbb{F}$, then $E_{a,d}$ is isomorphic to $E_{1,d/a}$ over $\mathbb{F}$. The set of these curves is invariant under quadratic twists, in other words, every quadratic twist of a twisted Edwards curve is isomorphic to a twisted Edwards curve. The point addition for (6) is obtained by the following formulae: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on $E_{a,d}$. Then $P + Q = R = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2} \\ y_3 = \dfrac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \end{cases}$$

These formulae are unified. The point $(0, 1)$ is the identity element of addition law and the inverse of the point (x_1, y_1) on $E_{a,d}(\mathbb{F})$ is $(-x_1, y_1)$. If a is square in $\mathbb{F}$ and d is non-square in $\mathbb{F}$, then the addition law for Twisted Edwards curve is complete.

In order to avoid inversion in addition formulae given above, twisted Edwards curves in projective

coordinates is defined by

$$(aX^2 + Y^2)Z^2 = Z^4 + dX^2Y^2. \quad (7)$$

For $Z_1 \neq 0$, the homogeneous point $(X_1 : Y_1 : Z_1)$ represents the affine point $(X_1/Z_1, Y_1/Z_1)$ on $E_{a,d}$. Bernstein et al. [8] obtained the following explicit formulae for addition and doubling on twisted Edwards curves in projective coordinates as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (7), then $P+Q = R = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = (X_1Y_2 - Y_1X_2)(X_1Y_1Z_2^2 + X_2Y_2Z_1^2) \\ Y_3 = (Y_1Y_2 + aX_1X_2)(X_1Y_1Z_2^2 - X_2Y_2Z_1^2) \\ Z_3 = Z_1Z_2(X_1Y_2 - Y_1X_2)(Y_1Y_2 + aX_1X_2) \end{cases}$$

and $2P = R = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = (aX_1^2 + Y_1^2 - 2Z_1^2)[(X_1 + Y_1)^2 \\ \qquad -X_1^2 - Y_1^2] \\ Y_3 = (aX_1^2 + Y_1^2)(aX_1^2 - Y_1^2) \\ Z_3 = (aX_1^2 + Y_1^2)(aX_1^2 + Y_1^2 - 2Z_1^2) \end{cases}$$

The computational cost of point addition and point doubling are $11\mathbf{M} + 2\mathbf{D} + 9\mathbf{a}$ and $3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D} + 7\mathbf{a}$, respectively. It turns out that a mixed addition requires $9\mathbf{M} + 2\mathbf{D} + 9\mathbf{a}$ by setting $Z_2 = 1$.

The unified addition formulae for twisted Edwards curves in projective coordinates are also obtained as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (7), then $P + Q = R = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = Z_1Z_2(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)[(X_1 + Y_1) \\ \qquad (X_2 + Y_2) - X_1X_2 - Y_1Y_2] \\ Y_3 = Z_1Z_2(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Y_1Y_2 - aX_1X_2) \\ Z_3 = (Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2) \end{cases}$$

The computational cost of unified addition is $10\mathbf{M}+ 1\mathbf{S} + 2\mathbf{D} + 7\mathbf{a}$.

Another way to avoid inversions is to define inverted coordinates as follows:

$$(X^2 + aY^2)Z^2 = X^2Y^2 + dZ^4. \quad (8)$$

where $XYZ \neq 0$. The homogeneous point $(X_1 : Y_1 : Z_1)$ with $X_1Y_1Z_1 \neq 0$ represents the affine point $(Z_1/X_1, Z_1/Y_1)$ on $E_{a,d}$. In [5], Bernstein and Lange introduced these inverted coordinates for the case $a = 1$, and observed that the coordinates save time in addition. Bernstein et al. generalized to arbitrary a in [8]. They also obtained the following explicit formulae for unified addition and doubling on twisted Edwards curves in inverted coordinates as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (8), then $P + Q = R = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = Z_1Z_2(X_1X_2 + aY_1Y_2)(X_1Y_1Z_2^2 - Z_1^2X_2Y_2) \\ Y_3 = Z_1Z_2(X_1Y_2 - Y_1X_2)(X_1Y_1Z_2^2 + Z_1^2X_2Y_2) \\ Z_3 = (X_1Y_1Z_2^2 - Z_1^2X_2Y_2)(X_1Y_1Z_2^2 - Z_1^2X_2Y_2) \end{cases}$$

and $2P = R = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = (X_1^2 + aY_1^2)(X_1^2 - aY_1^2) \\ Y_3 = [(X_1 + Y_1)^2 - X_1^2 - Y_1^2](X_1^2 + aY_1^2 - 2dZ_1^2) \\ Z_3 = (X_1^2 - aY_1^2)[(X_1 + Y_1)^2 - X_1^2 - Y_1^2] \end{cases}$$

The unified addition formulae for twisted Edwards curves in inverted coordinates are also obtained as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (7), then $P + Q = R = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = (X_1X_2Y_1Y_2 + dZ_1^2Z_2^2)(X_1X_2 - aY_1Y_2) \\ Y_3 = (X_1X_2Y_1Y_2 - dZ_1^2Z_2^2)[(X_1 + Y_1)(X_2 + Y_2) \\ \qquad -X_1X_2 - Y_1Y_2] \\ Z_3 = Z_1Z_2(X_1X_2 - aY_1Y_2)[(X_1 + Y_1)(X_2 + Y_2) \\ \qquad -X_1X_2 - Y_1Y_2] \end{cases}$$

The computational cost of point addition, point doubling and unified addition are $11\mathbf{M} + 2\mathbf{D} + 9\mathbf{a}$, $3\mathbf{M} + 4\mathbf{S} + 2\mathbf{D} + 6\mathbf{a}$, and $9\mathbf{M} + 1\mathbf{S} + 2\mathbf{D} + 7\mathbf{a}$, respectively. The mixed addition formulae can also be obtained by replacing $Z_2 = 1$, which gives an obvious saving of $2\mathbf{M}$ since $Z_1 \cdot Z_2 = Z_1$, leading to a total cost of $9\mathbf{M} + 2\mathbf{D} + 9\mathbf{a}$.

Hisil et al. [22] introduced the extended Twisted Edwards coordinates by defining an auxiliary coordinate $t = xy$ to represent a point (x, y) on $E_{a,d}$ in

extended affine coordinates (x, y, t). One can pass to the projective representation $(X : Y : T : Z)$ which satisfies (7) and corresponds to the extended affine point $(X/Z, Y/Z, T/Z)$ with $Z \neq 0$. The auxiliary coordinate T has the property $T = XY/Z$. Let $P = (X_1 : Y_1 : T_1 : Z_1)$ and $Q = (X_2 : Y_2 : T_2 : Z_2)$ be two points on (7) with $Z_1 \neq 0$ and $Z_2 \neq 0$, then $P + Q = R = (X_3 : Y_3 : T_3 : Z_3)$, where

$$\begin{cases} X_3 = (X_1Y_2 + Y_1X_2)(Z_1Z_2 - dT_1T_2) \\ Y_3 = (Y_1Y_2 - aX_1X_2)(Z_1Z_2 + dT_1T_2) \\ T_3 = (Y_1Y_2 - aX_1X_2)(X_1Y_2 + Y_1X_2) \\ Z_3 = (Z_1Z_2 - dT_1T_2)(Z_1Z_2 + dT_1T_2) \end{cases}$$

These formulae are unified that derived from the addition formulae on $E_{a,d}$. It is deduced from [3] and [8] that these formulae are also complete when d is not a square in $\mathbb{F}$ and a is a square in $\mathbb{F}$. The identity element is represented by $(0 : 1 : 0 : 1)$. The negative of $(X_1 : Y_1 : T_1 : Z_1)$ on (7) is $(-X_1 : Y_1 : -T_1 : Z_1)$. The computational cost of point addition, point doubling and unified addition are $9\mathbf{M}+1\mathbf{D}+7\mathbf{a}$, $4\mathbf{M}+4\mathbf{S}+1\mathbf{D}+7\mathbf{a}$, and $9\mathbf{M}+2\mathbf{D}+7\mathbf{a}$, respectively. The mixed addition formulae can also be obtained by setting $Z_2 = 1$ in the above formulae, reduces the total costs to $8\mathbf{M}+1\mathbf{D}+7\mathbf{a}$. This means that one can add $(X_1 : Y_1 : T_1 : Z_1)$ and an extended affine point (x_2, y_2, x_2y_2), which is equally written as $(x_2 : y_2 : x_2y_2 : 1)$.

3.3. Binary Edwards Curves

Let $\mathbb{F}$ be a field with char($\mathbb{F}$)$= 2$. Then Binary Edwards curve is defined by

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

where $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. The point addition is obtained by the following formulae: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on E_{B,d_1,d_2}. Then $P + Q = R = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{d_1(x_1 + x_2) + d_2(x_1 + y_1)(x_2 + y_2)}{d_1 + (x_1 + x_1^2)(x_2 + y_2)} \\ \qquad + \dfrac{(x_1 + x_1^2)(x_2(y_1 + y_2 + 1) + y_1y_2)}{d_1 + (x_1 + x_1^2)(x_2 + y_2)} \\ y_3 = \dfrac{d_1(y_1 + y_2) + d_2(x_1 + y_1)(x_2 + y_2)}{d_1 + (y_1 + y_1^2)(x_2 + y_2)} \\ \qquad + \dfrac{(y_1 + y_1^2)(y_2(x_1 + x_2 + 1) + x_1x_2)}{d_1 + (y_1 + y_1^2)(x_2 + y_2)} \end{cases}$$

The addition law on E_{B,d_1,d_2} is strongly unified. The point $(0, 0)$ is the identity element of addition law and the inverse of the point (x_1, y_1) on E_{B,d_1,d_2} is (y_1, x_1). The computational cost of addition and doubling in projective coordinates are $21\mathbf{M}+1\mathbf{S}+4\mathbf{D}$ and $2\mathbf{M}+6\mathbf{S}+3\mathbf{D}$, respectively. When $t^2+t+d_2 \neq 0$ for all $t \in \mathbb{F}$, the addition law on the binary Edwards curve $E_{B,d_1,d_2}(\mathbb{F})$ is complete. The mixed addition formulae lead to a total cost of $13\mathbf{M} + 3\mathbf{S} + 3\mathbf{D}$ that can be obtained by $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (x_2, y_2)$, where $(X_1 : Y_1 : Z_1)$ and (x_2, y_2) on $E_{B,d_1,d_2}(\mathbb{F})$. Bernstein et al. introduced different methods for computing point addition and point doubling with that of computational costs in [7].

4. Jacobi Curves

Jacobi curves gained special attention due to resistance against SPA attacks. In this section, the various forms of Jacobi curves are discussed in respect of point addition and point doubling.

4.1. Jacobi Intersections

Liardet and Smart [28] introduced the Jacobi Intersections over the finite field $\mathbb{F}$ with char($\mathbb{F}$) $\neq 2$ which are defined by

$$E_{J,b} : \begin{cases} x^2 + y^2 = 1 \\ bx^2 + t^2 = 1 \end{cases} \tag{9}$$

where $b \in \mathbb{F}$ and $b(1-b) \neq 0$. They obtained an explicit unified formulae for point addition on $E_{J,b}$ as follows: Let $P = (x_1, y_1, t_1)$ and $Q = (x_2, y_2, t_2)$ be two points on $E_{J,b}$. Then $P+Q = R = (x_3, y_3, t_3)$, where

$$\begin{cases} x_3 = \dfrac{x_1y_2t_2 + x_2y_1t_1}{y_2^2 + x_2^2t_1^2} \\ y_3 = \dfrac{y_1y_2 - x_1t_1x_2t_2}{y_2^2 + x_2^2t_1^2} \\ t_3 = \dfrac{t_1t_2 - bx_1y_1x_2y_2}{y_2^2 + x_2^2t_1^2} \end{cases}$$

and $2P = R = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{2x_1y_1t_1}{y_1^2 + x_1^2t_1^2} \\ y_3 = \dfrac{y_1^2 - x_1^2t_1^2}{y_1^2 + x_1^2t_1^2} \\ t_3 = \dfrac{t_1^2 - bx_1^2y_1^2}{y_1^2 + x_1^2t_1^2} \end{cases}$$

The point $(0, 1, 1)$ is the identity element of addition law and the inverse of the point (x_1, y_1, t_1) on $E_{J,b}$ is $(-x_1, y_1, t_1)$.

The affine version of Jacobi Intersections has inherent greater computational cost due to the field inversion involved in addition formulae. In order to avoid inversions in addition formulae, Jacobi Intersections in projective coordinates [28] is defined by

$$E_{J,b} : \begin{cases} X^2 + Y^2 = Z^2 \\ bX^2 + T^2 = Z^2 \end{cases} \tag{10}$$

with the map $(x, y, t) = (X/Z, Y/Z, T/Z) \mapsto (X : Y : T : Z)$ for $Z \neq 0$. The unified point addition for (10) is obtained by the following formulae: Let $P = (X_1 : Y_1 : T_1 : Z_1)$ and $Q = (X_2 : Y_2 : T_2 : Z_2)$ be two points on (10), then $P + Q = R = (X_3 : Y_3 : T_3 : Z_3)$, where

$$\begin{cases} X_3 = X_1Z_1Y_2T_2 + Y_1T_1X_2Z_2 \\ Y_3 = Y_1Z_1Y_2Z_2 - X_1T_1X_2T_2 \\ T_3 = T_1Z_1T_2Z_2 - bX_1Y_1X_2Y_2 \\ Z_3 = Z_1^2Y_2^2 + X_2^2T_1^2 \end{cases}$$

The point $(0 : 1 : 1 : 1)$ is the identity element of addition law and the inverse of the point $(X_1 : Y_1 : T_1 : Z_1)$ on $E_{J,b}$ is $(-X_1 : Y_1 : T_1 : Z_1)$. There are three points of order 2, namely, $(0 : 1 : 1 : 1)$, $(0 : 1 : 1 : 1)$ and $(0 : 1 : 1 : 1)$. In this case, the computational cost of point addition, point doubling, and unified addition are $13\mathbf{M}+2\mathbf{S}+1\mathbf{D}+7\mathbf{a}$, $4\mathbf{M}+3\mathbf{S}+5\mathbf{a}$, and $13\mathbf{M}+2\mathbf{S}+1\mathbf{D}+7\mathbf{a}$, respectively. The mixed addition formulae can also be obtained by replacing $Z_2 = 1$ in the above formulae that reduces the total costs to $11\mathbf{M}+2\mathbf{S}+1\mathbf{D}+7\mathbf{a}$.

4.2. Twisted Jacobi Intersections

In [19], the twisted Jacobi Intersections which contains Jacobi intersections as a special case was introduced by Feng et al. These curves encompass more number of elliptic curves and have explicit formulae for addition and doubling with almost as fast as the Jacobi Intersections. The twisted Jacobi Intersections over $\mathbb{F}$ with char$(\mathbb{F}) \neq 2$ are defined by

$$E_{J,a,b} : \begin{cases} ax^2 + y^2 = 1 \\ bx^2 + t^2 = 1 \end{cases} \tag{11}$$

where $a, b \in \mathbb{F}$ and $ab(a-b) \neq 0$. They obtained an explicit unified addition formulae on $E_{J,a,b}$ as follows: Let $P = (x_1, y_1, t_1)$ and $Q = (x_2, y_2, t_2)$ be two points on $E_{J,a,b}$. Then $P+Q = R = (x_3, y_3, t_3)$, where

$$\begin{cases} x_3 = \dfrac{x_1y_2t_2 + x_2y_1t_1}{y_2^2 + ax_1^2t_1^2} \\ y_3 = \dfrac{y_1y_2 - ax_1t_1x_2t_2}{y_2^2 + ax_1^2t_1^2} \\ t_3 = \dfrac{t_1t_2 - bx_1y_1x_2y_2}{y_2^2 + ax_1^2t_1^2} \end{cases}$$

The point $(0, 1, 1)$ is the identity element of addition law and the inverse of the point (x_1, y_1, t_1) on $E_{J,a,b}$ is $(-x_1, y_1, t_1)$.

The twisted Jacobi Intersections in projective coordinates [28] is defined by

$$E_{J,a,b} : \begin{cases} aX^2 + Y^2 = Z^2 \\ bX^2 + T^2 = Z^2 \end{cases} \quad (12)$$

with the map $(x, y, t) = (X/Z, Y/Z, T/Z) \mapsto (X : Y : T : Z)$ for $Z \neq 0$. The unified point addition on (12) is obtained by the following formulae: Let $P = (X_1 : Y_1 : T_1 : Z_1)$ and $Q = (X_2 : Y_2 : T_2 : Z_2)$ be two points on (12), then $P + Q = R = (X_3 : Y_3 : T_3 : Z_3)$, where

$$\begin{cases} X_3 = X_1Z_1Y_2T_2 + Y_1T_1X_2Z_2 \\ Y_3 = Y_1Z_1Y_2Z_2 - aX_1T_1X_2T_2 \\ T_3 = T_1Z_1T_2Z_2 - bX_1Y_1X_2Y_2 \\ Z_3 = Z_1^2Y_2^2 + aX_2^2T_1^2 \end{cases}$$

The point $(0 : 1 : 1 : 1)$ is the identity element of addition law and the inverse of the point $(X_1 : Y_1 : T_1 : Z_1)$ on $E_{J,a,b}$ is $(-X_1 : Y_1 : T_1 : Z_1)$. In this case, the computational cost of addition, doubling, and unified addition are $12\mathbf{M} + 11\mathbf{a}$, $3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D} + 7\mathbf{a}$, and $13\mathbf{M} + 2\mathbf{S} + 5\mathbf{D} + 13\mathbf{a}$, respectively. For a mixed point addition, the number of required multiplications drops to $10\mathbf{M} + 11\mathbf{a}$.

4.3. Jacobi Quartics

Jacobi Quartic [9] curves over the finite field $\mathbb{F}$ with $\text{char}(\mathbb{F}) \neq 2, 3$ are first defined by

$$E_{J,k} : y^2 = k^2x^4 - (k^2 + 1)x^2 + 1, \quad (13)$$

where $k \neq 0, \pm 1$. As usual to improve the security parameter that is to increase number of elliptic curves, a modification in Jacobi Quartic was introduced by Hisil et al. in [23]. The modified Jacobi Quartic curves are so called extended Jacobi Quartic curves which are defined by

$$E_{J,d,a} : y^2 = dx^4 + 2ax^2 + 1, \quad (14)$$

where $a, d \in \mathbb{F}$ with $\text{char}(\mathbb{F}) \neq 2, 3$. They showed that arithmetic on Jacobi Quartics is faster as compared with Jacobi Intersections. Moreover, unified point addition formulae offer additional security against some side channel attacks as well. The curve $E_{J,d,a}$ has an additive group structure together with the identity element $\mathcal{O} = (0, 1)$. Note the fact $\mathcal{O}' = (0, -1)$ is a point on the curve.

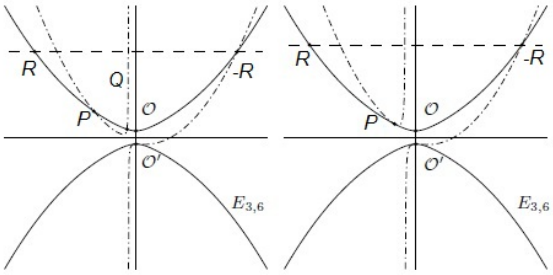

Fig. 5. Addition and doubling over $\mathbb{R}$

The geometric interpretation of the addition law for Jacobi Quartics is shown in the following [30]: We first observe that there is a singular point $\Omega = (0 : 1 : 0)$ in projective space, which is a point at infinity in affine plane. Let C be a conic passing through the points $P, Q, \mathcal{O}'$ and $-R$ with $\text{div}(C) = (P) + (Q) + (-R) + 3(\mathcal{O}') - 6(\Omega)$. Let ℓ be the vertical line passing through the points $\mathcal{O}$ and $\mathcal{O}'$, then $\text{div}(\ell) = (\mathcal{O}) + (\mathcal{O}') - 2(\Omega)$. Let f_R be a function with $\text{div}(f_R) = (R) + (-R) - 2(\mathcal{O})$. Therefore, the equation $R = P + Q$ corresponds to $\text{div}(C/f_R\ell^3) = (P) + (Q) - (R) - (\mathcal{O})$.

Using this observation, the explicit formulae for point addition and point doubling of the curve $E_{J,d,a}$ are adapted from [23] as follows: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on $E_{J,d,a}$, then $P +$

$Q = R = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{x_1y_2 + y_1x_2}{1 - dx_1^2x_2^2} \\ y_3 = \dfrac{(y_1y_2 + 2ax_1x_2)(1 + dx_1^2x_2^2)}{(1 - dx_1^2x_2^2)^2} \\ \qquad + \dfrac{2dx_1x_2(x_1^2 + x_2^2)}{(1 - dx_1^2x_2^2)^2} \end{cases}$$

and $2P = R = (x_3, y_3)$, where

$$\begin{cases} x_3 = \delta x_1 \\ y_3 = \delta(\delta - y_1) - 1 \end{cases}$$

where $\delta = 2y_1/(2 + 2ax_1^2 - y_1^2)$. The inverse of the point (x_1, y_1) on $E_{J,d,a}$ is $(-x_1, y_1)$.

In order to avoid inversion in addition formulae given above, the extended Jacobi Quartic curves in Jacobian coordinates with $x = X/Z$ and $y = Y/Z^2$ are defined by

$$Y^2 = dX^4 - 2aX^2Z^2 + Z^4, \tag{15}$$

where $a, d \in \mathbb{F}$ with $\text{char}(\mathbb{F}) \neq 2, 3$. Billet and Joye [9] proposed a faster inversion-free unified addition algorithm on (15) as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (15), then $P + Q = R = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = X_1Y_2Z_1 + X_2Y_1Z_2 \\ Y_3 = [(Z_1Z_2)^2 + d(X_1X_2)^2](Y_1Y_2 - 2aX_1X_2Z_1Z_2) \\ \qquad +2dX_1X_2Z_1Z_2(X_1^2Z_2^2 + Z_1^2X_2^2) \\ Z_3 = (Z_1Z_2)^2 - d(X_1X_2)^2 \end{cases}$$

The identity element of addition law is given by $(0 : 1 : 1)$ and the negative of the point $(X_1 : Y_1 : Z_1)$ on (15) is $(-X_1 : Y_1 : Z_1)$. The computational cost of addition, doubling, and unified addition are $10\mathbf{M}+3\mathbf{S}+1\mathbf{D}$, $1\mathbf{M}+9\mathbf{S}+1\mathbf{D}$, and $10\mathbf{M}+3\mathbf{S}+1\mathbf{D}$, respectively. The total cost of point addition reduces to $8\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$ by replacing $Z_2 = 1$.

An other improvement was obtained by Hisil et al. in [23]. They showed that the extended Jacobi Quartic curves in extended projective coordinates was defined by

$$\begin{cases} X^2 - TZ = 0 \\ Y^2 - dT^2 - 2aX^2 - Z^2 = 0 \end{cases} \tag{16}$$

or simply

$$Y^2Z^2 = dX^4 + 2aX^2Z^2 + Z^4, \tag{17}$$

where T is omitted in the latter case. In this case, a point $(x, y) \in E_{J,d,a}(\mathbb{F})$ corresponds to the point $(X : Y : T : Z)$, where $T = X^2/Z$. The identity element is represented by $(0 : 1 : 0 : 1)$ and negative of $(X_1 : Y_1 : T_1 : Z_1)$ on (17) is $(-X_1 : Y_1 : T_1 : Z_1)$. They obtained the following explicit formulae for addition and doubling on the extended Jacobi Quartic curves in extended projective coordinates as follows: Let $P = (X_1 : Y_1 : T_1 : Z_1)$ and $Q = (X_2 : Y_2 : T_2 : Z_2)$ be two points on (17), then $P + Q = R = (X_3 : Y_3 : T_3 : Z_3)$ with $Z_1 \neq 0$, $Z_2 \neq 0$ and $P \neq Q$, where

$$\begin{cases} X_3 = (X_1Y_2 - Y_1X_2)(T_1Z_2 - Z_1T_2) \\ Y_3 = (T_1Z_2 + Z_1T_2 - 2X_1X_2)(Y_1Y_2 - 2aX_1X_2 \\ \qquad +Z_1Z_2 + dT_1T_2) - Z_3 \\ T_3 = (T_1Z_2 - Z_1T_2)^2 \\ Z_3 = (X_1Y_2 - Y_1X_2)^2 \end{cases}$$

and $2P = R = (X_3 : Y_3 : T_3 : Z_3)$, where

$$\begin{cases} X_3 = X_1Y_2Z_1 + X_2Y_1Z_2 \\ Y_3 = [(Z_1Z_2)^2 + d(X_1X_2)^2](Y_1Y_2 - 2aX_1X_2Z_1Z_2) \\ \qquad +2dX_1X_2Z_1Z_2(X_1^2Z_2^2 + Z_1^2X_2^2) \\ T_3 = (2X_1Y_1)^2 \\ Z_3 = (Z_1Z_2)^2 - d(X_1X_2)^2 \end{cases}$$

If $a = -1/2$, the computational cost of point addition and point doubling are $7\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$ and $8\mathbf{S}$, respectively. The total cost of point addition reduces to $6\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$ by replacing $Z_2 = 1$.

They also obtained the unified addition formulae for extended Jacobi Quartics in extended projective coordinates as follows: Let $P = (X_1 : Y_1 : T_1 : Z_1)$ and $Q = (X_2 : Y_2 : T_2 : Z_2)$ be two points on (17),

then $P+Q=R=(X_3:Y_3:T_3:Z_3)$ with $Z_1\neq 0$ and $Z_2\neq 0$, where

$$\begin{cases} X_3=(X_1Y_2+Y_1X_2)(Z_1Z_2-dZ_1T_2) \\ Y_3=(Y_1Y_2+2aX_1X_2)(Z_1Z_2+dT_1T_2) \\ \qquad +2dX_1X_2(T_1Z_2+Z_1T_2) \\ T_3=(X_1Y_2+Y_1X_2)^2 \\ Z_3=(Z_1Z_2-dT_1T_2)^2 \end{cases}$$

If d is not a square in $\mathbb{F}$, then the unified addition formulae are complete. The computational cost is $8\mathbf{M}+3\mathbf{S}+2\mathbf{D}+17\mathbf{a}$ when $a=-1/2$. More on formulae and operation counts can be found Appendix B in [23].

5. Hessian Curves

In [24], Hessian elliptic curves are investigated by Joye and Quisquater. They obtained the formulae of point addition, point doubling and unified addition. The Hessian elliptic curve over $\mathbb{F}$ with $\text{char}(\mathbb{F})\neq 2,3$ is a plane cubic curve given by

$$H_d\ :\ x^3+y^3+1=3dxy, \tag{18}$$

or in projective coordinates,

$$H_d\ :\ X^3+Y^3+Z^3=3dXYZ, \tag{19}$$

where $d\in\mathbb{F}$ and $d^3\neq 1$. The curve H_d has an additive group structure together with the identity element $\mathcal{O}=(1:-1:0)$. The points $(0:1:-1)$ and $(1:0:-1)$ are two points of order 3.

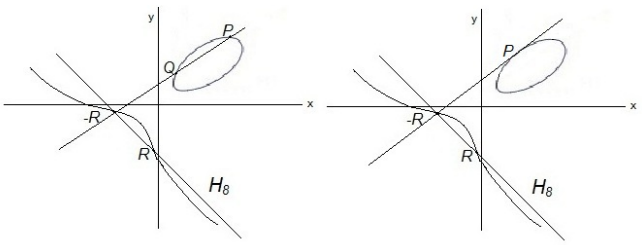

Fig. 6. Addition and doubling over $\mathbb{R}$

The geometric interpretation of the addition law for Hessian curves is given by the following way [17]: For $P,Q\in H_d$, let ℓ_1 be the line passing through the points P and Q. Then the divisor of L is $\text{div}(\ell_1)=(P)+(Q)+(-R)-3(\mathcal{O})$. Let ℓ_2 be the line passing through the points $-R$ and R. Then $\text{div}(\ell_2)=(R)+(-R)-2(\mathcal{O})$. Therefore, the equation $R=P+Q$ corresponds to $\text{div}(\ell_1/\ell_2)=(P)+(Q)-(R)-(\infty)$.

This observation allows us to write down the explicit formula for point addition and point doubling of the curve H_d as follows [24]: Let $P=(X_1:Y_1:Z_1)$ and $Q=(X_2:Y_2:Z_2)$ be two points on (19), then $P+Q=R=(X_3:Y_3:Z_3)$, where

$$\begin{cases} X_3=Y_1^2X_2Z_2-Y_2^2X_1Z_1 \\ Y_3=X_1^2Y_2Z_2-X_2^2Y_1Z_1 \\ Z_3=Z_1^2Y_2X_2-Z_2^2Y_1X_1 \end{cases}$$

and $2P=R=(X_3:Y_3:Z_3)$, where

$$\begin{cases} X_3=Y_1(Z_1^3-X_1^3) \\ Y_3=X_1(Y_1^3-Z_1^3) \\ Z_3=Z_1(X_1^3-Y_1^3) \end{cases}$$

The inverse of the point $(X_1:Y_1:Z_1)$ on H_d is $(Y_1:X_1:Z_1)$. Owing to the formulae $2(X_1:Y_1:Z_1)=(Z_1:X_1:Y_1)+(Y_1:Z_1:X_1)$ and $(X_1:Y_1:Z_1)-(X_2:Y_2:Z_2)=(X_1:Y_1:Z_1)+(Y_2:X_2:Z_2)$, the following addition algorithm given by Joye and Quisquater in [24] can be used also doubling and subtraction as well as addition: Let $P=(X_1:Y_1:Z_1)$ and $Q=(X_2:Y_2:Z_2)$ be two points on (19), then $P+Q=R=(X_3:Y_3:Z_3)$,

where

$$\text{Step 1}\begin{cases} L_1 \leftarrow X_1;\ L_2 \leftarrow Y_1;\ L_3 \leftarrow Z_1 \\ L_4 \leftarrow X_2;\ L_5 \leftarrow Y_2;\ L_6 \leftarrow Z_2 \end{cases}$$

$$\text{Step 2}\begin{cases} L_7 \leftarrow L_1 \cdot L_6;\ L_1 \leftarrow L_1 \cdot L_5 \\ L_5 \leftarrow L_3 \cdot L_5;\ L_3 \leftarrow L_3 \cdot L_4 \\ L_4 \leftarrow L_2 \cdot L_4;\ L_2 \leftarrow L_2 \cdot L_6 \end{cases}$$

$$\text{Step 3}\begin{cases} L_6 \leftarrow L_2 \cdot L_7;\ L_2 \leftarrow L_2 \cdot L_4 \\ L_4 \leftarrow L_3 \cdot L_4;\ L_3 \leftarrow L_3 \cdot L_5 \\ L_5 \leftarrow L_1 \cdot L_5;\ L_1 \leftarrow L_1 \cdot L_7 \end{cases}$$

$$\text{Step 4}\begin{cases} X_3 \leftarrow L_2 - L_5;\ Y_3 \leftarrow L_1 - L_4 \\ Z_3 \leftarrow L_3 - L_6 \end{cases}$$

The computational cost of these operations are $12\mathbf{M} + 3\mathbf{a}$. The total cost of point addition reduces to $10\mathbf{M} + 3\mathbf{a}$ by replacing $Z_2 = 1$.

More recently, Farashahi and Joye [16] considered a generalized form of Hessian curves that covers more isomorphism classes of elliptic curves. These curves are similar to the twisted Hessian form [6], introduced by Bernstein, Kohel and Lange, up to the order of the coordinates. The generalized Hessian curve over $\mathbb{F}$ is defined by

$$H_{c,d} \ : \ x^3 + y^3 + c = dxy, \qquad (20)$$

where $c, d \in \mathbb{F}$ with $c \neq 0$ and $d^3 \neq 27c$. A generalized Hessian curve over $\mathbb{F}$ is isomorphic over $\mathbb{F}$ to a Hessian curve if and only if c is a cube in $\mathbb{F}$. It is easy to adapt the addition and doubling formulae for generalized Hessian curves which are so-called Sylvester formulas as follows: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on $H_{c,d}$, then $P + Q = R = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{y_1^2 x_2 - y_2^2 x_1}{x_2 y_2 - x_1 y_1} \\ y_3 = \dfrac{x_1^2 y_2 - x_2^2 y_1}{x_2 y_2 - x_1 y_1} \end{cases}$$

and $2P = R = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{y_1(c - x_1^3)}{x_1^3 - y_1^3} \\ y_3 = \dfrac{x_1(c - y_1^3)}{x_1^3 - y_1^3} \end{cases}$$

Furthermore, the inverse of the point (x_1, y_1) on $H_{c,d}$ is the point (y_1, x_1). The generalized Hessian curves in projective coordinates are defined by

$$H_{c,d} \ : \ X^3 + Y^3 + cZ^3 = dXYZ. \qquad (21)$$

The point $(1 : -1 : 0)$ is identity element and the inverse of the point $(X_1 : Y_1 : Z_1)$ on $H_{c,d}$ is $(Y_1 : X_1 : Z_1)$. They obtained point addition and doubling formulae on generalized Hessian curves in projective coordinates as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on $H_{c,d}$, then $P + Q = R = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = X_2 Z_2 Y_1^2 - X_1 Z_1 Y_2^2 \\ Y_3 = Y_2 Z_2 X_1^2 - Y_1 Z_1 X_2^2 \\ Z_3 = X_2 Y_2 Z_1^2 - X_1 Y_1 Z_2^2 \end{cases}$$

and $2P = R = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = Y_1(cZ_1^3 - X_1^3) \\ Y_3 = X_1(Y_1^3 - cZ_1^3) \\ Z_3 = Z_1(X_1^3 - Y_1^3) \end{cases}$$

In this case, the computational cost of point addition is $4\mathbf{M}$, $3\mathbf{M}$, or $2\mathbf{M}$ correspond to use of $3, 4$ or 6 processors, respectively. The point addition formulae are complete if the difference of all pairs of points on $H_{c,d}$ is not equal the identity. The cost of point doubling is $6\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$. The point doubling formulae are complete for all inputs.

The unified addition formulae for generalized Hessian curves in projective coordinates are also obtained as follows: Let $P = (X_1 : Y_1 : Z_1)$ and

$Q = (X_2 : Y_2 : Z_2)$ be two points on $H_{c,d}$, then $P + Q = R = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = cY_2Z_2Z_1^2 - X_1Y_1X_2^2 \\ Y_3 = X_2Y_2Y_1^2 - cX_1Z_1Z_2^2 \\ Z_3 = X_2Z_2X_1^2 - Y_1Z_1Y_2^2 \end{cases}$$

The computational cost of unified point addition is $12\mathbf{M} + 1\mathbf{D}$. The unified point addition formulae on $H_{c,d}$ are complete if c is not a cube in $\mathbb{F}$. It turns out that a mixed addition requires $10\mathbf{M} + 1\mathbf{D}$ by setting $Z_2 = 1$.

Farashahi and Joye [16] obtained point addition, doubling and tripling formulae for binary generalized Hessian curves with the computational cost of them. Differential addition, that is, point addition with a known difference was also devised for binary Hessian curves by them.

6. Huff Model of Elliptic Curves

In this section, we will give the details of the models of Huff curves, especially their group structure and related formulae with associated computational costs.

6.1. Huff Curves

In [21], Huff investigated the Huff elliptic curves over rational fields $\mathbb{Q}$ in 1948. Joye et al. [25] improved these curves to the finite field $\mathbb{F}$ with $\text{char}(\mathbb{F}) \neq 2$ that are given by

$$E_{a,b} \; : \; ax(y^2 - 1) = by(x^2 - 1), \qquad (22)$$

where $a, b \neq 0$ and $a^2 - b^2 \neq 0$. The unified point addition for (22) is obtained by the following formulae: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on (22). Then $P + Q = R = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{(x_1 + x_2)(1 + y_1y_2)}{(1 + x_1x_2)(1 - y_1y_2)} \\ y_3 = \dfrac{(y_1 + y_2)(1 + x_1x_2)}{(1 - x_1x_2)(1 + y_1y_2)} \end{cases}$$

These formulae are complete whenever $x_1x_2 \neq \pm 1$ and $y_1y_2 \neq \pm 1$. The Huff model of elliptic curves in projective coordinates are defined by

$$aX(Y^2 - Z^2) = bY(X^2 - Z^2), \qquad (23)$$

where $a, b \neq 0$ and $a^2 - b^2 \neq 0$. Huff curves has an additive group structure together with the identity element $\mathcal{O} = (0 : 0 : 1)$. We note that a point at infinity is its own inverse. Hence, there are three points at infinity, namely, $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(a : b : 0)$. The sum of any two of them is equal to the third one.

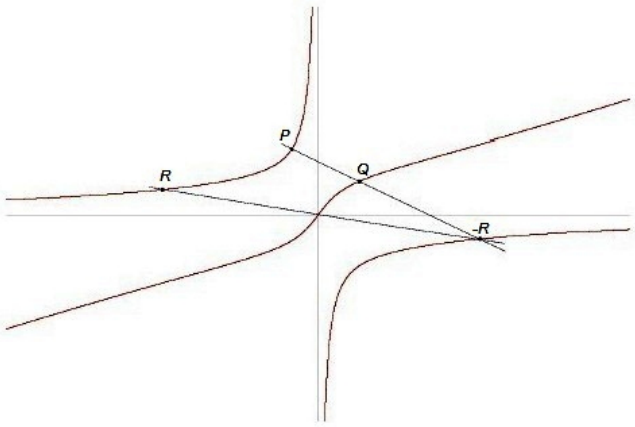

Fig. 7. Addition over $\mathbb{R}$

The geometric interpretation of the addition law for Huff curves is given by the following way [25]: For $P, Q \in E_{a,b}$, let ℓ be the rational function passing through the points P and Q with $\text{div}(\ell) = (P) + (Q) + (-R) - (1 : 0 : 0) - (0 : 1 : 0) - (a : b : 0)$, where $-R$ is the third point of intersection of the line ℓ with the elliptic curve. The neutral element of the group law is $\mathcal{O} = (0 : 0 : 1)$. Let f be the line function with $\text{div}(f) = (R) + (-R) + (\mathcal{O}) - (1 : 0 : 0) - (0 : 1 : 0) - (a : b : 0)$. Therefore, the equation $R = P + Q$ corresponds to $\text{div}(\ell/f) = (P) + (Q) - (R) - (\mathcal{O})$.

This observation allows us to write down the explicit unified addition formulae on (23) as follows:

Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (23), then $P + Q = R = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = (X_1Z_2 + X_2Z_1)(Y_1Y_2 + Z_1Z_2)(Y_1Z_2 + Y_2Z_1) \\ Y_3 = (X_1X_2 - Z_1Z_2)(Z_1^2Z_2^2 - Y_1^2Y_2^2) \\ Z_3 = (Y_1Z_2 + Y_2Z_1)(X_1X_2 + Z_1Z_2)(Y_1Y_2 - Z_1Z_2) \end{cases}$$

These formulae are obtained by choosing $\mathcal{O}' = (0 : 1 : 0)$ as the neutral element results in translating the group law, in other words, the point addition $P + Q$ transforms to $P + Q + \mathcal{O}'$. The inverse of the point $(X_1 : Y_1 : Z_1)$ on (23) is $(X_1 : Y_1 : -Z_1)$, which is unchanged. Note also that the above formulae are complete provided that $X_1X_2 \neq Z_1Z_2$ and $Y_1Y_2 \neq Z_1Z_2$, and are independent of curve parameters $a, b \in \mathbb{F}$. The computational cost of point addition, point doubling, and unified addition are $12\mathbf{M}$, $6\mathbf{M} + 5\mathbf{S}$, and $11\mathbf{M}$, respectively. For a mixed point addition (i.e., when $Z_2 = 1$), the number of required multiplications drops to $10\mathbf{M}$.

Joye et al. [25] investigated twisted Huff curves defined by

$$ax(y^2 - d) = by(x^2 - d), \tag{24}$$

where $abd(a^2 - b^2) \neq 0$. These curves are also defined in projective coordinates as follows:

$$aX(Y^2 - dZ^2) = bY(X^2 - dZ^2), \tag{25}$$

where $abd(a^2 - b^2) \neq 0$. They obtained point addition formulae with performing $12\mathbf{M}$. For more formulae, one can look at [25].

In order to improve the number of isomorphism classes, a generalized Huff curves was introduced by Wu and Feng in [18]. It is note worthy that the Huff curve family is included in the generalized Huff curves. These curves over the finite field $\mathbb{F}$ with $char(\mathbb{F}) \neq 2$ are defined by

$$x(ay^2 - 1) = y(bx^2 - 1), \tag{26}$$

where $ab(a - b) \neq 0$. They obtained the following formulae for addition and doubling on generalized Huff curves in affine coordinates as follows: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on (26), then $P + Q = R = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{(x_1 + x_2)(ay_1y_2 + 1)}{(bx_1x_2 + 1)(ay_1y_2 - 1)} \\ y_3 = \dfrac{(y_1 + y_2)(bx_1x_2 + 1)}{(bx_1x_2 - 1)(ay_1y_2 + 1)} \end{cases}$$

and $2P = R = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{2x_1(ay_1^2 + 1)}{(bx_1^2 + 1)(ay_1^2 - 1)} \\ y_3 = \dfrac{2y_1(bx_1^2 + 1)}{(bx_1^2 - 1)(ay_1^2 + 1)} \end{cases}$$

In order to avoid inversion for addition formulae in affine coordinates, the generalized Huff curves in projective coordinates are defined by

$$X(aY^2 - Z^2) = Y(bX^2 - Z^2), \tag{27}$$

with the map $(x, y) \mapsto (X : Y : Z)$ for $Z \neq 0$. In this case, there are three infinite points, namely $(1 : 0 : 0), (0 : 1 : 0)$ and $(a : b : 0)$. We will now discuss addition of any two points by selecting $(1 : 0 : 0)$ as identity element. The negative of $(X_1 : Y_1 : Z_1)$ on (27) is $(X_1 : Y_1 : -Z_1)$. Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (27). Then $P + Q = R = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = (bX_1X_2 - Z_1Z_2)(bX_1X_2 + Z_1Z_2) \\ \qquad (Z_1Z_2 - aY_1Y_2) \\ Y_3 = b(X_1Z_2 + X_2Z_1)(bX_1X_2 + Z_1Z_2) \\ \qquad (Y_1Z_2 + Y_2Z_1) \\ Z_3 = b(X_1Z_2 + X_2Z_1)(bX_1X_2 - Z_1Z_2) \\ \qquad (aY_1Y_2 + Z_1Z_2) \end{cases}$$

These formulae are unified. The computational cost of point addition and doubling corresponding the

identity element $(1 : 0 : 0)$ are $11\mathbf{M} + 3\mathbf{D}$ and $6\mathbf{M} + 5\mathbf{S} + 3\mathbf{D}$, respectively. For a mixed point addition (i.e., when $Z_2 = 1$), the number of required multiplications drops to $10\mathbf{M} + 3\mathbf{D}$. It is possible to choose $(0 : 1 : 0)$ and $(a : b : 0)$ as identity elements. In each case, the negative of $(X_1 : Y_1 : Z_1)$ on (27) is $(X_1 : Y_1 : -Z_1)$. In order to examine the related point addition formulae and more, we refer the reader to [18].

In 2011, Ciss and Sow [13] introduced the new generalized Huff curves over the finite field $\mathbb{F}$ of char$(\mathbb{F}) \neq 2$. These curves are defined by

$$ax(y^2 - c) = by(x^2 - d), \tag{28}$$

where $a, b, c, d \in \mathbb{F}$ with $abcd(a^2c - b^2d) \neq 0$. The new generalized Huff curves contains the generalized Huff's model $ax(y^2 - d) = by(x^2 - d)$ with $abd(a^2 - b^2) \neq 0$ of Joye et al. [25] and the generalized Huff curves $x(ay^2 - 1) = y(bx^2 - 1)$ with $ab(a - b) \neq 0$ of Wu and Feng [18] as a special case. Ciss and Sow obtained the addition and doubling formulae of new generalized Huff curves in affine coordinates as follows: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on (28). Then $P + Q = R = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{d(x_1 + x_2)(c + y_1y_2)}{(d + x_1x_2)(c - y_1y_2)} \\ y_3 = \dfrac{c(y_1 + y_2)(d + x_1x_2)}{(d - x_1x_2)(c + y_1y_2)} \end{cases}$$

and $2P = R = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{2dx_1(c + {y_1}^2)}{(d + {x_1}^2)(c - {y_1}^2)} \\ y_3 = \dfrac{2cy_1(d + {x_1}^2)}{(d - {x_1}^2)(c + {y_1}^2)} \end{cases}$$

The addition formulae are complete if $x_1x_2 \neq \pm c$ and $y_1y_2 \neq \pm d$ and the doubling formulae are complete if ${x_1}^2 \neq \pm c$ and ${y_1}^2 \neq \pm d$ and in particular if c and d are not square in $\mathbb{F}$.

In order to avoid inversion in addition formulae, the new generalized Huff curves in projective coordinates are defined by

$$aX(Y^2 - cZ^2) = bY(X^2 - dZ^2), \tag{29}$$

where $a, b, c, d \in \mathbb{F}$ with $abcd(a^2c - b^2d) \neq 0$. The neutral element of the group law is $\mathcal{O} = (0 : 0 : 1)$ and the negative of $(X_1 : Y_1 : Z_1)$ on (29) is $(X_1 : Y_1 : -Z_1)$. The addition law in projective coordinates is as fast as in the previous particular cases. They obtained point addition and point doubling on (29) by the following formulae: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (29), then $P + Q = R = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = d(X_1Z_2 + X_2Z_1)(cZ_1Z_2 + Y_1Y_2)^2 \\ \qquad (dZ_1Z_2 - X_1X_2) \\ Y_3 = c(Y_1Z_2 + Y_2Z_1)(dZ_1Z_2 + X_1X_2) \\ \qquad (cZ_1Z_2 - Y_1Y_2) \\ Z_3 = (d^2Z_1^2Z_2^2 - X_1^2X_2^2)(c^2Z_1^2Z_2^2 - Y_1^2Y_2^2) \end{cases}$$

and $2P = R = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = 2dX_1(cZ_1^2 + Y_1^2)^2(dZ_1^2 - X_1^2) \\ Y_3 = 2cY_1(dZ_1^2 + X_1^2)^2(cZ_1^2 - Y_1^2) \\ Z_3 = (d^2Z_1^4 - X_1^4)(c^2Z_1^4 - Y_1^4) \end{cases}$$

The above point addition formulae are complete provided that $X_1X_2 \neq dZ_1Z_2$ and $Y_1Y_2 \neq cZ_1Z_2$. The computational cost of point addition and point doubling formulae are $12\mathbf{M} + 4\mathbf{D}$ and $7\mathbf{M} + 5\mathbf{S} + 4\mathbf{D}$, respectively. The total cost of point addition reduces to $11\mathbf{M} + 4\mathbf{D}$ by replacing $Z_2 = 1$. For further details, we refer the reader to look at [13].

6.2. Binary Huff Curves

Joye et al. [25] introduced the binary Huff curves over $\mathbb{F}$ with char$(\mathbb{F}) = 2$ which are defined by

$$ax(y^2 + y + 1) = by(x^2 + x + 1), \tag{30}$$

or in projective coordinates

$$aX(Y^2 + YZ + Z^2) = bY(X^2 + XZ + Z^2), \quad (31)$$

where $ab(a - b) \neq 0$. Devigne and Joye [14] described the addition law for binary Huff curves. They showed that there are three points at infinity satisfying the curve equation, namely $(a : b : 0)$, $(1 : 0 : 0)$, and $(0 : 1 : 0)$. They obtained unified point addition formulae as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (31), then $P + Q = R = (X_3 : Y_3 : Z_3)$ with

$$\begin{cases} X_3 = (Z_1Z_2 + Y_1Y_2)[(X_1Z_2 + X_2Z_1)(Z_1^2Z_2^2 \\ \quad + X_1X_2Y_1Y_2) + \alpha X_1X_2Z_1Z_2(Z_1Z_2 + Y_1Y_2)] \\ Y_3 = (Z_1Z_2 + X_1X_2)[(Y_1Z_2 + Y_2Z_1)(Z_1^2Z_2^2 \\ \quad + X_1X_2Y_1Y_2) + \beta Y_1Y_2Z_1Z_2(Z_1Z_2 + X_1X_2)] \\ Z_3 = (Z_1Z_2 + X_1X_2)(Z_1Z_2 + Y_1Y_2) \\ \quad (Z_1^2Z_2^2 + X_1X_2Y_1Y_2) \end{cases}$$

where $\alpha = (a + b)/b$ and $\beta = (a + b)/a$. The computational cost of unified point addition is $15\mathbf{M} + 2\mathbf{D}$.

The generalized binary Huff curves over $\mathbb{F}$ with $\text{char}(\mathbb{F}) = 2$ are also defined by Devigne and Joye [14] which are of the form

$$ax(y^2 + fy + 1) = by(x^2 + fx + 1), \quad (32)$$

or in projective coordinates

$$aX(Y^2 + fYZ + Z^2) = bY(X^2 + fXZ + Z^2), \quad (33)$$

where $abf(a-b) \neq 0$. They obtained the unified addition formulae of generalized binary Huff curves in affine coordinates which are given by the following formulae: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on (32). Then $P + Q = R = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{b(x_1 + x_2)(1 + x_1x_2y_1y_2)}{b(1 + x_1x_2)(1 + x_1x_2y_1y_2)} \\ \quad + \dfrac{f(a + b)x_1x_2(1 + y_1y_2)}{b(1 + x_1x_2)(1 + x_1x_2y_1y_2)} \\ y_3 = \dfrac{a(y_1 + y_2)(1 + x_1x_2y_1y_2)}{a(1 + y_1y_2)(1 + x_1x_2y_1y_2)} \\ \quad + \dfrac{f(a + b)y_1y_2(1 + x_1x_2)}{a(1 + y_1y_2)(1 + x_1x_2y_1y_2)} \end{cases}$$

The computational cost of point addition, point doubling and unified addition formulae are $15\mathbf{M}$, $6\mathbf{M} + 2\mathbf{D}$ and $15\mathbf{M} + 2\mathbf{D}$, respectively. For more information and formulae, we refer the reader to [14].

7. Comparison and Conclusions

In this paper, the alternative models of elliptic curves are surveyed by pinning down group operations, and performance in various coordinate systems. Table 1 summarizes the speeds of addition, doubling, mixed addition and unified addition on alternate models of elliptic curves. The comparison in affine coordinates is skipped so that the cost of field inversion is so expensive. We enumerate the cost of field operations in terms of multiplication **M**, squaring **S**, and multiplication by a constant **D** in $\mathbb{F}$.

The unified addition formulae offer inherited countermeasure against SPA with comparable performance. In these models, SPA is avoided by employing the unified addition formulae or an algorithmic adaptation of it that behaves in similar fashion during the process of point addition and point doubling. Hence, for algorithmic flexibility, alternate models of elliptic curves with desirable properties are put together in this paper for elliptic curve cryptographic protocols.

Acknowledgment

We would like to express our sincere gratitude to the anonymous referees for their valuable comments, to Professor Ersan Akyıldız for his diligent guidance. An extended abstract of this paper appears in the Proceedings of 5th International Information Security and Cryptology Conference, pages 160-168, 2012.

TABLE 1
Cost of Arithmetic on Alternate Models of Elliptic Curves

EC Model	Coordinates	Addition	Doubling	Mixed Addition ($Z_2 = 1$)	Unified Addition
Weierstrass	Projective	12**M** + 2**S**	5**M**+6**S**	9**M**+2**S**	11**M** + 5**S** + 1**D**
Edwards	Projective	10**M**+1**S**+1**D**	3**M**+4**S**	9**M**+1**S**+1**D**	10**M**+1**S**+1**D**
Twisted Edwards	Projective	11**M**+2**D**	3**M**+4**S**+1**D**	9**M**+2**D**	10**M**+1**S**+2**D**
	Inverted	11**M**+2**D**	3**M**+4**S**+2**D**	9**M**+2**D**	9**M**+1**S**+2**D**
	Extended	9**M**+1**D**	4**M**+4**S**+1**D**	8**M**+1**D**	9**M**+2**D**
Jacobi Intersections	Projective	13**M**+2**S**+1**D**	4**M**+3**S**	11**M**+2**S**+1**D**	13**M**+2**S**+1**D**
Twisted Jacobi Intersections	Projective	12**M**	3**M**+4**S**+1**D**	10**M**	13**M**+2**S**+5**D**
Extended Jacobi Quartics	Jacobian	10**M**+3**S**+1**D**	1**M**+9**S**+1**D**	8**M**+3**S**+1**D**	10**M**+3**S**+1**D**
	Extended Projective	7**M**+3**S**+2**D**	8**S**	6**M**+3**S**+2**D**	8**M**+3**S**+2**D**
Hessian Curves	Projective	12**M**	12**M**	10**M**	12**M**
Generalized Hessian Curves	Projective	12**M**+1**D**	6**M**+3**S**+1**D**	10**M**+1**D**	12**M**+1**D**
Huff Curves	Projective	12**M**	6**M**+5**S**	10**M**	11**M**
Generalized Huff Curves	Projective	11**M**+3**D**	6**M**+5**S**+3**D**	10**M**+3**D**	11**M**+3**D**
New Generalized Huff Curves	Projective	12**M**+4**D**	7**M**+5**S**+4**D**	11**M**+4**D**	Open Problem

References

[1] D. Agrawal, B. Archambeault, J.R. Rao, P. Rohatgi, *The EM Side-Channel(s)*. Cryptographic Hardware and Embedded Systems - CHES 2002, Lecture Notes in Computer Science Vol. 2523. Springer-Verlag, pp. 29-45, 2003.

[2] C. Arenea, T. Lange, M. Naehrig, C. Ritzenthaler, *Faster Computation of the Tate Pairing*, Journal of Number Theory 131(5), pp. 842857, 2011.

[3] D. Bernstein and T. Lange, *Faster addition and doubling on elliptic curves*. Progress in Cryptology - Africacrypt 2007, Lecture Notes in Computer Science Vol. 4833, Springer, pp. 29-50, 2007.

[4] D. Bernstein and T. Lange, *Explicit Formulas Database*, Available at http://www.hyperelliptic.org/EFD

[5] D. Bernstein and T. Lange, *Inverted Edwards coordinates*. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 17th International Symposium - AAECC-17, Lecture Notes in Computer Science Vol. 4851, Springer, pp. 20-27, 2007.

[6] D. Bernstein, D. Kohel and T. Lange, *Twisted Hessian curves*. Available at http://www.hyperelliptic.org/EFD/g1p/auto-twistedhessian.html.

[7] D. Bernstein, T. Lange and R. R. Farashahi, *Binary Edwards Curves*. Cryptographic Hardware and Embedded Systems - CHES 2008, Lecture Notes in Computer Science Vol. 5154, Springer, pp. 244-265, 2008.

[8] D. Bernstein, P. Birkner, M. Joye, T. Lange and C. Peters, *Twisted Edwards curves*, Progress in Cryptology - Africacrypt 2008, Lecture Notes in Computer Science Vol. 5023, Springer, pp. 389-405, 2008.

[9] O. Billet and M. Joye, *The Jacobi model of an elliptic curve and side-channel analysis*, AAECC 2003, Lecture Notes in Computer Science Vol. 2643, Springer-Verlag, pp. 34-42, 2003.

[10] E. Biham and A. Shamir, *Differential fault analysis of secret key cryptosystems*. Advances in Cryptology - Crypto '97, Lecture Notes in Computer Science Vol. 1294, Springer-Verlag, pp. 513-525, 1997.

[11] E. Brier and M. Joye, *Weierstrass elliptic curves and side-channel attacks*. Public Key Cryptography - PKC 2002, Lecture Notes in Computer Science Vol. 2274, Springer, pp. 335-345, 2002.

[12] I. F. Blake, G. Seroussi and N. P. Smart, *Advances in Elliptic Curve Cryptography*, London Mathematical Society Lecture Note Series 317, Cambridge University, 2005.

[13] A. A. Ciss and D. Sow, *On a New Generalization of Huff Curves*. Available at http://eprint.iacr.org/2011/580.pdf.

[14] J. Devigne and M. Joye, *Binary Huff Curves*. Topics in Cryptology - CT-RSA 2011, Lecture Notes in Computer Science Vol. 6558, Springer, pp. 340-355, 2011.

[15] H. Edwards, *A normal form for elliptic curves*. Bulletin of the American Mathematical Society 44(3) , pp. 393-422, 2007.

[16] R. R. Farashahi and M. Joye, *Efficient Arithmetic on Hessian Curves*. Public Key Cryptography - PKC 2010, Lecture Notes in Computer Science Vol. 6056, Springer, pp. 243-260, 2010.

[17] H. Gu, D. Gu and W. Xie, *Efficient Pairing Computation*

on Elliptic Curves in Hessian form. Information Security and Cryptology - ICISC 2010, Lecture Notes in Computer Science Vol. 6829, Springer, pp. 169-176, 2011.

[18] H. Wu and R. Feng, *Elliptic curves in Huff's model*. Available at http://eprint.iacr.org/2010/390.pdf, 2010.

[19] R. Feng, M. Nie and H. Wu, *Twisted Jacobi Intersections Curves*. Available at http://eprint.iacr.org/2009/597.pdf

[20] T. S. Gustavsen and K. Ranestad, *A Simple Point Counting Algorithm for Hessian Elliptic Curves in Characteristic Three*. Appl. Algebra Eng. Commun. Comput. 17(2), pp. 141150, 2006.

[21] G. Huff, *Diophantine problems in geometry and elliptic ternary forms*. Duke Math. J., 15, pp. 443-453, 1948.

[22] H. Hisil, K. Koon-Ho Wong, G. Carter and E. Dawson, *Twisted Edwards Curves Revisited*. Advances in Cryptology - Asiacrypt 2008, Lecture Notes in Computer Science Vol. 5350, Springer-Verlag, pp. 326-343, 2008.

[23] H. Hisil, K. Koon-Ho Wong, G. Carter and E. Dawson, *Jacobi Quartic Curves Revisited*. ACISP 2009, pp. 452-468, 2009.

[24] M. Joye and J. Quisquater, *Hessian elliptic curves and side-channel attacks*. Cryptographic Hardware and Embedded Systems - CHES 2001, Lecture Notes in Computer Science Vol. 2162, Springer, pp. 402-410, 2001.

[25] M.Joye, M. Tibbouchi and D. Vergnaud, *Huff's Model for Elliptic Curves*. Algorithmic Number Theory - ANTS-IX, Lecture Notes in Computer Science Vol. 6197, Springer, pp. 234-250, 2010.

[26] P. C. Kocher, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*. Advances in Cryptology - Crypto '96, Lecture Notes in Computer Science Vol. 1109, Springer, pp. 104-113, 1996.

[27] P. Kocher, J. Jaffe and B. Jun, *Differential Power Analysis*. Advances in Cryptology - Crypto'99, Lecture Notes in Computer Science Vol. 1666, Springer-Verlag, pp. 388-397, 1999.

[28] P. Liardet and N. Smart, *Preventing SPA/DPA in ECC systems using the Jacobi form*. Cryptographic Hardware and Embedded Systems - CHES 2001, Lecture Notes in Computer Science Vol. 2162, Springer-Verlag, pp. 391-401, 2001.

[29] N. Smart and E. J. Westwood, *Point Multiplication on Ordinary Elliptic Curves over Fields of Characteristic Three*. Appl. Algebra Eng. Commun. Comput. 13(6), pp. 485-497, 2003.

[30] H. Wang, K. Wang, L. Zhang and B. Li, *Pairing Computation on Elliptic Curves of Jacobi Quartic Form*, Chinese Journal of Electronics 20(4), pp. 655-661, 2011.