Published in G. Hanrot, F. Morain, and E. Thomé, Eds, *Algorithmic Number Theory (ANTS-IX)*, vol. 6197 of *Lecture Notes in Computer Science*, pp. 234–250, Springer, 2010.

Huff's Model for Elliptic Curves

Marc Joye[1], Mehdi Tibouchi[2,⋆], and Damien Vergnaud[2]

[1] Technicolor, Security & Content Protection Labs
1 avenue de Belle Fontaine, 35576 Cesson-Sévigné Cedex, France
marc.joye@technicolor.com
[2] École Normale Supérieure – C.N.R.S. – I.N.R.I.A.
45, Rue d'Ulm – 75230 Paris CEDEX 05 – France
{mehdi.tibouchi,damien.vergnaud}@ens.fr

Abstract. This paper revisits a model for elliptic curves over $\mathbb{Q}$ introduced by Huff in 1948 to study a diophantine problem. Huff's model readily extends over fields of odd characteristic. Every elliptic curve over such a field and containing a copy of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is birationally equivalent to a Huff curve over the original field.
This paper extends and generalizes Huff's model. It presents fast explicit formulæ for point addition and doubling on Huff curves. It also addresses the problem of the efficient evaluation of pairings over Huff curves. Remarkably, the so-obtained formulæ feature some useful properties, including completeness and independence of the curve parameters.

Key words: Elliptic curves, Huff's model, unified addition law, complete addition law, explicit formulæ, scalar multiplication, Tate pairing, Miller's algorithm.

1 Introduction

Elliptic curves have been extensively studied in algebraic geometry and number theory since the middle of the nineteenth century. More recently, they have been used to devise efficient algorithms for factoring large integers [19, 22] or for primality proving [2, 13, 23]. They also revealed useful in the construction of cryptosystems [18, 20].

In this paper, we develop an elliptic curve model introduced by Huff in 1948 to study a diophantine problem. We present fast explicit formulæ for adding or doubling points on Huff curves. We also devise a couple of extensions and generalizations upon this model. We analyze the impact of these curves in cryptographic applications. Some of our addition formulæ are unified; *i.e.*, they remain valid for doubling a point. Even better, they achieve completeness (*i.e.*, are valid for all inputs) when restricted to a cyclic subgroup, as is customary in cryptographic settings. We also consider the problem of pairing computation over Huff curves.

⋆ This research was completed while the second author was visiting the Okamoto Research Laboratory at the NTT Information Sharing Platform (Tokyo, Japan).

1.1 Background

Elliptic curves and cryptography. In 1985, Koblitz [18] and Miller [20] independently proposed the use of elliptic curves in public-key cryptography. The main advantage of elliptic curve systems stems from the absence of a subexponential-time algorithm to compute discrete logarithms on general elliptic curves over finite fields. Consequently, one can use an elliptic curve group that is smaller in size compared with systems based on either integer factorization or the discrete log problem in the multiplicative group of a finite field, while maintaining the same (heuristic) level of security (see [17] for a recent survey on elliptic curve cryptography).

The use of elliptic curves in cryptography makes the key sizes smaller but the arithmetic of the underlying group is more tedious (for example, with the widely-used Jacobian coordinates, the general addition of two points on an elliptic curve typically requires 16 field multiplications). Therefore a huge amount of research has been devoted to the analysis of the performance of various forms of elliptic curves proposed in the mathematical literature: Weierstraß cubics, Jacobi intersections, Hessian curves, Jacobi quartics, or the more recent forms of elliptic curves due to Montgomery, Doche-Icart-Kohel or Edwards (see [6] for an encyclopedic overview of these models). For instance, since 2007, there has been a rapid development of the curves introduced by Edwards in [12] and their use in cryptology. Bernstein and Lange proposed a more general version of these curves in [7] and the *inverted Edwards* coordinates in [8]. Bernstein, Birkner, Joye, Lange, and Peters studied *twisted Edwards* curves in [5]. Hisil, Wong, Carter and Dawson proposed *extended twisted Edwards* coordinates in [14]. Bernstein, Lange, and Farashahi covered the *binary case* in [9]. The first formulæ for computing *pairings* over Edwards curves were published by Das and Sarkar [11]. They were subsequently improved by Ionica and Joux [16]. The best implementation to date is due to Arène, Lange, Naehrig, and Ritzenhaler [1]. The present paper is aimed at providing a similar study for a forgotten model of elliptic curves hinted by Huff in 1948.

A diophantine problem. Huff [15] considered rational distance sets S (*i.e.*, subsets S of the plane $\mathbb{R}^2$ such that for all $s, t \in S$, the distance between s and t is a rational number) of the following form: given distinct $a, b \in \mathbb{Q}$, S contains the four points $(0, \pm a)$ and $(0, \pm b)$ on the y-axis, plus points $(x, 0)$ on the x-axis, for some $x \in \mathbb{Q}$. Such a point $(x, 0)$ must then satisfy the equations $x^2 + a^2 = u^2$ and $x^2 + b^2 = v^2$ with $u, v \in \mathbb{Q}$. The system of associated homogeneous equations $x^2 + a^2z^2 = u^2$ and $x^2 + b^2z^2 = v^2$ defines a curve of genus 1 in $\mathbb{P}^3$. Huff, and later his student Peeples [24], provided examples where this curve has positive rank over $\mathbb{Q}$, thus exhibiting examples of arbitrarily large rational distance sets of cardinality $k > 4$ such that exactly $k - 4$ points are on one line.

The above mentioned genus 1 curve is birationally equivalent to the curve

$$ax(y^2 - 1) = by(x^2 - 1) \tag{1}$$

for some parameters a and b in $\mathbb{Q}$. It is easily seen that, over any field $\mathbb{K}$ of odd characteristic, Equation (1) defines an elliptic curve if $a^2 \neq b^2$ and $a, b \neq 0$.

Indeed, if $ab \neq 0$, the gradient of the curve $F(X,Y,Z) = aX(Y^2-Z^2)-bY(X^2-Z^2)$ in the projective plane $\mathbb{P}^2(\mathbb{K})$ is

$$\left(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}, \frac{\partial F}{\partial Z}\right) = \left(a(Y^2-Z^2) - 2bXY, 2aXY - b(X^2-Z^2), 2(-aX+bY)Z\right),$$

which does not vanish at the three points at infinity $(1:0:0)$, $(0:1:0)$ and $(a:b:0)$ and vanishes at a finite point $(x:y:1)$ if and only if $ax = by$, which together with Eq. (1) implies that $x^2 = y^2$ and therefore $a^2 = b^2$. It is worth noting that in characteristic 2, the point $(1:1:1)$ is always singular and therefore the family of curves defined by (1) does not contain any smooth curve. As will be shown in Section 3, we can extend our study to even characteristic by considering a generalized model.

1.2 Contributions of the paper

Our first contribution is a detailed study of Huff's form for elliptic curves over finite fields of odd characteristic and a statement of the addition law in these groups. We show in particular that all elliptic curves over non-binary finite fields with a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ can be transformed to Huff's form. We then analyze their arithmetic and investigate several generalizations and extensions. In particular, we present explicit formulæ (*i.e.*, as a series of field operations) that

- compute a *complete* addition $(X_1:Y_1:Z_1) \oplus (X_2:Y_2:Z_2)$ using $12\mathsf{m}$;
- compute a *unified* addition $(X_1:Y_1:Z_1) \oplus (X_2:Y_2:Z_2)$ using $11\mathsf{m}$;
- compute a mixed addition $(X_1:Y_1:Z_1) \oplus (X_2:Y_2:1)$ using $10\mathsf{m}$;
- compute a doubling $[2](X_1:Y_1:Z_1)$ using $6\mathsf{m}+5\mathsf{s}$

where m and s denote multiplications and squarings in the base field $\mathbb{K}$.

As a further contribution, since bilinear pairings have found numerous applications in cryptography, we also present formulæ for computing Tate pairings using Huff's form. Specifically, we present explicit formulæ that

- compute a *full* Miller addition using $1\mathsf{M}+(k+15)\mathsf{m}$;
- compute a *mixed* Miller addition using $1\mathsf{M}+(k+13)\mathsf{m}$;
- compute a Miller doubling using $1\mathsf{M}+1\mathsf{S}+(k+11)\mathsf{m}+6\mathsf{s}$

on a Huff curve over $\mathbb{K} = \mathbb{F}_q$ of embedding degree k. M and S denote multiplications and squarings in the larger field $\mathbb{F}_{q^k}$ while m and s are operations in $\mathbb{F}_q$ as before.

Outline. The rest of this paper is organized as follows. The next section introduces Huff's model. We develop efficient unified addition formulæ and discuss the applicability of the model. We explicit the class of elliptic curves covered by Huff's model. In Section 3, we present several generalizations and extensions. We offer dedicated addition formulæ. We generalize Huff's model to cover a larger class of elliptic curves. We also extend the model to the case of binary fields. Section 4 deals with pairings over Huff curves. We exploit the relative simplicity of the underlying group law to devise efficient formulæ for the evaluation of the Tate pairing. Finally, we conclude in Section 5.

2 Huff's Model

Let $\mathbb{K}$ denote a field of characteristic $\neq 2$. Consider the set of projective points $(X : Y : Z) \in \mathbb{P}^2(\mathbb{K})$ satisfying the equation

$$E_{/\mathbb{K}} : aX(Y^2 - Z^2) = bY(X^2 - Z^2) \tag{2}$$

where $a, b \in \mathbb{K}^\times$ and $a^2 \neq b^2$. This form is referred to as *Huff's model* of an elliptic curve.

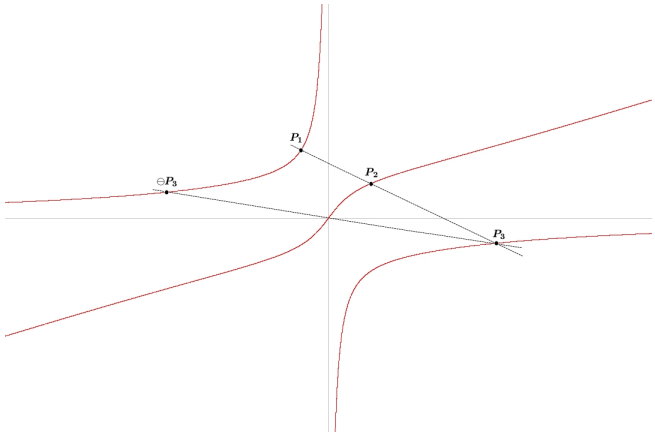

Fig. 1. Example of a Huff curve (over $\mathbb{R}$)

The tangent line at $(0 : 0 : 1)$ is $aX = bY$, which intersects the curve with multiplicity 3, so that $\boldsymbol{O} = (0 : 0 : 1)$ is an inflection point of E. $(E, \boldsymbol{O})$ is therefore an elliptic curve with $\boldsymbol{O}$ as neutral element and whose group law, denoted $\oplus$, has the following property: for any line intersecting the cubic curve E at the three points $\boldsymbol{P_1}$, $\boldsymbol{P_2}$ and $\boldsymbol{P_3}$ (counting multiplicities), we have $\boldsymbol{P_1} \oplus \boldsymbol{P_2} \oplus \boldsymbol{P_3} = \boldsymbol{O}$. In particular, the inverse of point $\boldsymbol{P_1} = (X_1 : Y_1 : Z_1)$ is $\ominus \boldsymbol{P_1} = (X_1 : Y_1 : -Z_1)$ and the sum of $\boldsymbol{P_1}$ and $\boldsymbol{P_2}$ is $\boldsymbol{P_1} \oplus \boldsymbol{P_2} = \ominus \boldsymbol{P_3}$. We note that a point at infinity is its own inverse. Hence, the three points at infinity (*i.e.*, on the line $Z = 0$ in $\mathbb{P}^2$) — namely, $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(a : b : 0)$, are exactly the three primitive 2-torsion points of E. The sum of any two of them is equal to the third one. More generally, $(X_1 : Y_1 : Z_1) \oplus (1 : 0 : 0)$ is the inverse of the point of intersection of the "horizontal" line passing through $(X_1 : Y_1 : Z_1)$ with E. When $Z_1 \neq 0$, we have

$$(X_1 : Y_1 : Z_1) \oplus (1 : 0 : 0) = ({Z_1}^2 : -X_1 Y_1 : X_1 Z_1)\,,$$

and analogously,

$$(X_1 : Y_1 : Z_1) \oplus (0 : 1 : 0) = (-X_1 Y_1 : {Z_1}^2 : Y_1 Z_1)\ .$$

From $(a:b:0) = (1:0:0) \oplus (0:1:0)$, when $Z_1 \neq 0$, we get $(X_1 : Y_1 : Z_1) + (a : b : 0) = ({Z_1}^2 : -X_1Y_1 : X_1Z_1) \oplus (0:1:0)$ and therefore

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

We remark that adding $(a : b : 0)$ to any of the points $(\pm 1 : \pm 1 : 1)$ transforms it into its inverse. It follows that these four points are the four solutions to the equation $[2]\boldsymbol{P} = (a : b : 0)$ and so are primitive 4-torsion points. The eight remarkable points we identified form a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. When $\mathbb{K} = \mathbb{Q}$, this must be the full torsion since, according to a theorem by Mazur, the torsion subgroup is of order at most 12 (and thus exactly 8 here).

Remark 1. In [15, p. 445], it is noted that the inverse projective transformations

$$\begin{aligned} &\Upsilon : \mathbb{P}^2(\mathbb{K}) \to \mathbb{P}^2(\mathbb{K}) : \\ &\quad (X : Y : Z) \mapsto (U : V : W) = \big(ab(bX - aY) : ab(b^2 - a^2)Z : -aX + bY\big) \end{aligned}$$

and

$$\begin{aligned} &\Upsilon^{-1} : \mathbb{P}^2(\mathbb{K}) \to \mathbb{P}^2(\mathbb{K}) : \\ &\qquad (U : V : W) \mapsto (X : Y : Z) = \big(b(U + a^2W) : a(U + b^2W) : V\big) \end{aligned}$$

induce a correspondence between Eq. (2) and the Weierstraß equation

$$V^2W = U(U + a^2W)(U + b^2W) \ .$$

Observe that point at infinity $(0 : 1 : 0)$ on the Weierstraß curve is mapped to $(0 : 0 : 1)$ on the Huff curve through Υ^{-1}. Observe also that map Υ^{-1} is a line-preserving transformation. This is another way to see that the group law on a Huff curve E follows the chord-and-tangent rule [25, § 2] with $\boldsymbol{O} = (0 : 0 : 1)$ as neutral element.

2.1 Affine formulæ

We give explicit formulæ for the group law. Excluding the 2-torsion, we use the non-homogeneous form $ax(y^2 - 1) = by(x^2 - 1)$. Let $y = \lambda x + \mu$ denote the secant line passing through two different points $\boldsymbol{P_1} = (x_1, y_1)$ and $\boldsymbol{P_2} = (x_2, y_2)$. This line intersects the curve at a third point $\ominus \boldsymbol{P_3} = (-x_3, -y_3)$. Plugging the line equation into the curve equation, we get

$$ax\big((\lambda x + \mu)^2 - 1\big) = b(\lambda x + \mu)(x^2 - 1) \implies \lambda(a\lambda - b)x^3 + \mu(2a\lambda - b)x^2 + \cdots = 0 \ .$$

Whenever defined, we so obtain

$$\begin{cases} x_3 = x_1 + x_2 + \dfrac{\mu(2a\lambda - b)}{\lambda(a\lambda - b)} \\ y_3 = \lambda x_3 - \mu \end{cases}$$

with $\lambda = \dfrac{y_1 - y_2}{x_1 - x_2}$ and $\mu = y_1 - \lambda x_1$. After simplification, we have

$$\begin{aligned} x_3 &= x_1 + x_2 + \frac{(x_1y_2 - x_2y_1)\big(2a(y_1 - y_2) - b(x_1 - x_2)\big)}{(y_1 - y_2)\big(a(y_1 - y_2) - b(x_1 - x_2)\big)} \\ &= \frac{(x_1 - x_2)\big(a({y_1}^2 - {y_2}^2) - b(x_1y_1 - x_2y_2)\big)}{(y_1 - y_2)\big(a(y_1 - y_2) - b(x_1 - x_2)\big)} \end{aligned}$$

and

$$y_3 = -\frac{(y_1 - y_2)\big(b({x_1}^2 - {x_2}^2) - a(x_1y_1 - x_2y_2)\big)}{(x_1 - x_2)\big(a(y_1 - y_2) - b(x_1 - x_2)\big)} \ .$$

The above formulæ can be further simplified by reusing the curve equation. A simple calculation shows that

$$\big(a(y_1 - y_2) - b(x_1 - x_2)\big)(x_1 + x_2)y_1y_2 = a(x_2y_1 - x_1y_2)(y_1y_2 - 1) \ .$$

Hence, we can write

$$\begin{aligned} x_3 &= x_1 + x_2 - \frac{\big(2a(y_1 - y_2) - b(x_1 - x_2)\big)(x_1 + x_2)y_1y_2}{(y_1 - y_2)a(y_1y_2 - 1)} \\ &= x_1 + x_2 - \frac{x_2y_1 - x_1y_2}{y_1 - y_2} - \frac{(x_1 + x_2)y_1y_2}{y_1y_2 - 1} \\ &= \frac{x_1y_1 - x_2y_2}{y_1 - y_2} - \frac{(x_1 + x_2)y_1y_2}{y_1y_2 - 1} \ . \end{aligned}$$

Furthermore, as easily shown

$$b(x_1y_1 - x_2y_2)(x_1x_2 + 1) = (y_1 - y_2)\big(ax_1x_2(y_1 + y_2) + b(x_1 + x_2)\big) \, ,$$

it thus follows that

$$\begin{aligned} x_3 &= \frac{ax_1x_2(y_1 + y_2) + b(x_1 + x_2)}{b(x_1x_2 + 1)} - \frac{(x_1 + x_2)y_1y_2}{y_1y_2 - 1} \\ &= \frac{(x_1 + x_2)(1 + y_1y_2)}{(1 + x_1x_2)(1 - y_1y_2)} \ , \end{aligned} \tag{3}$$

since $ax_1x_2(y_1 + y_2)(1 - y_1y_2) = by_1y_2(x_1 + x_2)(1 - x_1x_2)$.

Likewise, by symmetry, we have

$$y_3 = \frac{(y_1 + y_2)(1 + x_1x_2)}{(1 - x_1x_2)(1 + y_1y_2)} \ . \tag{4}$$

Equations (3) and (4) are defined whenever $x_1x_2 \neq \pm 1$ and $y_1y_2 \neq \pm 1$. Advantageously, curve parameters are not involved. Moreover, this addition law is *unified*: it can be used to double a point (*i.e.*, when $\boldsymbol{P_2} = \boldsymbol{P_1}$).

2.2 Projective formulæ

Previous affine formulæ involve inversions in $\mathbb{K}$. To avoid these operations and get faster arithmetic, projective coordinates may be preferred.

We let m and s represent the cost of a multiplication and of a squaring in $\mathbb{K}$, respectively. The projective form of Eqs (3) and (4) is

$$\begin{cases} X_3 = (X_1Z_2 + X_2Z_1)(Y_1Y_2 + Z_1Z_2)^2(Z_1Z_2 - X_1X_2) \\ Y_3 = (Y_1Z_2 + Y_2Z_1)(X_1X_2 + Z_1Z_2)^2(Z_1Z_2 - Y_1Y_2) \\ Z_3 = ({Z_1}^2{Z_2}^2 - {X_1}^2{X_2}^2)({Z_1}^2{Z_2}^2 - {Y_1}^2{Y_2}^2) \end{cases} . \tag{5}$$

In more detail, this can be evaluated as

$$\begin{gathered} m_1 = X_1X_2,\ \ m_2 = Y_1Y_2,\ \ m_3 = Z_1Z_2, \\ m_4 = (X_1 + Z_1)(X_2 + Z_2) - m_1 - m_3,\ \ m_5 = (Y_1 + Z_1)(Y_2 + Z_2) - m_2 - m_3, \\ m_6 = (m_2 + m_3)(m_3 - m_1),\ \ m_7 = (m_1 + m_3)(m_3 - m_2), \\ m_8 = m_4(m_2 + m_3),\ \ m_9 = m_5(m_1 + m_3), \\ X_3 = m_8m_6,\ \ Y_3 = m_9m_7,\ \ Z_3 = m_6m_7, \end{gathered}$$

that is, with $\underline{12\mathsf{m}}$.

2.3 Applicability

If $(x_1, y_1) \neq (0, 0)$ then $(x_1, y_1) \oplus (a : b : 0) = -(\frac{1}{x_1}, \frac{1}{y_1})$. Observe that Equation (5) remains valid for doubling point $(a : b : 0)$ or for adding point $(a : b : 0)$ to another finite point (*i.e.*, which is not at infinity) different from $\boldsymbol{O}$; we get $(X_1 : Y_1 : Z_1) \oplus (a : b : 0) = (-Y_1Z_1 : -X_1Z_1 : X_1Y_1)$ as expected. The addition formula is however not valid for adding $(0 : 1 : 0)$ or $(1 : 0 : 0)$. More generally, we have:

Theorem 1. *Let $\mathbb{K}$ be a field of characteristic $\neq 2$. Let $\boldsymbol{P_1} = (X_1 : Y_1 : Z_1)$ and $\boldsymbol{P_2} = (X_2 : Y_2 : Z_2)$ be two points on a Huff curve over $\mathbb{K}$. Then the addition formula given by Eq.* (5) *is valid provided that $X_1X_2 \neq \pm Z_1Z_2$ and $Y_1Y_2 \neq \pm Z_1Z_2$.*

Proof. If $\boldsymbol{P_1}$ and $\boldsymbol{P_2}$ are finite, we can write $\boldsymbol{P_1} = (x_1, y_1)$ and $\boldsymbol{P_2} = (x_2, y_2)$. The above affine formula for (x_3, y_3) as given by Eqs (3) and (4) is defined whenever $x_1x_2 \neq \pm 1$ and $y_1y_2 \neq \pm 1$. This translates into $X_1X_2 \neq \pm Z_1Z_2$ and $Y_1Y_2 \neq \pm Z_1Z_2$ for their projective coordinates.

It remains to analyze points at infinity. The points with their Z-coordinate equal to 0 are $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(a : b : 0)$. If $\boldsymbol{P_1}$ or $\boldsymbol{P_2} \in \{(1 : 0 : 0), (0 : 1 : 0)\}$, the condition $X_1X_2 \neq \pm Z_1Z_2$ and $Y_1Y_2 \neq \pm Z_1Z_2$ is not satisfied. Suppose now $\boldsymbol{P_2} = (a : b : 0)$. The condition becomes $X_1 \neq 0$ and $Y_1 \neq 0$, which corresponds to $\boldsymbol{P_1} \notin \{\boldsymbol{O}, (1 : 0 : 0), (0 : 1 : 0)\}$. As aforementioned, the addition law is then valid for adding $\boldsymbol{P_1}$ to $(a : b : 0)$. □

The previous theorem says that the addition on a Huff curve is almost complete. However, the exceptional inputs are easily prevented in practice. Cryptographic applications typically involve (large) prime-order subgroups. More specifically, we state:

Corollary 1. *Let E be a Huff curve over a field $\mathbb{K}$ of odd characteristic. Let also $\boldsymbol{P} \in E(\mathbb{K})$ be a point of odd order. Then the addition law in the subgroup generated by $\boldsymbol{P}$ is complete.*

Proof. All points in $\langle \boldsymbol{P} \rangle$ are of odd order and thus are finite (remember that points at infinity are of order 2). It remains to show that for any points $\boldsymbol{P_1} = (x_1, y_1), \boldsymbol{P_2} = (x_2, y_2) \in \langle \boldsymbol{P} \rangle$, we have $x_1 x_2 \neq \pm 1$ and $y_1 y_2 \neq \pm 1$. Note that $x_1, y_1, x_2, y_2 \neq \pm 1$ since this corresponds to points of order 4 (and thus not in $\langle \boldsymbol{P} \rangle$). Suppose that $x_1 x_2 = \pm 1$. Then $ax_1({y_1}^2 - 1) = by_1({x_1}^2 - 1) \implies a\frac{1}{x_1}({y_1}^2 - 1) = by_1(1 - \frac{1}{{x_1}^2}) \implies \pm ax_2({y_1}^2 - 1) = -by_1({x_2}^2 - 1)$. Hence, since $ax_2({y_2}^2 - 1) = by_2({x_2}^2 - 1)$, it follows that $\mp y_2({y_1}^2 - 1) = y_1({y_2}^2 - 1) \implies (y_1 \pm y_2)(1 \mp y_1 y_2) = 0 \implies y_2 = \mp y_1$ or $y_1 y_2 = \pm 1$. As a result, when $x_1 x_2 = \pm 1$, we have $(x_2, y_2) \in \left\{(\frac{1}{x_1}, -y_1), (\frac{1}{x_1}, \frac{1}{y_1}), (-\frac{1}{x_1}, y_1), (-\frac{1}{x_1}, -\frac{1}{y_1})\right\}$. In all cases, one of $(x_1, y_1) \oplus (x_2, y_2)$ or $(x_1, y_1) \ominus (x_2, y_2)$ is a 2-torsion point, a contradiction. Likewise, it can be verified that the case $y_1 y_2 = \pm 1$ leads to a contradiction, which concludes the proof. □

The *completeness* of the addition law is very useful as it yields a natural protection against certain side-channel attacks (*e.g.*, see [10]). Another useful feature is that the addition law is *independent* of the curve parameters.

2.4 Universality of the model

The next theorem states that every elliptic curve over a field of characteristic $\neq 2$ containing a copy of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ can be put in Huff's form. Generalizations and extensions are discussed in Section 3.

Theorem 2. *Any elliptic curve $(E, \boldsymbol{O})$ over a perfect field $\mathbb{K}$ of characteristic $\neq 2$ such that $E(\mathbb{K})$ contains a subgroup $\mathbb{G}$ isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is birationally equivalent over $\mathbb{K}$ to a Huff curve.*

Proof. The Riemann-Roch theorem implies that if $\boldsymbol{D} = a_1 \boldsymbol{P_1} + \cdots + a_r \boldsymbol{P_r}$ is a divisor of degree 0 on E then the dimension of the vector space

$$\mathscr{L}(\boldsymbol{D}) = \{f \in \mathbb{K}(E)^\times \mid \operatorname{div}(f) \geqslant -\boldsymbol{D}\} \cup \{0\}$$

is equal to 1 when $a_1 \boldsymbol{P_1} \oplus \cdots \oplus a_r \boldsymbol{P_r} = \boldsymbol{O}$, and to 0 otherwise.

Let $\boldsymbol{H}_{++}, \boldsymbol{H}_{+-}, \boldsymbol{H}_{-+}$ and $\boldsymbol{H}_{--}$ denote the four points of $\mathbb{G}$ of order exactly 4 (with the convention $\boldsymbol{H}_{++} \oplus \boldsymbol{H}_{--} = \boldsymbol{O}$). Doubling these points produces a unique primitive 2-torsion point that we denote $\boldsymbol{R}$. We further let $\boldsymbol{P}$ and $\boldsymbol{Q}$ denote the other two 2-torsion points; say, $\boldsymbol{P} = \ominus \boldsymbol{H}_{++} \oplus \boldsymbol{H}_{+-}$ and $\boldsymbol{Q} = \boldsymbol{H}_{++} \oplus \boldsymbol{H}_{+-}$. We have $\boldsymbol{P} \oplus \boldsymbol{R} \ominus \boldsymbol{Q} \ominus \boldsymbol{O} = \boldsymbol{O}$; so there exists a nonzero

rational function x with divisor exactly $\boldsymbol{Q}+\boldsymbol{O}-\boldsymbol{P}-\boldsymbol{R}$. In particular, x is well-defined and nonzero at $\boldsymbol{H}_{++}$ and thus without loss of generality we may assume that $x(\boldsymbol{H}_{++})=1$. Similarly, there exists a rational function y with divisor $\boldsymbol{P}+\boldsymbol{O}-\boldsymbol{Q}-\boldsymbol{R}$ such that $y(\boldsymbol{H}_{++})=1$.

The rational function $x-1$ has the same poles as x and vanishes at $\boldsymbol{H}_{++}$. Its divisor $\operatorname{div}(x-1)$ is thus given by $\boldsymbol{H}_{++}+\boldsymbol{X}-\boldsymbol{P}-\boldsymbol{R}$ for some point $\boldsymbol{X}$. Since this divisor is principal, we have $\boldsymbol{H}_{++}\oplus\boldsymbol{X}\ominus\boldsymbol{P}\ominus\boldsymbol{R}=\boldsymbol{O}$. Hence, it follows that $\boldsymbol{X}=\boldsymbol{P}\oplus\boldsymbol{R}\ominus\boldsymbol{H}_{++}=\ominus\boldsymbol{H}_{++}\oplus\boldsymbol{H}_{+-}\oplus\boldsymbol{R}\ominus\boldsymbol{H}_{++}=\boldsymbol{H}_{+-}$. Consequently, we have $x(\boldsymbol{H}_{+-})=1$. Likewise, it is verified that $y(\boldsymbol{H}_{-+})=1$.

Now, consider the map ι taking a rational function f to $\iota f:\boldsymbol{M}\mapsto f(\ominus\boldsymbol{M})$. This is an endomorphism of the vector space $\mathscr{L}(\boldsymbol{P}+\boldsymbol{R}-\boldsymbol{Q}-\boldsymbol{O})$. Indeed, the poles of ιf are $\ominus\boldsymbol{P}=\boldsymbol{P}$ and $\ominus\boldsymbol{R}=\boldsymbol{R}$ and its zeros are $\ominus\boldsymbol{Q}=\boldsymbol{Q}$ and $\ominus\boldsymbol{O}=\boldsymbol{O}$. Moreover, since $\iota^2=\mathrm{id}$ and since $\mathscr{L}(\boldsymbol{P}+\boldsymbol{R}-\boldsymbol{Q}-\boldsymbol{O})$ is a one-dimensional vector space, ι is the multiplication map by 1 or -1. The equality $\iota x=x$ would imply $x(\boldsymbol{H}_{--})=x(\boldsymbol{H}_{++})=1$, which contradicts the previous calculation of $\operatorname{div}(x-1)$. As a result, we must have $\iota x=-x$. In particular, noting that $\boldsymbol{H}_{-+}=\ominus\boldsymbol{H}_{+-}$, we obtain

$$x(\boldsymbol{H}_{-+})=\iota x(\boldsymbol{H}_{+-})=-x(\boldsymbol{H}_{+-})=-1\,,$$

and similarly for $\boldsymbol{H}_{--}$. Since $x+1$ has the same poles as x, its divisor is then given by $\operatorname{div}(x+1)=\boldsymbol{H}_{-+}+\boldsymbol{H}_{--}-\boldsymbol{P}-\boldsymbol{R}$. Analogously, we obtain $\operatorname{div}(y+1)=\boldsymbol{H}_{+-}+\boldsymbol{H}_{--}-\boldsymbol{Q}-\boldsymbol{R}$.

Finally, consider the rational functions $u=x(y^2-1)$ and $v=y(x^2-1)$. We have:

$$\begin{aligned}\operatorname{div}(u)&=\operatorname{div}(x)+\operatorname{div}(y-1)+\operatorname{div}(y+1)\\&=(\boldsymbol{Q}+\boldsymbol{O}-\boldsymbol{P}-\boldsymbol{R})+(\boldsymbol{H}_{++}+\boldsymbol{H}_{-+}-\boldsymbol{Q}-\boldsymbol{R})+\\&\qquad\qquad(\boldsymbol{H}_{+-}+\boldsymbol{H}_{--}-\boldsymbol{Q}-\boldsymbol{R})\\&=\boldsymbol{H}_{++}+\boldsymbol{H}_{+-}+\boldsymbol{H}_{-+}+\boldsymbol{H}_{--}+\boldsymbol{O}-\boldsymbol{P}-\boldsymbol{Q}-3\boldsymbol{R}\end{aligned}$$

and

$$\begin{aligned}\operatorname{div}(v)&=\operatorname{div}(y)+\operatorname{div}(x-1)+\operatorname{div}(x+1)\\&=(\boldsymbol{P}+\boldsymbol{O}-\boldsymbol{Q}-\boldsymbol{R})+(\boldsymbol{H}_{++}+\boldsymbol{H}_{+-}-\boldsymbol{P}-\boldsymbol{R})+\\&\qquad\qquad(\boldsymbol{H}_{-+}+\boldsymbol{H}_{--}-\boldsymbol{P}-\boldsymbol{R})\\&=\boldsymbol{H}_{++}+\boldsymbol{H}_{+-}+\boldsymbol{H}_{-+}+\boldsymbol{H}_{--}+\boldsymbol{O}-\boldsymbol{P}-\boldsymbol{Q}-3\boldsymbol{R}\ .\end{aligned}$$

But the vector space $\mathscr{L}(\boldsymbol{P}+\boldsymbol{Q}+3\boldsymbol{R}-\boldsymbol{O}-\boldsymbol{H}_{++}-\boldsymbol{H}_{+-}-\boldsymbol{H}_{-+}-\boldsymbol{H}_{--})$ is of dimension 1, so there exists a linear relation between u and v. In other words, there exist $a,b\in\mathbb{K}^\times$ such that $au=bv$; *i.e.*, such that $ax(y^2-1)=by(x^2-1)$.

The rational map $E\to\mathbb{P}^2(\mathbb{K})$ given by $\boldsymbol{M}\mapsto(x(\boldsymbol{M}):y(\boldsymbol{M}):1)$ extends to a morphism defined on all of E, and its image is contained in $E_{a,b}$ in view of the previous relation (and $E_{a,b}$ itself is a smooth irreducible curve as seen in §1.1). We therefore have a non-constant — and hence surjective — morphism of curves $E\to E_{a,b}$. Moreover, its degree is at most 1: indeed, if a point $(x_0:y_0:1)\in E_{a,b}(\overline{\mathbb{K}})$ has two distinct pre-images $\boldsymbol{M}\neq\boldsymbol{M'}\in E(\overline{\mathbb{K}})$, the functions $x-x_0$

and $y - y_0$ vanish at $\boldsymbol{M}$ and $\boldsymbol{M'}$. Since they have the same poles as x and y, their divisors are respectively $\boldsymbol{M} + \boldsymbol{M'} - \boldsymbol{P} - \boldsymbol{R}$ and $\boldsymbol{M} + \boldsymbol{M'} - \boldsymbol{Q} - \boldsymbol{R}$, which yields $\boldsymbol{P} \oplus \boldsymbol{R} = \boldsymbol{M} \oplus \boldsymbol{M'} = \boldsymbol{Q} \oplus \boldsymbol{R}$, a contradiction. As a surjective morphism of degree 1, the map $E \to E_{a,b}$ is thus an isomorphism. □

3 Generalizations and Extensions

This section presents dedicated addition formulæ. It also presents a generalization of the model as originally introduced by Huff so that it covers more curves and extends to binary fields.

3.1 Faster computations

Dedicated doubling. The doubling formula can be sped up by evaluating squarings in $\mathbb{K}$ with a specialized implementation. The cost of a point doubling then becomes $\underline{7\mathsf{m} + 5\mathsf{s}}$. When $\mathsf{s} > \frac{3}{4}\mathsf{m}$, an even faster way for doubling a point is given by

$$\begin{gathered}
m_1 = X_1 Y_1,\ \ m_2 = X_1 Z_1,\ \ m_3 = Y_1 Z_1,\ \ s_1 = {Z_1}^2, \\
m_4 = (m_2 - m_3)(m_2 + m_3),\ \ m_5 = (m_1 - s_1)(m_1 + s_1), \\
m_6 = (m_1 - s_1)(m_2 - m_3),\ \ m_7 = (m_1 + s_1)(m_2 + m_3), \\
X([2]\boldsymbol{P_1}) = (m_6 - m_7)(m_4 + m_5),\ \ Y([2]\boldsymbol{P_1}) = (m_6 + m_7)(m_4 - m_5), \\
Z([2]\boldsymbol{P_1}) = (m_4 + m_5)(m_4 - m_5),
\end{gathered}$$

that is, with $\underline{10\mathsf{m} + 1\mathsf{s}}$.

Moving the origin. Choosing $\boldsymbol{O'} = (0 : 1 : 0)$ as the neutral element results in translating the group law. If we let $\oplus'$ denote the corresponding point addition, we have $\boldsymbol{P_1} \oplus' \boldsymbol{P_2} = (\boldsymbol{P_1} \ominus \boldsymbol{O'}) \oplus (\boldsymbol{P_2} \ominus \boldsymbol{O'}) \oplus \boldsymbol{O'} = \boldsymbol{P_1} \oplus \boldsymbol{P_2} \oplus \boldsymbol{O'}$. Hence, we get

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

This can be evaluated with $\underline{11\mathsf{m}}$ as

$$\begin{gathered}
m_1 = X_1 X_2,\ \ m_2 = Y_1 Y_2,\ \ m_3 = Z_1 Z_2, \\
m_4 = (X_1 + Z_1)(X_2 + Z_2) - m_1 - m_3,\ \ m_5 = (Y_1 + Z_1)(Y_2 + Z_2) - m_2 - m_3, \\
X_3 = m_4(m_2 + m_3)m_5,\ \ Y_3 = (m_1 - m_3)(m_3 - m_2)(m_3 + m_2), \\
Z_3 = m_5(m_1 + m_3)(m_2 - m_3)\ .
\end{gathered} \tag{6}$$

This addition formula is unified: it can be used for doubling as well.

For a mixed point addition (*i.e.*, when $Z_2 = 1$), we have $m_3 = Z_1$ and the number of required multiplications drops to $\underline{10\mathsf{m}}$. When used for dedicated

doubling, the above addition formula requires $\underline{6\mathsf{m} + 5\mathsf{s}}$, which can equivalently be obtained as

$$\begin{gathered} s_1 = {X_1}^2,\ \ s_2 = {Y_1}^2,\ \ s_3 = {Z_1}^2, \\ s_4 = (X_1 + Y_1)^2 - s_1 - s_2,\ \ s_5 = (Y_1 + Z_1)^2 - s_2 - s_3, \\ X([2]\boldsymbol{P_1}) = 2s_3 s_4(s_2 + s_3),\ \ Y([2]\boldsymbol{P_1}) = (s_1 - s_3)(s_3 - s_2)(s_3 + s_2), \\ Z([2]\boldsymbol{P_1}) = s_5(s_1 + s_3)(s_2 - s_3)\ . \end{gathered} \tag{7}$$

Note that the expression for the inverse of point $\boldsymbol{P_1}$ is unchanged: $\ominus'\boldsymbol{P_1} = \ominus(\boldsymbol{P_1} \ominus \boldsymbol{O'}) \oplus \boldsymbol{O'} = \ominus\boldsymbol{P_1} = (X_1 : Y_1 : -Z_1)$.

3.2 More formulæ

Alternative addition formulæ can be derived using the curve equation. For example, whenever defined, we can write $(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2)$ with

$$x_3 = \frac{(x_1 - x_2)(y_1 + y_2)}{(y_1 - y_2)(1 - x_1 x_2)} \quad \text{and} \quad y_3 = \frac{(y_1 - y_2)(x_1 + x_2)}{(x_1 - x_2)(1 - y_1 y_2)}\ .$$

In projective coordinates, this gives

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

which can be evaluated with $13\mathsf{m}$ as

$$\begin{gathered} m_1 = X_1 Z_2,\ \ m_2 = X_2 Z_1,\ \ m_3 = Y_1 Z_2,\ \ m_4 = Y_2 Z_1, \\ m_5 = (Z_1 - X_1)(Z_2 + X_2) + m_1 - m_2,\ \ m_6 = (Z_1 - Y_1)(Z_2 + Y_2) + m_3 - m_4, \\ m_7 = (m_1 - m_2)m_6,\ \ m_8 = (m_3 - m_4)m_5, \\ X_3 = (m_1 - m_2)(m_3 + m_4)m_7,\ \ Y_3 = (m_1 + m_2)(m_3 - m_4)m_8,\ \ Z_3 = m_7 m_8\ . \end{gathered}$$

Although not as efficient as the usual addition, this alternative formula is useful in some pairing computations (see Section 4.2).

3.3 Twisted curves

As shown in Theorem 1, the group of points of a Huff elliptic curve contains a copy of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This implies that the curve order is a multiple of 8. Several cryptographic standards, however, require elliptic curves with group order of the form $h\,n$ where $h \in \{1, 2, 3, 4\}$ and n is a prime.

We can generalize Huff's model to accommodate the case $h = 4$. Let $\mathcal{P} \in \mathbb{K}[t]$ denote a monic polynomial of degree 2, with non-zero discriminant, and such that $\mathcal{P}(0) \neq 0$. We can then introduce the cubic curve

$$ax\mathcal{P}(y) = by\mathcal{P}(x)$$

where $a, b \in \mathbb{K}^\times$. The set of points $\{(0:0:1),(0:1:0),(1:0:0),(a:b:0)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ belongs to the curve. Moreover, when $\mathcal{P}$ factors in $\mathbb{K}$ — *i.e.*, when $\mathcal{P}(t) = (t-\omega_1)(t-\omega_2)$ with $\omega_1, \omega_2 \in \mathbb{K}^\times$, the four points $(\pm\omega_1 : \pm\omega_2 : 1)$ are also on the curve.

When $\operatorname{Char}\mathbb{K} \neq 2$, we consider $\mathcal{P}(t) = t^2 - d$ for some $d \in \mathbb{K}^\times$. So we deal with the set of projective points $(X:Y:Z) \in \mathbb{P}^2(\mathbb{K})$ satisfying the non-singular cubic equation

$$\hat{E}_d : aX(Y^2 - dZ^2) = bY(X^2 - dZ^2) \tag{8}$$

where $a, b, d \in \mathbb{K}^\times$ and $a^2 \neq b^2$. This equation corresponds to Weierstraß equation $V^2W = U(U + \frac{a^2}{d}W)(U + \frac{b^2}{d}W)$ under the inverse transformations $(X:Y:Z) = \big(b(dU + a^2W) : a(dU + b^2W) : dV\big)$ and $(U:V:W) = \big(ab(bX - aY) : ab(b^2 - a^2)Z : d(-aX + bY)\big)$. The transformation $(X:Y:Z) \leftarrow (X:Y:Z\sqrt{d})$ induces an isomorphism from $E = \hat{E}_1$ to $\hat{E}_d$ over $\mathbb{K}(\sqrt{d})$. Curves $\hat{E}_d$ are therefore *quadratic twists* of Huff curves.

In affine coordinates, we consider the curve equation $ax(y^2 - d) = by(x^2 - d)$. The sum of two finite points $\boldsymbol{P_1} = (x_1, y_1)$ and $\boldsymbol{P_2} = (x_2, y_2)$ such that $x_1x_2 \neq \pm d$ and $y_1y_2 \neq \pm d$ is given by (x_3, y_3) where

$$x_3 = \frac{d(x_1 + x_2)(d + y_1y_2)}{(d + x_1x_2)(d - y_1y_2)} \quad \text{and} \quad y_3 = \frac{d(y_1 + y_2)(d + x_1x_2)}{(d - x_1x_2)(d + y_1y_2)} \ . \tag{9}$$

Extending the computations of § 2.2, it is readily verified that the sum of two points can be evaluated with $\underline{12\mathsf{m}}$ (plus a couple of multiplications by constant d) using projective coordinates. The faster computations of the previous section also generalize to twisted curves.

3.4 Binary fields

Huff's form can be extended to a binary field as

$$ax(y^2 + y + 1) = by(x^2 + x + 1) \ .$$

This curve is birationally equivalent to Weierstraß curve

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

under the inverse maps

$$(x, y) = \left(\frac{b(u + a^2)}{v}, \frac{a(u + b^2)}{v + (a+b)u}\right) \quad \text{and} \quad (u, v) = \left(\frac{ab}{xy}, \frac{ab(axy + b)}{x^2y}\right) \ .$$

The neutral element is $\boldsymbol{O} = (0, 0)$.

4 Pairings

4.1 Preliminaries

Let $(E, \boldsymbol{O})$ be an elliptic curve over $\mathbb{K} = \mathbb{F}_q$, with q odd. Suppose that $\#E(\mathbb{F}_q) = hn$ where n is a prime such that $\gcd(n, q) = 1$. Let further k denote the embedding degree with respect to n, namely the smallest extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$ containing all n-th roots of unity. In other words, k is the smallest positive integer k such that $n \mid q^k - 1$. For better efficiency, we further assume that $k > 1$ is even.

For any point $\boldsymbol{P} \in E(\mathbb{F}_q)[n]$, we let $f_{\boldsymbol{P}}$ denote a rational function on E defined over $\mathbb{F}_q$ such that $\mathrm{div}(f_{\boldsymbol{P}}) = n\boldsymbol{P} - n\boldsymbol{O}$; it exists and is unique up to a multiplicative constant, according to the Riemann-Roch theorem. The group of n-th roots of unity in $\mathbb{F}_{q^k}$ is denoted by μ_n. The *(reduced) Tate pairing* is then defined as

$$T_n : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_{q^k})/[n]E(\mathbb{F}_{q^k}) \to \mu_n : (\boldsymbol{P}, \boldsymbol{Q}) \mapsto f_{\boldsymbol{P}}(\boldsymbol{Q})^{(q^k-1)/n} \ .$$

This definition does not depend on the choice of $f_{\boldsymbol{P}}$ with the appropriate divisor, nor on the class of $\boldsymbol{Q}$ mod $[n]E(\mathbb{F}_{q^k})$.

In practice, T_n can be computed using a technique due to Miller [21], in terms of rational functions $g_{\boldsymbol{R},\boldsymbol{P}}$ depending on $\boldsymbol{P}$ and on a variable point $\boldsymbol{R}$. Function $g_{\boldsymbol{R},\boldsymbol{P}}$ is the so-called *line function* with divisor $\boldsymbol{R} + \boldsymbol{P} - \boldsymbol{O} - (\boldsymbol{R} \oplus \boldsymbol{P})$, which arises in addition formulæ when E is represented as a plane cubic. The core idea is to derive function $f_{\boldsymbol{P}}$ iteratively. Letting $f_{i,\boldsymbol{P}}$ be the function with divisor $\mathrm{div}(f_{i,\boldsymbol{P}}) = i\boldsymbol{P} - ([i]\boldsymbol{P}) - (i-1)\boldsymbol{O}$, it is easily verified that

$$f_{i+j,\boldsymbol{P}} = f_{i,\boldsymbol{P}} \cdot f_{j,\boldsymbol{P}} \cdot g_{[i]\boldsymbol{P},[j]\boldsymbol{P}} \ .$$

Observe that $f_{1,\boldsymbol{P}} = 1$ and $f_{n,\boldsymbol{P}} = f_{\boldsymbol{P}}$. Hence, if $n = \overline{n_{\ell-1} n_{\ell-1} \cdots n_0}_2$ is the binary representation of n, the Tate pairing can be computed as follows.

Algorithm 1 Miller's algorithm

1: $f \leftarrow 1$; $\boldsymbol{R} \leftarrow \boldsymbol{P}$
2: **for** $i = \ell - 2$ down to 0 **do**
3: $\quad f \leftarrow f^2 \cdot g_{\boldsymbol{R},\boldsymbol{R}}(\boldsymbol{Q})$; $\boldsymbol{R} \leftarrow [2]\boldsymbol{R}$
4: $\quad$ **if** $(n_i = 1)$ **then**
5: $\quad\quad f \leftarrow f \cdot g_{\boldsymbol{R},\boldsymbol{P}}(\boldsymbol{Q})$; $\boldsymbol{R} \leftarrow \boldsymbol{R} \oplus \boldsymbol{P}$
6: $\quad$ **end if**
7: **end for**
8: **return** $f^{(q^k-1)/n}$

Contrary to Edwards curves or Jacobi quartics, Huff curves are represented as plane cubics. This makes Miller's algorithm, along with a number of improvements proposed for Weierstraß curves (*e.g.*, as presented in [3]), directly applicable to the computation of pairings over Huff curves.

4.2 Pairing formulæ for Huff curves

Throughout the for-loop of Algorithm 1, the line function is always evaluated at the same point $\boldsymbol{Q} \in E(\mathbb{F}_{q^k}) \setminus E(\mathbb{F}_q)$. It is therefore customary to represent this point in affine coordinates. In our case, it is most convenient to choose the coordinates of $\boldsymbol{Q}$ as $\boldsymbol{Q} = (y, z) = (1 : y : z)$. Indeed, since the embedding degree k is even, the field $\mathbb{F}_{q^k}$ can be represented as $\mathbb{F}_{q^{k/2}}(\alpha)$, where α is any quadratic non-residue in $\mathbb{F}_{q^{k/2}}$. As a result, $\boldsymbol{Q}$ can be chosen of the form $\boldsymbol{Q} = (y_{\boldsymbol{Q}}, z_{\boldsymbol{Q}}\alpha)$ with $y_{\boldsymbol{Q}}, z_{\boldsymbol{Q}} \in \mathbb{F}_{q^{k/2}}$ [4]. To do so, it suffices to pick a point on a quadratic twist of E over $\mathbb{F}_{q^{k/2}}$ and take its image under the isomorphism over $\mathbb{F}_{q^k}$.

Now, for any two points $\boldsymbol{R}$, $\boldsymbol{P}$ in $E(\mathbb{F}_q)$, let $\ell_{\boldsymbol{R},\boldsymbol{P}}$ denote the rational function vanishing on the line through $\boldsymbol{R}$ and $\boldsymbol{P}$. In general, we have

$$\ell_{\boldsymbol{R},\boldsymbol{P}}(\boldsymbol{Q}) = \frac{(zX_{\boldsymbol{P}} - Z_{\boldsymbol{P}}) - \lambda(yX_{\boldsymbol{P}} - Y_{\boldsymbol{P}})}{Y_{\boldsymbol{P}}}$$

where λ is the "(y, z)-slope" of the line through $\boldsymbol{R}$ and $\boldsymbol{P}$. Then, the divisor of $\ell_{\boldsymbol{R},\boldsymbol{P}}$ is

$$\mathrm{div}(\ell_{\boldsymbol{R},\boldsymbol{P}}) = \boldsymbol{R} + \boldsymbol{P} + \boldsymbol{T} - (1:0:0) - (0:1:0) - (a:b:0)$$

where $\boldsymbol{T}$ is the third point of intersection (counting multiplicities) of the line through $\boldsymbol{R}$ and $\boldsymbol{P}$ with the elliptic curve. In particular, if the neutral element of the group law $\oplus$ is denoted by $\boldsymbol{U}$, the line function $g_{\boldsymbol{R},\boldsymbol{P}}$ can be written as

$$g_{\boldsymbol{R},\boldsymbol{P}} = \frac{\ell_{\boldsymbol{R},\boldsymbol{P}}}{\ell_{\boldsymbol{R}\oplus\boldsymbol{P},\boldsymbol{U}}} \ .$$

We concentrate on the case when $\boldsymbol{U} = \boldsymbol{O} = (0 : 0 : 1)$. Then for any $\boldsymbol{Q} = (y_{\boldsymbol{Q}}, z_{\boldsymbol{Q}}\alpha)$, we have

$$\ell_{\boldsymbol{R}\oplus\boldsymbol{P},\boldsymbol{O}}(\boldsymbol{Q}) = y_{\boldsymbol{Q}} - \frac{Y_{\boldsymbol{R}\oplus\boldsymbol{P}}}{X_{\boldsymbol{R}\oplus\boldsymbol{P}}} \in \mathbb{F}_{q^{k/2}} \ .$$

Since this quantity lies in a proper subfield of $\mathbb{F}_{q^k}$, it goes to 1 after the final exponentiation in Miller's algorithm, which means that it can be discarded altogether. Similarly, divisions by $X_{\boldsymbol{P}}$ can be omitted, and denominators in the expression of λ can be canceled. In other words, if $\lambda = A/B$, we can compute the line function as

$$g_{\boldsymbol{R},\boldsymbol{P}}(\boldsymbol{Q}) = (zX_{\boldsymbol{P}} - Z_{\boldsymbol{P}}) \cdot B - (yX_{\boldsymbol{P}} - Y_{\boldsymbol{P}}) \cdot A$$

and get the required result.

We can now detail precise formulæ for the addition and doubling steps in the so-called Miller loop (*i.e.*, the main for-loop in Algorithm 1). We let M and S represent the cost of a multiplication and of a squaring in $\mathbb{F}_{q^k}$ while m and s are operations in $\mathbb{F}_q$ as before.

Addition step. In the case of addition, the (y, z)-slope of the line through $\boldsymbol{R} = (X_R : Y_R : Z_R)$ and $\boldsymbol{P} = (X_P : Y_P : Z_P)$ is

$$\lambda = \frac{Z_{\boldsymbol{R}} X_{\boldsymbol{P}} - Z_{\boldsymbol{P}} X_{\boldsymbol{R}}}{Y_{\boldsymbol{R}} X_{\boldsymbol{P}} - Y_{\boldsymbol{P}} X_{\boldsymbol{R}}} \ .$$

Therefore, the line function to be evaluated is of the form

$$g_{\boldsymbol{R},\boldsymbol{P}}(\boldsymbol{Q}) = (z_{\boldsymbol{Q}}\alpha \cdot X_{\boldsymbol{P}} - Z_{\boldsymbol{P}})(Y_{\boldsymbol{R}} X_{\boldsymbol{P}} - Y_{\boldsymbol{P}} X_{\boldsymbol{R}}) - (y_{\boldsymbol{Q}} \cdot X_{\boldsymbol{P}} - Y_{\boldsymbol{P}})(Z_{\boldsymbol{R}} X_{\boldsymbol{P}} - Z_{\boldsymbol{P}} X_{\boldsymbol{R}}) \ .$$

Since $\boldsymbol{P}$ and $\boldsymbol{Q}$ are constant throughout the loop, the values depending only on $\boldsymbol{P}$ and $\boldsymbol{Q}$ —in this case $y'_{\boldsymbol{Q}} = y_{\boldsymbol{Q}} \cdot X_{\boldsymbol{P}} - Y_{\boldsymbol{P}}$ and $z'_{\boldsymbol{Q}} = z_{\boldsymbol{Q}}\alpha \cdot X_{\boldsymbol{P}}$, can be precomputed.

Then, each Miller addition step requires computing $\boldsymbol{R} \oplus \boldsymbol{P}$ (one addition on the curve over $\mathbb{F}_q$), evaluating $g_{\boldsymbol{R},\boldsymbol{P}}(\boldsymbol{Q})$, and computing $f \cdot g_{\boldsymbol{R},\boldsymbol{P}}(\boldsymbol{Q})$ (one multiplication in the field $\mathbb{F}_{q^k}$).

We consider two types of Miller addition steps: full addition, for which no assumption is made on the representation of $\boldsymbol{P}$, and mixed addition, for which we further assume that $\boldsymbol{P}$ is given in affine coordinates (*i.e.*, $X_{\boldsymbol{P}} = 1$). Both steps start with computing $\boldsymbol{R} \oplus \boldsymbol{P}$, including all intermediate results.

Full addition. Computing $\boldsymbol{R} \oplus \boldsymbol{P}$ requires $13\mathsf{m}$ using the dedicated addition formula from §3.1, including all intermediate results $m_1, \ldots, m_8$. Compute further $m_9 = (X_{\boldsymbol{R}} + Y_{\boldsymbol{R}})(X_{\boldsymbol{P}} - Y_{\boldsymbol{P}})$. We then have

$$g_{\boldsymbol{R},\boldsymbol{P}}(\boldsymbol{Q}) = (z'_{\boldsymbol{Q}} - Z_{\boldsymbol{P}})(m_9 + m_5 - m_6) - y'_{\boldsymbol{Q}}(m_1 - m_2)$$

where the first term requires $(\frac{k}{2} + 1)\mathsf{m}$ and the second term $\frac{k}{2}\mathsf{m}$. With the final multiplication over $\mathbb{F}_{q^k}$, the total cost of full addition is thus of $\underline{1\mathsf{M} + (k + 15)\mathsf{m}}$.

Mixed addition. Now that $X_{\boldsymbol{P}} = 1$, computing $\boldsymbol{R} \oplus \boldsymbol{P}$ using the formula from §2.2, including all the intermediate results $m_1, \ldots, m_9$, only requires $11\mathsf{m}$, since the computation of m_1 is free. We then have

$$g_{\boldsymbol{R},\boldsymbol{P}}(\boldsymbol{Q}) = (z'_{\boldsymbol{Q}} - Z_{\boldsymbol{P}})(Y_{\boldsymbol{R}} - Y_{\boldsymbol{P}} X_{\boldsymbol{R}}) - y'_{\boldsymbol{Q}}(2Z_{\boldsymbol{R}} - m_4)$$

where both terms require the same number of multiplications as before, plus one for $Y_{\boldsymbol{P}} X_{\boldsymbol{R}}$. The total cost of mixed addition is thus of $\underline{1\mathsf{M} + (k + 13)\mathsf{m}}$.

Doubling step. In the case of doubling, the (y, z)-slope of the tangent line at $\boldsymbol{R} = (X_R : Y_R : Z_R)$ is

$$\lambda = \frac{a(Z_{\boldsymbol{R}})^2 - 2bY_{\boldsymbol{R}} Z_{\boldsymbol{R}} - a(X_{\boldsymbol{R}})^2}{b(Y_{\boldsymbol{R}})^2 - 2aY_{\boldsymbol{R}} Z_{\boldsymbol{R}} - b(X_{\boldsymbol{R}})^2} = \frac{A}{B} \ .$$

Thus, the line function is of the form

$$g_{\boldsymbol{R},\boldsymbol{R}}(\boldsymbol{Q}) = z_{\boldsymbol{Q}}\alpha \cdot X_{\boldsymbol{R}} B - Z_{\boldsymbol{R}} B - y_{\boldsymbol{Q}} \cdot X_{\boldsymbol{R}} A + Y_{\boldsymbol{R}} A \ .$$

Miller's doubling involves computing the point $[2]\boldsymbol{R}$, which we do using the formulæ from §2.2 in $7\mathsf{m} + 5\mathsf{s}$. Then the quantities A and B are obtained by computing the additional product $m_{10} = 2Y_{\boldsymbol{R}}Z_{\boldsymbol{R}} = (Y_{\boldsymbol{R}} + Z_{\boldsymbol{R}})^2 - m_2 - m_3$ using a single squaring. Computing $g_{\boldsymbol{R},\boldsymbol{R}}(\boldsymbol{Q})$ requires multiplying those two values by $X_{\boldsymbol{R}}$ and $Y_{\boldsymbol{R}}$ (resp. $X_{\boldsymbol{R}}$ and $Z_{\boldsymbol{R}}$), hence an additional $4\mathsf{m}$. And finally, multiplications by $y_{\boldsymbol{Q}}$ and $z_{\boldsymbol{Q}}\alpha$ both require $\frac{k}{2}\mathsf{m}$. Taking into account the multiplication and the squaring in $\mathbb{F}_{q^k}$ needed to complete the doubling step, the total cost of Miller doubling is thus of $\underline{1\mathsf{M} + 1\mathsf{S} + (k+11)\mathsf{m} + 6\mathsf{s}}$.

5 Conclusion

This paper introduced and studied Huff's model, a new representation of elliptic curves to be considered alongside previous models such as Montgomery, Doche-Icart-Kohel and Edwards. This new model provides efficient arithmetic, competitive with some of the fastest known implementations (although not quite as fast as "inverted Edwards" for now). Moreover, it has a number of additional desirable properties, including unified/complete addition laws and formulæ that do not depend on curve parameters (both properties are useful in cryptographic applications to thwart certain implementation attacks). It is also suitable to other computations on elliptic curves, such as the evaluation of pairings.

We believe that this model is worthy of consideration by the community, and hope our contribution might spark further research into efficient implementations of elliptic curve arithmetic.

Acknowledgments. We are grateful to an anonymous referee for useful comments. This work was partly supported by the French ANR-07-TCOM-013-04 PACE Project and by the European Commission through the IST Program under Contract ICT-2007-216646 ECRYPT II.

References

1. C. Arène, T. Lange, M. Naehrig, and C. Ritzenthaler. Faster computation of the Tate pairing. Cryptology ePrint Archive, Report 2009/155, 2009. http://eprint.iacr.org/.
2. A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, 1993.
3. P. S. L. M. Barreto, B. Lynn, and M. Scott. Efficient implementation of pairing-based cryptosystems. *J. Cryptology*, 17(4):321–334, 2004.
4. P. S. L. M. Barreto, B. Lynn, and M. Scott. On the selection of pairing-friendly groups. In M. Matsui and R. Zuccherato, editors, *Selected Areas in Cryptography*, volume 3006 of *Lect. Notes Comput. Sci.*, pages 17–25. Springer, 2004.
5. D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters. Twisted Edwards curves. In S. Vaudenay, editor, *Progress in Cryptology – AFRICACRYPT 2008*, volume 5023 of *Lect. Notes Comput. Sci.*, pages 389–405. Springer, 2008.
6. D. J. Bernstein and T. Lange. Explicit-formulas database. http://www.hyperelliptic.org/EFD/.

7. D. J. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. In K. Kurosawa, editor, *Advances in Cryptology – ASIACRYPT 2007*, volume 4833 of *Lect. Notes Comput. Sci.*, pages 29–50. Springer, 2007.
8. D. J. Bernstein and T. Lange. Inverted Edwards coordinates. In S. Boztas and H.-F. Lu, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 4851 of *Lect. Notes Comput. Sci.*, pages 20–27. Springer, 2007.
9. D. J. Bernstein, T. Lange, and R. R. Farashahi. Binary Edwards curves. In E. Oswald and P. Rohatgi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2008*, volume 5154 of *Lect. Notes Comput. Sci.*, pages 244–265. Springer, 2008.
10. I. F. Blake, G. Seroussi, and N. P. Smart. *Advances in Elliptic Curve Cryptography*, volume 317 of *London Mathematical Society Lecture Note Series*, chapter V. Cambridge University Press, 2005.
11. M. P. L. Das and P. Sarkar. Pairing computation on twisted Edwards form elliptic curves. In S. Galbraith and K. Paterson, editors, *Pairing-Based Cryptography – Pairing 2008*, volume 5209 of *Lect. Notes Comput. Sci.*, pages 192–210. Springer, 2008.
12. H. M. Edwards. A normal form for elliptic curves. *Bull. Am. Math. Soc., New Ser.*, 44(3):393–422, 2007.
13. S. Goldwasser and J. Kilian. Primality testing using elliptic curves. *J. ACM*, 46(4):450–472, 1999.
14. H. Hisil, K. K.-H. Wong, G. Carter, and E. Dawson. Twisted Edwards curves revisited. In J. Pieprzyk, editor, *Advances in Cryptology – ASIACRYPT 2008*, volume 5350 of *Lect. Notes Comput. Sci.*, pages 326–343. Springer, 2008.
15. G. B. Huff. Diophantine problems in geometry and elliptic ternary forms. *Duke Math. J.*, 15:443–453, 1948.
16. S. Ionica and A. Joux. Another approach to pairing computation in Edwards coordinates. In D. Chowdhury, V. Rijmen, and A. Das, editors, *Progress in Cryptology – INDOCRYPT 2008*, volume 5365 of *Lect. Notes Comput. Sci.*, pages 400–413. Springer, 2008.
17. A. H. Koblitz, N. Koblitz, and A. Menezes. Elliptic curve cryptography: The serpentine course of a paradigm shift. *J. Number Theory*, to appear.
18. N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48:203–209, 1987.
19. H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. Math.*, 126(2):649–673, 1987.
20. V. S. Miller. Use of elliptic curves in cryptography. In H. C. Williams, editor, *Advances in Cryptology – CRYPTO '85*, volume 218 of *Lect. Notes Comput. Sci.*, pages 417–426. Springer, 1986.
21. V. S. Miller. The Weil paring, and its efficient implementation. *J. Cryptology*, 17(1):235–261, 2004.
22. P. L. Montgomery. Speeding up the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177):243–264, 1987.
23. F. Morain. Primality proving using elliptic curves: An update. In J. Buhler, editor, *Algorithmic Number Theory (ANTS-III)*, volume 1423 of *Lect. Notes Comput. Sci.*, pages 111–127. Springer, 1998.
24. W. D. Peeples, Jr. Elliptic curves and rational distance sets. *Proc. Am. Math. Soc.*, 5:29–33, 1954.
25. J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*, chapter III. Springer-Verlag, 1986.