Elliptic Curves in Generalized Huff's Model

Ronal Pranil Chand[1] and Maheswara Rao Valluri[2]
[1,2]School of Mathematical and Computing Sciences
Fiji National University
P.O.Box:7222, Derrick Campus, Suva, Fiji
{ronal.chand, maheswara.valluri}@fnu.ac.fj

Abstract

This paper introduces elliptic curves in generalized Huff's model. These curves endowed with addition are shown to be a group over a finite field. We present formulae for point addition and doubling point on the curves and evaluate computational cost of point addition and doubling point using projective, Jacobian and Lopez-Dahab coordinates. It is noted that the computational cost for point addition and doubling on the curves is lower on the projective coordinates than the other mentioned above coordinates.These curves are slower when compared to other forms of Huff's curve; however these are birational isomorphic to Weierstrass form.

Keywords: Doubling points, elliptic curves, groups, Huff's model, projective coordinates, scalar multiplication, birational forms.

MSC2010 (Mathematical Subject Classification): 11G05, 11G07, 14H52.

1 Introduction

Elliptic curves are algebraic curves and have been widely studied in number theory and cryptography [**?** 18, 7, 17, 21]. The study of elliptic curves could be of a variety of areas: Algebra, Algebraic Geometry, Number Theory, Diophantine problems and so on. Lang [25] mentions in his book that

"*It is possible to write endlessly on elliptic curves. (This is not a treat.)*"

In 1995, Andrew Wiles proved the *Fermat's Last Theorem* using proof of the modularity conjecture for semistable elliptic curves [30]. The use of elliptic curves have commercialized and are studied intensively for its application in cryptography [15, 8, 9].

The plane curves of degree 3 are known as cubics and have the general form of

$$Ax^3 + Bx^2y + Cxy^2 + Dy^3 + Ex^2 + Fxy + Gy^2 + Hx + Iy + J = 0.$$

Elliptic curves are non-singular cubic curves and have points defined over a field $\mathbb{K}$ [14, 29].

In the mid-1980s, Koblitz and Miller independently proposed Elliptic Curve Cryptography (ECC) using Elliptic Curve Discrete Logarithmic Problem (ECDLP) [23, 26]. The ECC provides better security when compared to Diffie-Hellman (DH) key exchange and Rivest-Shamir-Adleman (RSA) algorithm using substantially lower key sizes but the arithmetic underlying group is more tedious, which makes the study particularly interesting for systems with confined computing power and memory [24].

Some of the famous forms of elliptic curves existing in literature are Weierstrass cubics [14, 29], Hessian curves [6, 21], Jacobi quartics [7], Montgomery [27], Edwards [4, 5, 13, 2, 11] and Huff's curve [18]. There has been a lot of development to these models of elliptic curves, for instance, Joye et al. studied Huff's model for elliptic curves in 2010 [22]. In 2012, Wu and Feng also carried out research on Huff's curves in [31]. A year later, Binary Huff's curves were investigated by Devigne and Joye [12]. In 2015, He et al. [17] studied generalized Huff's curves. The recent study on Huff's curves was done by Orhon and Hisil in [28]. The different families of Huff's elliptic curves studied over the past decade are listed below.

1. The curves over a field $\mathbb{K}$, $\text{char}(\mathbb{K}) \neq 2$ by Joye et al. in [22] are of the form of:
$$ax(y^2 - 1) = by(x^2 - 1), \text{where } a^2 - b^2 \neq 0,$$

2. The generalized Huff's curves over a field $\mathbb{K}$, $\text{char}(\mathbb{K}) \neq 2$ by Joye et al. in [22] are of the form of:
$$ax(y^2 - d) = by(x^2 - d), \text{where } abd(a^2 - b^2) \neq 0,$$

3. The generalized Huff's curves over a field $\mathbb{K}$, $\text{char}(\mathbb{K}) \neq 2$ by Wu and Feng in [31] are of the form of:
$$x(ay^2 - 1) = y(bx^2 - 1), \text{where } ab(a - b) \neq 0,$$

4. The binary Huff curves over a field $\mathbb{K}$, $\text{char}(\mathbb{K}) = 2$ by Joye et al. in [12] are of the form of:
$$ax(y^2 + y + 1) = by(x^2 + x + 1), \text{where } ab(a - b) \neq 0,$$

5. The generalized binary Huff curves over a field $\mathbb{K}$, $\text{char}(\mathbb{K}) = 2$ by Joye et al. in [22] are of the form of:
$$ax(y^2 + fy + 1) = by(x^2 + fx + 1), \text{where } abf(a - b) \neq 0,$$

6. The generalized Huff's curves over a field $\mathbb{K}$, $\text{char}(\mathbb{K}) \neq 2$ by Ciss and Sow in [10] are of the form of:
$$ax(y^2 - c) = by(x^2 - d), \text{where } abcd(a^2c - b^2d) \neq 0.$$

7. The generalized Huff's curves over finite field $\mathbb{K}$, $\text{char}(\mathbb{K}) \neq 2$ by Orhon and Hisil in [28] are of the form of:
$$y(1 + ax^2) = cx(1 + dy^2)$$
, where, $acd(a - c^2d) \neq 0$.

We can also find similar progress of other elliptic curves. For instance, after the introduction of Edwards curve in [13] by Harold Edwards, it became an active area of research resulting in an extensive literature [3, 4, 5, 19, 1, 2].

In this paper, we propose a generalization of Huff's model of elliptic curves over a field $\mathbb{K}$, char($\mathbb{K}$) $\neq 2$ which are of the form

$$E(\mathbb{K}) : ax\left(y^2 + xy + f\right) = by\left(x^2 + xy + g\right),$$

where $a, b, f, g \in \mathbb{K}$ and $abfg(a-b) \neq 0$, and under appropriate addition operation shows that these curves satisfy axioms of an abelian group. Furthermore, we provide formulae for point addition and doubling point in affine, projective, Jacobian and Lopez-Dahab coordinates, including an estimate of the number of points on E over a field $\mathbb{K}$, and evaluate computational cost in each coordinate systems and compare computational cost with other known Huff's curves.

The rest of the paper is organized as follows. In Section 2, we show that the proposed generalized Huffs model curves are commutative groups over a finite field and give formulae for point addition and doubling points for affine, projective, Jacobian, and Lopez-Dahab coordinates, including an estimate of the number of points on $E(\mathbb{K})$. We also show that these forms of Huff's curves are birational isomorphic to Weierstrass form. Furthermore, we give computational costs and comparison for different projective coordinates. Finally, we conclude in Section 3 with prospects of future study.

2 Generalized Huff's Model

Let $\mathbb{K}$ be a finite field of characteristic $\neq 2$. We define an elliptic curve, denote it by E over $\mathbb{K}$ as

$$E(\mathbb{K}) : ax\left(y^2 + xy + f\right) = by\left(x^2 + xy + g\right), \tag{2.1}$$

where $a, b, f, g \in \mathbb{K}$ and $abfg(a-b) \neq 0$. The $j-invariant$ of E is given by $\frac{256\left(a^2f^2+abfg+b^2g^2\right)^3}{a^2b^2f^2g^2(af+bg)^2}$.The inflection point $(0, 0, 1)$ of $E(\mathbb{K})$ has the tangent line

as $bgy = afx$, that passes through the curve with the multiplicity of 3, thus $O = (0 : 0 : 1)$ is a neutral point of $E(\mathbb{K})$. Furthermore, we denote group law as $\oplus$. Figure 2.1 shows that the line passing through the points P and Q, and intersecting at third point R on $E(\mathbb{K})$.

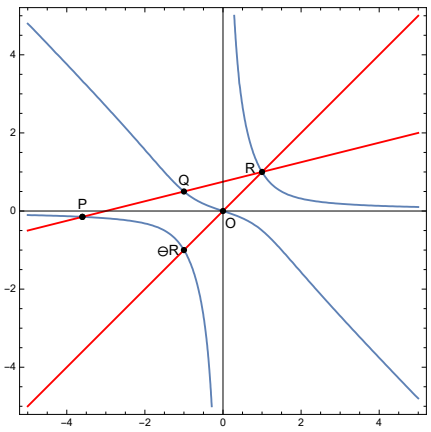

Figure 2.1: An example of the elliptic curve $E(\mathbb{K})$

Let $P = (X_1 : Y_1 : Z_1)$, $Q = (X_2 : Y_2 : Z_2)$ and $R = (X_3 : Y_3 : Z_3)$ be three points on $E(\mathbb{K})$. Then, $P \oplus Q$ could be obtained by the line connecting R and O that intersects at third point $\ominus R$ on $E(\mathbb{K})$ such that
$P \oplus Q = \ominus R$ which implies that $P \oplus Q \oplus R = O$. In particular, the inverse of the point P is $\ominus P = (X_1 : Y_1 : -Z_1)$. It is clear that the curve $E(\mathbb{K})$ posses commutative law. We note that there are three points at infinity, namely $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(a : b : 0)$ on $E(\mathbb{K})$, and the sum of any two points at infinity equals to the third point. For any point $(X_1 : Y_1 : Z_1)$, when $Z_1 \neq 0$, for some real number α and γ bounded by the field $\mathbb{K}$, we observe that

$$(1 : 0 : 0) \oplus (X_1 : Y_1 : Z_1) = (\alpha Z_1^2 : -X_1Y_1 : X_1Z_1) \text{ and}$$

$$(0 : 1 : 0) \oplus (X_1 : Y_1 : Z_1) = (-X_1Y_1 : \gamma Z_1^2 : Y_1Z_1).$$

Furthermore, we note that

$$(a : b : 0) \oplus (X_1 : Y_1 : Z_1) = (0 : 1 : 0) \oplus (\alpha Z_1^2 : -X_1Y_1 : X_1Z_1), \text{ therefore}$$

$$(a : b : 0) \oplus (X_1 : Y_1 : Z_1) = \begin{cases} (a : b : 0) \text{ if } (X_1 : Y_1 : Z_1) = (0 : 0 : 1) \\ (-\alpha Y_1Z_1 : -\gamma X_1Z_1 : X_1Y_1) \quad \text{otherwise} \end{cases}.$$

We have doubling point if $P = Q$, thus the line connecting P and Q is the tangent at the point P.

2.1 Affine formulae

In this Subsection, we provide explicit formulae for the group law for the elliptic curve defined by equation 4.1 where $a, b, f, g \in \mathbb{K}$ and $abfg(a - b) \neq 0$.

Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $R = (x_3, y_3)$ be the three different points on $E(\mathbb{K})$ such that R is obtained by connecting a line through P and Q. Let the secant line joining P and Q have the slope defined as $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$. Thus, $y = \lambda x + \beta$ is the equation of the secant line passing through the points P, Q and R, where $\beta = y_1 - \lambda x_1$. For the curve equation
$ax(y^2 + xy + f) = by(x^2 + xy + g)$, we can replace y with $\lambda x + \beta$.

$$\begin{aligned} ax((\lambda x+\beta)^2+x(\lambda x+\beta)+f) &= b(\lambda x+\beta) \\ &\quad (x^2+x(\lambda x+\beta)+g) \\ x\left(af+a\beta^2\right)+x^2(a\beta+2a\beta\lambda) & \\ +x^3\left(a\lambda+a\lambda^2\right) &= (bg\beta+x\left(b\beta^2+bg\lambda\right) \\ &\quad +x^2(b\beta+2b\beta\lambda)+x^3\left(b\lambda+b\lambda^2\right) \end{aligned}$$

Let

$$A = a\beta - b\beta + 2a\beta\lambda - 2b\beta\lambda$$

and

$$B = a\lambda - b\lambda + a\lambda^2 - b\lambda^2$$

then

$$-bg\beta + x\left(af + a\beta^2 - b\beta^2 - bg\lambda\right) + Ax^2 + Bx^3 = 0.$$

We now note that

$$x_1 + x_2 + x_3 = -\frac{A}{B}$$

$$-x_3 = x_1 + x_2 + \frac{a\beta - b\beta + 2a\beta\lambda - 2b\beta\lambda}{a\lambda - b\lambda + a\lambda^2 - b\lambda^2}$$

substituting $\beta = y_1 - \lambda x_1$ and $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$.

$$\begin{aligned} x_3 &= -\left(x_1 + x_2 + \frac{(x_1 - x_2 + 2y_1 - 2y_2)\left(-x_2y_1 + x_1y_2\right)}{(y_1 - y_2)\left(x_1 - x_2 + y_1 - y_2\right)}\right) \\ &= -x_1 - x_2 - \frac{(x_1 - x_2 + 2y_1 - 2y_2)\left(-x_2y_1 + x_1y_2\right)}{(y_1 - y_2)\left(x_1 - x_2 + y_1 - y_2\right)} \end{aligned}$$

which simplifies to

$$x_3 = -\frac{(x_1 - x_2)\left(y_1\left(x_1 + y_1\right) - y_2\left(x_2 + y_2\right)\right)}{(y_1 - y_2)\left(x_1 - x_2 + y_1 - y_2\right)}. \tag{2.2}$$

We claim, by symmetry that

$$y_3 = -\frac{(y_1 - y_2)\left(x_1^2 + x_1y_1 - x_2\left(x_2 + y_2\right)\right)}{(x_1 - x_2)\left(x_1 - x_2 + y_1 - y_2\right)}. \tag{2.3}$$

Thus, this is an evidence that the curve $E(\mathbb{K})$ has three points $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $R = (x_3, y_3)$. We observe that inverse of the point R is $\ominus R = (-x_3, -y_3)$. We note that the point $R = (x_3, y_3)$ is computed only when $x_1 \neq x_2$, $y_1 \neq y_2$ and $x_1 - x_2 + y_1 - y_2 \neq 0$ and the addition formula used in the affine coordinate system could not be employed for doubling points since $x_1 \neq x_2$ and $y_1 \neq y_2$.

Theorem 1. *Let*

$$E \quad : \quad ax(y^2 + xy + f) \quad = \quad by(y^2 + xy + g) \quad \text{with} \quad abfg(a - b) \quad \neq \quad 0$$

be an elliptic curve with points P, Q and $\mathcal{O} = (0,0)$ as neutral point on E . Then E has the following properties:

1. *If $P = \mathcal{O}$, then $P \oplus Q = Q$.*
2. *Otherwise, if $Q = \mathcal{O}$, then $P \oplus Q = P$.*
3. *Otherwise, let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$.*
4. *If $-x_1 = x_2$ and $-y_1 = y_2$, then $P \oplus Q = \mathcal{O}$.*
5. *Otherwise, let*

   $x_3 = -\frac{(x_1-x_2)(y_1(x_1+y_1)-y_2(x_2+y_2))}{(y_1-y_2)(x_1-x_2+y_1-y_2)}$ *and* $y_3 = -\frac{(y_1-y_2)\left(x_1^2+x_1y_1-x_2(x_2+y_2)\right)}{(x_1-x_2)(x_1-x_2+y_1-y_2)}$.

   Then $P \oplus Q = (-x_3, -y_3)$

Proof. Parts (1) and (2) are similar concept and is easy to see. For (1), P is neutral point (0,0), then the line through P and Q intersects E with multiplicity of 3, as P, Q and $-Q$. To obtain $P \oplus Q$, one must take the inverse of the third point of the intersection. Thus, $-(-Q) = Q$. Similar proof follows for (2). Part (4) is also easily obtained. If $P = (x_1, y_1)$ and $Q = (x_2, y_2) = (-x_1, y_1)$ then the third point of intersection of P and Q is $\mathcal{O}$. The inverse of $\mathcal{O}$ is $-\mathcal{O} = \mathcal{O}$. To prove (5), we take algebraic step. We note that if points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are two distinct points on E and neither of them equivalent to $\mathcal{O}$ then the line through points P and Q has the slope as λ. The line equation could be written as $y = \lambda x + \beta$, where $\beta = y_1 - \lambda x_1$. Substituting the line equation in E gives us the following:

$$ax\left(f + (\beta + \lambda x)^2 + x(\beta + \lambda x)\right) = b(\beta + \lambda x)\left(f + x^2 + x(\beta + \lambda x)\right)$$

$$\begin{aligned}\left(a\lambda^2 + a\lambda - b\lambda^2 - b\lambda\right)x^3 + (2a\beta\lambda + a\beta - 2b\beta\lambda - b\beta)x^2 \\ + \left(a\beta^2 + af - b\beta^2 - bf\lambda\right)x - b\beta f = 0\end{aligned}$$

It is clear that x_1 and $x_2$and two roots of the above cubic equation thus we can write,

$$\begin{aligned}(x - x_1)(x - x_2)(x - x_3) = x^3 + (-x_1 - x_2 - x_3)x^2 \\ + (xx_2 + x_3x_2 + x_1x_3)x - x_1x_2x_3.\end{aligned}$$

Then the proof simply follows the derivation of equation 2.2 and equation 2.3. □

We now define a point of infinity on $E(\mathbb{K})$ as $\mathcal{O} = (0, 0)$. For the point $P = (x_1, y_1)$, we have $\ominus P = (-x_1, -y_1)$. Thus, it follows that

$$\begin{aligned} x_3 &= -\frac{(x_1 - x_2)(y_1(x_1 + y_1) - y_2(x_2 + y_2))}{(y_1 - y_2)(x_1 - x_2 + y_1 - y_2)} \\ &= -\frac{(x_1 - -x_1)(y_1(x_1 + y_1) - -y_2(-x_2 - y_2))}{(y_1 - -y_2)(x_1 - -x_2 + y_1 - -y_2)} \\ &= -\frac{(x_1 + x_1)(y_1(x_1 + y_1) + y_1(-x_1 - y_1))}{(y_1 - -y_1)(x_1 - -x_1 + y_1 - -y_1)} \\ &= -\frac{(2x_1)(0)}{(2y_1)(2x_1 + 2y_1)} \\ &= 0 \end{aligned}$$

and

$$\begin{aligned} y_3 &= -\frac{(y_1 - y_2)(x_1^2 + x_1y_1 - x_2(x_2 + y_2))}{(x_1 - x_2)(x_1 - x_2 + y_1 - y_2)} \\ &= -\frac{(y_1 - -y_1)(x_1^2 + x_1y_1 - -x_1(-x_1 - y_1))}{(x_1 - -x_1)(x_1 - -x_1 + y_1 - -y_1)} \\ &= -\frac{(2y_1)(x_1^2 + x_1y_1 + x_1(-x_1 - y_1))}{(x_1 + x_1)(x_1 + x_1 + y_1 + y_1)} \\ &= -\frac{(2y_1)(0)}{(2x_1)(2x_1 + 2y_1)} \\ &= 0. \end{aligned}$$

Thus $P \oplus (\ominus P) = \mathcal{O}$.

Corollary 2. *The identity $\mathcal{O}$ is always on the elliptic curve defined by*

$$E : ax(y^2 + xy + f) = by(y^2 + xy + g).$$

Theorem 3. *A line cutting $E(\mathbb{K})$ at three distinct points namely P,Q and R add up to give $\mathcal{O} = (0, 0)$.*

Proof. We now show that the curve $E(\mathbb{K})$ holds associative law, that is
$P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$.
For x-coordinates,
we have

$$Q \oplus R = \frac{(x_2 - x_3)(y_2(x_3 + y_2) - y_3(x_3 + y_3))}{(y_2 - y_3)(x_2 - x_3 + y_2 - y_3)}$$

and by equation 4.1,

$$P = \frac{(x_2 - x_3)(y_2(x_3 + y_2) - y_3(x_3 + y_3))}{(y_2 - y_3)(x_2 - x_3 + y_2 - y_3)}$$

then

$$\begin{aligned} P \oplus (Q \oplus R) &= -\frac{(x_2 - x_3)\,(y_2\,(x_3 + y_2) - y_3\,(x_3 + y_3))}{(y_2 - y_3)\,(x_2 - x_3 + y_2 - y_3)} + \\ &\quad \frac{(x_2 - x_3)\,(y_2\,(x_3 + y_2) - y_3\,(x_3 + y_3))}{(y_2 - y_3)\,(x_2 - x_3 + y_2 - y_3)}. \\ &= 0 \end{aligned}$$

For

$$\begin{aligned} (P \oplus Q) \oplus R &= -\frac{(x_1 - x_2)\,(y_1\,(x_1 + y_1) - y_2\,(x_2 + y_2))}{(y_1 - y_2)\,(x_1 - x_2 + y_1 - y_2)} + \\ &\quad \frac{(x_1 - x_2)\,(y_1\,(x_1 + y_1) - y_2\,(x_2 + y_2))}{(y_1 - y_2)\,(x_1 - x_2 + y_1 - y_2)} \\ &= 0 \end{aligned}$$

For y-coordinates, we have

$$\begin{aligned} P \oplus (Q \oplus R) &= -\frac{(y_2 - y_3)\,(x_2^2 + x_2 y_2 - x_3\,(x_3 + y_3))}{(x_2 - x_3)\,(x_2 - x_3 + y_2 - y_3)} \\ &\quad + \frac{(y_2 - y_3)\,(x_2^2 + x_2 y_2 - x_3\,(x_3 + y_3))}{(x_2 - x_3)\,(x_2 - x_3 + y_2 - y_3)}. \\ &= 0 \end{aligned}$$

and

$$\begin{aligned} (P \oplus Q) \oplus R &= -\frac{(y_1 - y_2)\,(x_1^2 + x_1 y_1 - x_2\,(x_2 + y_2))}{(x_1 - x_2)\,(x_1 - x_2 + y_1 - y_2)} + \\ &\quad \frac{(y_1 - y_2)\,(x_1^2 + x_1 y_1 - x_2\,(x_2 + y_2))}{(x_1 - x_2)\,(x_1 - x_2 + y_1 - y_2)} \\ &= 0 \end{aligned}$$

In both scenario we get $\mathcal{O}$. Now to get final point we must reflect $\mathcal{O}$ on $\mathcal{O}$ (ie: $\mathcal{O} \oplus \mathcal{O}$), however $\mathcal{O}$ is the neutral point thus, we have

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

□

The slope of the tangent line on the curve defined by equation 2.1, where $abfg(a - b) \neq 0$ could be computed by implicit differentiation, thus by differentiation of $E(\mathbb{K})$ with respect to x, we have

$$\begin{aligned} af + 2axy + ay^2 + ax^2y' + 2axyy' &= 2bxy + by^2 + bgy' + bx^2y' + 2bxyy' \\ y' &= \frac{af + 2axy + ay^2 - 2bxy - by^2}{bg - ax^2 + bx^2 - 2axy + 2bxy}. \end{aligned}$$

For the point $P = (x_1, y_1)$, we can describe the slope as

$$\lambda_p = \frac{af + 2ax_1y_1 + ay_1^2 - 2bx_1y_1 - by_1^2}{bg - ax_1^2 + bx_1^2 - 2ax_1y_1 + 2bx_1y_1} = \frac{af + (a-b)y_1\,(2x_1 + y_1)}{bg - (a-b)x_1\,(x_1 + 2y_1)}.$$

Let

$$A_1 = afx_1 + (2af + bg + (a-b)x_1^2)\,y_1,\ A_2 = 3(a-b)x_1y_1^2 + 2(a-b)y_1^3,$$
$$A_3 = (bg - (a-b)x_1\,(x_1 + 2y_1))$$

and

$$B_1 = (af + (a-b)y_1\,(2x_1 + y_1)),\ B_2 = 2(-a+b)x_1^3 + bgy_1 + 3(-a+b)x_1^2y_1,$$
$$B_3 = x_1\,(af + 2bg + (-a+b)y_1^2).$$

We claim that

$$x_2 = -\frac{A_3\,(A_1 + A_2)}{(af + bg + (-a+b)x_1^2 + (a-b)y_1^2)\,(af + (a-b)y_1\,(2x_1 + y_1))}$$

and

$$y_2 = -\frac{B_1\,(B_2 + B_3)}{(af + bg + (-a+b)x_1^2 + (a-b)y_1^2)\,(bg - (a-b)x_1\,(x_1 + 2y_1))}$$

are the second coordinates of the point of intersection for the tangent line at P. We can prove our claim by simply checking the slope given by

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

and by simplification, we can obtain

$$\lambda = \frac{af + (a-b)y_1\,(2x_1 + y_1)}{bg - (a-b)x_1\,(x_1 + 2y_1)}$$

which have the same slope as λ_p.

2.2 Projective formulae

Let $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ and $Z = 1$ [14, 29], then the affine coordinate of equation 2.1, where $a, b, f, g \in \mathbb{K}$ and $abfg(a-b) \neq 0$ becomes

$$a\frac{X}{Z}\left(\frac{Y^2}{Z^2} + \frac{XY}{Z^2} + f\right) = b\frac{Y}{Z}\left(\frac{X^2}{Z^2} + \frac{XY}{Z^2} + g\right).$$

Finally, multiplying by Z^3 on both the sides to get rid of denominators and achieve the projective form of the curve equation
$E(\mathbb{K}) : aX\left(Y^2 + XY + fZ^2\right) = bY\left(X^2 + XY + gZ^2\right)$, where $a, b, f, g \in \mathbb{K}$ and $abfg(a-b) \neq 0$.

For the point $P = (X_1, Y_1, Z_1)$ and $Q = (X_2, Y_2, Z_2)$, the third point of intersection known as $R = (U_3, V_3, W_3)$ of the line joining P and Q has the coordinates as follows:

$$\begin{aligned}
U_3 =& (X_2Z_1 - X_1Z_2)^2(Y_2Z_1^2(X_2 + Y_2) - Y_1Z_2^2(X_1 + Y_1)) \\
V_3 =& (Y_2Z_1 - Y_1Z_2)^2(X_2Z_1^2(X_2 + Y_2) - X_1Z_2^2(X_1 + Y_1)) \\
W_3 =& - Z_1Z_2(X_2Z_1 - X_1Z_2)(Y_2Z_1 - Y_1Z_2)(Z_1(X_2 + Y_2) - Z_2(X + Y_1)).
\end{aligned} \tag{2.4}$$

For doubling points, the coordinates are as follows:

$$\begin{aligned}
U_2 &= -(X_1(a-b)(X + 2Y_1) - bgZ_1^2)^2 \\
&\quad (Y_1(a-b)(X_1 + Y_1)(X_1 + 2Y_1) + Z_1^2(afX_1 + (2af + bg)Y_1)) \\
V_2 &= -(Y_1(a-b)(2X_1 + Y_1) + afZ_1^2)^2 \\
&\quad (-X_1(a-b)(X_1 + Y_1)(2X_1 + Y_1) + Z_1^2(X_1(af + 2bg) + bgX_1)) \\
W_2 &= Z_1(Y_1(a-b)(2X_1 + Y_1) + afZ_1^2)(-X_1(a-b)(X_1 + 2Y_1) + bgZ_1^2) \\
&\quad (-(a-b)(X_1^2 - Y_1^2) + (af + bg)Z_1^2).
\end{aligned} \tag{2.5}$$

Theorem 4. *Let $\mathbb{K}$ be a finite field of characteristic $\neq 2$. Let $P_1 = (X_1, Y_1, Z_1)$ and $P_2 = (X_2, Y_2, Z_2)$ be two points on $E(\mathbb{K})$. Then, the addition formula given by equation 2.4 is valid provided that $X_1Z_2 \neq X_2Z_1$, $Y_1Z_2 \neq Y_2Z_1$ and $X_1Z_2 + Y_1Z_2 \neq X_2Z_1 + Y_2Z_1$.*

Proof. Let P_1 and P_2 be finite, we can write $P_1 = (x_1, y_1)$, where
$(x_1, y_1) \neq (0, 0)$ and $P_2 = (x_2, y_2)$. The point addition given by the equations 2.2 and 2.3 is only valid if $x_1 \neq x_2$, $y_1 \neq y_2$ and
$x_1 - x_2 + y_1 - y_2 \neq 0$, which translate to projective coordinates as
$X_1Z_2 \neq X_2Z_1$, $Y_1Z_2 \neq Y_2Z_1$ and $X_1Z_2 + Y_1Z_2 \neq X_2Z_1 + Y_2Z_1$, respectively.

It remains to analyze that the condition is satisfied at the infinity points. The points at infinity are $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(a, b, 0)$, if P_1 or
$P_2 \in \{(1 : 0 : 0), (0 : 1 : 0)\}$, then $X_1Z_2 \neq X_2Z_1$, $Y_1Z_2 \neq Y_2Z_1$ and $X_1Z_2 + Y_1Z_2 \neq X_2Z_1 + Y_2Z_1$ is not satisfied. Since $P_1 \notin \{O, (1 : 0 : 0), (0 : 1 : 0)\}$ then the addition law is valid for $P_2 = (a : b : 0)$ as mentioned earlier. □

2.3 Jacobian formulae

Let $x = \frac{X}{Z^2}$, $y = \frac{Y}{Z^3}$ and $Z = 1$ [14, 29]. Then the affine coordinate given by equation 2.1 after simplification becomes
$E(\mathbb{K}) : aX(Y^2+XYZ+fZ^6) = bY(XZ^2+XYZ+gZ^6)$, where $a, b, f, g \in \mathbb{K}$ and $abfg(a-b) \neq 0$.

For the point $P = (X_1, Y_1, Z_1)$ and $Q = (X_2, Y_2, Z_2)$, the third point of intersection known as $R = (U_3, V_3, W_3)$ of the line joining P and Q has the coordinates as follows:

$$\begin{aligned}
U_3 &= -Z_1Z_2\left(X_2Z_1^2 - X_1Z_2^2\right)^2\left(Y_2^2Z_1^6 + X_2Y_2Z_1^6Z_2 - Y_1Z_2^6\left(Y_1 + X_1Z_1\right)\right), \\
V_3 &= -\left(Y_2Z_1^3 - Y_1Z_2^3\right)^2\left(X_2Y_2Z_1^5 + X_2^2Z_1^5Z_2 - X_1Z_2^5\left(Y_1 + X_1Z_1\right)\right), \\
W_3 &= Z_1^2Z_2^2\left(Y_2Z_1^3 - Y_1Z_2^3\right)\left(X_2Z_1^3Z_2 - X_1Z_1Z_2^3\right)\left(Y_2Z_1^3 + X_2Z_1^3Z_2 - Z_2^3\left(Y_1 + X_1Z_1\right)\right).
\end{aligned}$$

For doubling points, the coordinates are as follows:

$$\begin{aligned}
U_2 &= -Z_1\left(2X_1Y_1(-a+b) + (-a+b)X_1^2Z_1 + bgZ_1^5\right)^2 \\
&\quad \left(2(a-b)Y_1^3 + 3(a-b)X_1Y_1^2Z_1 + afX_1Z_1^7 + Y_1Z_1^2\left((a-b)X_1^2 + (2af+bg)Z_1^4\right)\right), \\
V_2 &= -\left((a-b)Y_1^2 + 2(a-b)X_1Y_1Z_1 + afZ_1^6\right)^2 \\
&\quad \left(3(-a+b)X_1^2Y_1Z_1 + 2(-a+b)X_1^3Z_1^2 + bgY_1Z_1^5 + X_1\left((-a+b)Y_1^2 + (af+2bg)Z_1^6\right)\right), \\
W_2 &= Z_1^3\left(2(-a+b)X_1Y_1 + (-a+b)X_1^2Z_1 + bgZ_1^5\right)\left((a-b)Y_1^2 + 2(a-b)X_1Y_1Z_1 + afZ_1^6\right) \\
&\quad \left((a-b)Y_1^2 + (-a+b)X_1^2Z_1^2 + (af+bg)Z_1^6\right).
\end{aligned}$$

The costs of point addition and doubling point on the curve $E(\mathbb{K})$ are $32m+4s$ and $29m+5s$, respectively.

2.4 Lopez-Dahab formuale

Let $x = \frac{X}{Z}$, $y = \frac{Y}{Z^2}$ and $Z = 1$ [14, 29]. Then the affine coordinate given by equation 2.1 after simplification becomes
$E(\mathbb{K}) : aX(Y^2+XYZ+fZ^5) = bY(XZ^2+XY+gZ^6)$, where $a, b, f, g \in \mathbb{K}$ and $abfg(a-b) \neq 0$.

For the point $P = (X_1, Y_1, Z_1)$ and $Q = (X_2, Y_2, Z_2)$, the third point of intersection known as $R = (U_3, V_3, W_3)$ of the line joining P and Q has the coordinates as follows:

$$\begin{aligned}
U_3 &= -Z_1Z_2\left(X_2Z_1 - X_1Z_2\right)^2\left(Y_2^2Z_1^4 + X_2Y_2Z_1^4Z_2 - Y_1Z_2^4\left(Y_1 + X_1Z_1\right)\right), \\
V_3 &= -\left(Y_2Z_1^2 - Y_1Z_2^2\right)^2\left(X_2Y_2Z_1^3 + X_2^2Z_1^3Z_2 - X_1Z_2^3\left(Y_1 + X_1Z_1\right)\right), \\
W_3 &= Z_1^2Z_2^2\left(X_2Z_1 - X_1Z_2\right)\left(Y_2Z_1^2 - Y_1Z_2^2\right)\left(Y_2Z_1^2 + Z_2\left(X_2Z_1^2 - Z_2\left(Y_1 + X_1Z_1\right)\right)\right).
\end{aligned}$$

For doubling points, the coordinates are as follows:

$$
\begin{aligned}
U_2 &= -Z_1\left(2(-a+b)X_1Y_1+(-a+b)X_1^2Z_1+bgZ_1^3\right)^2 \\
&\quad \left(2(a-b)Y_1^3+3(a-b)X_1Y_1^2Z_1+afX_1Z_1^5+Y_1Z_1^2\left((a-b)X_1^2+(2af+bg)Z_1^2\right)\right), \\
V_2 &= -\left((a-b)Y_1^2+2(a-b)X_1Y_1Z_1+afZ_1^4\right)^2 \\
&\quad \left(3(-a+b)X_1^2Y_1Z_1+2(-a+b)X_1^3Z_1^2+bgY_1Z_1^3+X_1\left((-a+b)Y_1^2+(af+2bg)Z_1^4\right)\right), \\
W_2 &= Z_1^2\left(2(-a+b)X_1Y_1+(-a+b)X_1^2Z_1+bgZ_1^3\right)\left((a-b)Y_1^2+2(a-b)X_1Y_1Z_1+afZ_1^4\right) \\
&\quad \left((a-b)Y_1^2+(-a+b)X_1^2Y_1^2+(af+bg)Z_1^4\right).
\end{aligned}
$$

The costs of point addition and doubling point on the curve $E(\mathbb{K})$ are $32m+6s$ and $26m+5s$, respectively.

2.5 Rational Points on $E(\mathbb{K})$

For the elliptic curve defined by equation 2.1 we replace $\mathbb{K}$ by $\mathbb{F}_q$, where q is a prime. We observe that for each x yields at most two values for y, and the point of infinity $(0,0)$ is always on the curve $E(\mathbb{F}_q)$. Thus, we can set up an upper bound for the number of rationals on $E(\mathbb{F}_q)$ as

$$\#E(\mathbb{F}_q) \leq 2q+1.$$

However, computing the exact number of points on the curve $E(\mathbb{F}_q)$ is a challenge to us. Hasse's theorem [16] on elliptic curve $E(\mathbb{F}_q)$ provides an estimate on the number of points over the finite field $\mathbb{F}_q$ as

$$\mid \#E(\mathbb{F}_q)-(q+1) \mid \leq 2\sqrt{q}.$$

For the understanding purpose, the curve
$E(\mathbb{F}_q): ax\left(y^2+xy+f\right)=by\left(x^2+xy+g\right)$, where $a,b,f,g \in \mathbb{F}_q$ and $abfg(a-b)\neq 0$ with the condition
$abfg(a-b)\neq 0$ could be rearranged as
$afx+\left(-bg+ax^2-bx^2\right)y+(ax-bx)y^2=0$ and may be seen as quadratic equation of y. The discriminant can be calculated by
$\Delta=-4afx(ax-bx)+\left(-bg+ax^2-bx^2\right)^2$and y can be rational if and only if $\Delta=j^2$ for some rational j. The variables of the curve are a,b,g and f and we can easily find some points on the curve by simply assigning values of a,f and g and solving for b. The examples below will show how one can obtain y coordinate.

Example 5. We assign $a=1$, $f=1$, $x=1$ and $g=-1$. The discriminant formula then becomes

$$
\begin{aligned}
i^2 &= -4a(ax-bx)+(-bg+ax^2-bx^2)^2 \\
i^2 &= -4(1-b)+1 \\
i^2 &= 4b-3.
\end{aligned}
$$

We note that $4b-3$ should be a rational square. Thus choosing
$4b-3=1$ yields $b=1$ but we omit this value due to the initial condition of the curve. We now use $4b-3=4$ and it gives $b=3$. Now our curve becomes $E(\mathbb{F}_{17}):\ x\left(y^2+xy+1\right)=3y\left(x^2+xy-1\right)$ which has a rational coordinate of $(1,1)$. Since $(1,1)$ is on the curve then so does $(-1,-1)$. We now apply point doubling formula on the points $(1,1)$ and $(-1,-1)$. The solution to $(1,1)$ is another point $(\frac{18}{5},-\frac{10}{3})$ and solution to $(-1,-1)$ is $(-\frac{18}{5},\frac{10}{3})$. We now apply point addition of the point $(1,1)$ and $(-\frac{18}{5},\frac{10}{3})$ which yields $(\frac{299}{119},\frac{91}{391})$. We can also apply point addition of points $(-1,-1)$ and $(\frac{18}{5},-\frac{10}{3})$ which yields $(-\frac{299}{119},-\frac{91}{391})$. We can use this method to generate more points on the curve $E(\mathbb{F}_{17})$.

Theorem 6. *If (x,y) is a rational point on*

$$E(\mathbb{K}):ax\left(y^2+xy+f\right)-by\left(x^2+xy+g\right)=0$$

and $x\neq 0$, $y\neq 0$,then $(-x,-y)$ is also rational point on $E(\mathbb{K})$.

Proof. It is clear that if (x,y) is rational then $(-x,-y)$ also rational. All we have to do is to show that $(-x,-y)$ is also on $E(\mathbb{K})$. Substituting $(-x,-y)$ in $E(\mathbb{K})$ gives the following,

$$\begin{aligned} a(-x)\left((-y)^2+(-x)(-y)+f\right)-b(-y)\left((-x)^2+(-x)(-y)+g\right)&=0\\ -ax\left(y^2+xy+f\right)+by\left(x^2+xy+g\right)&=0\\ E(\mathbb{K}):\ ax\left(y^2+xy+f\right)-by\left(x^2+xy+g\right)&=0. \end{aligned}$$

Thus, $(-x,-y)$ is also rational point on $E(\mathbb{K})$. □

2.6 Birational Equivalence of Our Huff's curve to Weierstrass Form.

Let E be a non-singular elliptic curve defined by the affine formulae defined by equation 2.1. We will show that E is birational equivalence to Weierstrass form. It is easy to see that E is also equivalent to

$$axy^2+ax^2y+axf=bx^2y+bxy^2+byg.$$

The signs of a,b,f and g are either positive or negative and never equal to zero. The curve has $O=(0,0)$ as a neutral point and is a point of inflection. The curve also has $(0:1:0)$, the point at infinity in projective transformation. For simplicity we take E of the following form:

$$E:\ (a-b)XY^2+(a-b)X^2Y+afXZ^2-bgYZ^2=0.$$

In chapter 8 [20], Cassels states that an elliptic curve genus 1 with at least a rational point on the curve and Weierstrass form is enough to get the birational equivalence to curve and where $\mathcal{O}$ is on Weierstrass curve. If the curve has an inflectional tangent at Point O then let $\mathcal{O}=(0:1:0)$. The linear transformation of co-ordinates is enough to take O to $\mathcal{O}$. We define $O=(0:0:1)$ an inflection point on E. We will first map O to curve E_M.

Let

$$\psi=(X:Y:Z)\longmapsto(U:V:W)=(U:\frac{af}{bg}U+W,\,V).$$

then with little bit of help from mathematica we have following parameters:

$$\begin{aligned} A &= a(a-b)f(af+bg), \\ B &= (a-b)bg(2af+bg)\,, \\ C &= b^3g^3\,, \\ D &= (a-b)b^2g^2. \end{aligned}$$

Then we achieve $E_M = AU^3 + BU^2W + DUW^2 - CV^2W = 0$. One can note that E_M could be easily changed to Weierstrass form. To return back to Huffs elliptic curve from E_M one may apply the following map:

$$\psi^{-1} = (U\,:\,V\,:\,W) \longmapsto (X\,:\,Y\,:\,Z) = (X\,:\,Z\,:\,\frac{-af}{bg}X + Y\,).$$

It is noted that (0:0:1) on E is mapped to (0:1:0) on E_M through ψ.

To achieve Weierstrass affine form we let,

$X = x$, $V = \dfrac{A}{C}y$ and $Z = \dfrac{C}{A}$ then we can simplify the equation

$$E_M =: y^2 = x^3 + \frac{BC}{A^2}x^2 + \frac{DC^2}{A^3}x.$$

After achieving affine equation of E_M we let $x = t + \dfrac{A}{BC}$ to achieve the following Weierstrass form as

$$E_w : y^2 = t^3 + a_2x^2 + a_4x + a_6,$$

where

$$\begin{aligned} a_2 &= \frac{3A^3 + B^2C^2}{A^2BC}, \\ a_4 &= \frac{3A^5 + 2A^2B^2C^2 + B^2C^4D}{A^3B^2C^2}, \\ a_6 &= \frac{A^5 + A^2B^2C^2 + B^2C^4D}{A^2B^3C^3}. \end{aligned}$$

2.7 Computational cost analysis

In this subsection, we evaluate the efficiency of point addition and doubling point on the curve $E(\mathbb{K})$. The computation cost ratio between square (s) and multiplication (m) is typically $s = 0.8m$, addition / subtraction as (a) and multiplication by curve constant as (d) . We omit other operations such as (a) and (d) as computation cost is lower.

Projective coordinates may be preferred for faster arithmetic than the affine formula. The affine formulae equation 2.2 and 2.3 for the addition of two different points on $E(\mathbb{K})$ is described by equation 2.4.

We let the cost of a multiplication be m and the cost of a square be s in the field $\mathbb{K}$. Then, we have

$$m_1 = X_1Z_2,\ m_2 = X_2Z_1,\ m_3 = Y_1Z_2,\ m_4 = Y_2Z_1,$$

$$m_5 = m_4(m_2 + m_4),\ m_6 = m_3(m_1 + m_3),\ m_7 = m_2(m_2 + m_4),\ m_8 = m_1(m_1 + m_3),$$
$$m_9 = -Z_1Z_2,$$

$$s_1 = (m_2 - m_1)^2,\ s_2 = (m_4 - m_3)^2,$$

$$U_3 = s_1(m_5 - m_6),\ V_3 = s_2(m_7 - m_8),\ W_3 = m_9(m_2 - m_1)(m_4 - m_3)(m_2 + m_4 - m_1 - m_3).$$

Therefore, the total cost of point addition on the curve $E(\mathbb{K})$ is $14m + 2s$.
For the doubling point as described by equation 2.5, we have

$$s_1 = Z_1^2,\ s_2 = X_1^2,\ s_3 = Y_1^2,$$

$$m_1 = X_1(a - b)(X_1 + 2Y_1),\ m_2 = (X_1 + Y_1)(X_1 + 2Y_1),\ m_3 = s_1(afX_1 + Y_1(2af + bg)),$$
$$m_4 = (a - b)Y_1m_2,\ m_5 = Y_1(a - b)(2X_1 + Y_1)$$

$$m_6 = (X_1 + Y_1)(2X_1 + Y_1),\ m_7 = s_1((af + 2bg)X_1 + bgY_1),\ m_8 = -X_1m_6(a - b),$$
$$m_9 = (m_5 + afs_1)((a - b)(s_2 + s_3) + s_1(af + bg))$$

$$U_2 = -(m_1 - bgs_1)^2(m_3 + m_4),\ V_2 = -(m_5 + afs_1)^2(m_7 + m_8),\ W_2 = -m_1m_9Z_1.$$

Therefore, the total cost of doubling point on the curve $E(\mathbb{K})$ is $13m + 5s$. The other forms of coordinate systems is summarizes in the table below for the computational cost of point addition and doubling point in standard coordinate.

Table 1: Computational cost comparison

Coordinates	Cost	
	Addition	Doubling
Projective	14m+2s	13m+5s
Jacobian	32m+4s	29m+5s
Lopez-Dahab	32m+6s	26m+5s

We note that the computational cost of using the projective coordinate system on the curve $E(\mathbb{K})$ is lower than the Jacobian and Lopez Dahab coordinates. Thus, we recommend using projective coordinates as the cost is lower for point addition and doubling points for this work.

To compare our results with other Huff's model we have take extra operations as a to be addition/subtraction and d as multiplication by curve constants.

Table 2: Computational cost comparison of other forms of Huff's curve

Source and the curve equation	Addition	Doubling
Wu, Feng [31] plus assuming b=1, $X(aY^2 - Z^2) = Y(X^2 - Z^2)$	11m+d+14a	6m+5s+d+12a
Joye, Tibouchi, Vergnaud [?], $aX(Y^2 - Z^2) = bY(X^2 - Z^2)$	6m+5s+13a	11m+14a
Orhon and Hisil [28], $YT(Z^2 + 2X^2) = cXZ(T^2 + 2Y^2)$	10m+14a	8m+10a
Orhon and Hisil [28], $YT(Z^2 + X^2) = cXZ(T^2 + 2Y)$	10m+12a	8m+8a
This work using projective coordinate, $aX(Y + XY + fZ^2) = bY(X^2 + XY + gZ^2)$	14m+2s+2d+12a	13m+5s+2d+3a

Its is noted that the curve described in this paper is of a higher cost than other models of curves in literature. This results suggest to improve computational cost or use mapping (isomorphism) of our curve to some fast elliptic curve such as Weierstrass form. Our next chapter deals with birational isomorphism of our curve to Weierstrass form.

3 Conclusion

This paper introduced a generalized model of Huff's elliptic curve. We have presented formulae for point addition and doubling on the affine, projective, Jacobian and Lopez-Dahab coordinates. We have noted that the computational cost of the point addition and doubling point is lower on the projective coordinates than the other mentioned coordinates. These curves have greater computational cost than other Huff's curves in literature. These forms of Huff's curves are birational isomorphic to Weierstrass form and one can extend the study to supersingular elliptic curves, improvement of the speed and isogeny-based cryptography using these curves.

References

[1] C. Arene, T. Lange, M. Naehrig, and C. Ritzenthaler. Faster computation of the tate pairing. *Journal of number theory*, 131(5):842–857, 2011.

[2] D. Bernstein, P. Birkner, T. Lange, and C. Peters. Ecm using edwards curves. *Mathematics of Computation*, 82(282):1139–1179, 2013.

[3] D. J. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 29–50. Springer, 2007.

[4] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters. Twisted edwards curves. In *International Conference on Cryptology in Africa*, pages 389–405. Springer, 2008.

[5] D. J. Bernstein, T. Lange, and R. R. Farashahi. Binary edwards curves. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 244–265. Springer, 2008.

[6] D. J. Bernstein, C. Chuengsatiansup, D. Kohel, and T. Lange. Twisted hessian curves. In *International Conference on Cryptology and Information Security in Latin America*, pages 269–294. Springer, 2015.

[7] O. Billet and M. Joye. The jacobi model of an elliptic curve and side-channel analysis. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 34–42, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg. ISBN 978-3-540-44828-0.

[8] J. Bos, C. Costello, P. Longa, and M. Naehrig. Specification of curve selection and supported curve parameters in msr ecclib. Technical report, Technical Report MSR-TR-2014-92, Microsoft Research, 2014.

[9] J. W. Bos, C. Costello, P. Longa, and M. Naehrig. Selecting elliptic curves for cryptography: An efficiency and security analysis. *Journal of Cryptographic Engineering*, 6(4): 259–286, 2016.

[10] A. A. Ciss and D. Sow. On a new generalization of huff curves. *IACR Cryptology ePrint Archive*, 2011:580, 2011.

[11] M Prem Laxman Das and Palash Sarkar. Pairing computation on twisted edwards form elliptic curves. In *International Conference on Pairing-Based Cryptography*, pages 192–210. Springer, 2008.

[12] J. Devigne and M. Joye. Binary huff curves. In *Cryptographers Track at the RSA Conference*, pages 340–355. Springer, 2011.

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

[14] S. D. Galbraith. *Mathematics of public key cryptography*. Cambridge University Press, 2012.

[15] P. Gallagher. Digital signature standard (dss). *Federal Information Processing Standards Publications, volume FIPS*, pages 186–3, 2013.

[16] H. Hasse. Zur theorie der abstrakten elliptischen funktionenkï¿œrper iii. die struktur des meromorphismenrings. die riemannsche vermutung. *Journal fï¿œr die reine und angewandte Mathematik*, 175:193–208, 1936. URL `http://eudml.org/doc/149968`.

[17] X. He, W. Yu, and K. Wang. Hashing into generalized huff curves. In *International Conference on Information Security and Cryptology*, pages 22–44. Springer, 2015.

[18] Gerald B Huff. Diophantine problems in geometry and elliptic ternary forms. *Duke Mathematical Journal*, 15(2):443–453, 1948.

[19] S. Ionica and A. Joux. Another approach to pairing computation in edwards coordinates. In *International Conference on Cryptology in India*, pages 400–413. Springer, 2008.

[20] Terence Jackson. Lectures on elliptic curves, london mathematical society student texts 24, by jws cassels. pp 137.£ 13-95 (paper)£ 27-95 (hard). 1991. isbn 0-521-42530-1,-41517-9.(cambridge university press). *The Mathematical Gazette*, 79(484):216–216, 1995.

[21] M. Joye and J. Quisquater. Hessian elliptic curves and side-channel attacks. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 402–410. Springer, 2001.

[22] M. Joye, M. Tibouchi, and D. Vergnaud. Huff's model for elliptic curves. In Guillaume Hanrot, François Morain, and Emmanuel Thomé, editors, *Algorithmic Number Theory*, pages 234–250, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg. ISBN 978-3-642-14518-6.

[23] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.

[24] N. Koblitz and A. J. Menezes. A survey of public-key cryptosystems. *SIAM review*, 46(4): 599–634, 2004.

[25] S. Lang. *Elliptic curves: Diophantine analysis*, volume 231. Springer, 1978.

[26] V. S. Miller. Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*, pages 417–426. Springer, 1985.

[27] Peter L Montgomery. Speeding the pollard and elliptic curve methods of factorization. *Mathematics of computation*, 48(177):243–264, 1987.

[28] Neriman Gamze Orhon and Huseyin Hisil. Speeding up huff form of elliptic curves. *Designs, Codes and Cryptography*, 86(12):2807–2823, 2018.

[29] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[30] A. Wiles. Modular elliptic curves and fermat's last theorem. *Annals of mathematics*, 141 (3):443–551, 1995.

[31] H. Wu and R. Feng. Elliptic curves in huff's model. *Wuhan University Journal of Natural Sciences*, 17(6):473–480, Dec 2012. ISSN 1993-4998. doi: 10.1007/s11859-012-0873-9. URL https://doi.org/10.1007/s11859-012-0873-9.