Published in A. Kiayias, Ed., *Topics in Cryptology – CT-RSA 2011*, vol. 6558 of *Lecture Notes in Computer Science*, pp. 340-355, Springer, 2011.

Binary Huff Curves

Julien Devigne and Marc Joye

Technicolor, Security & Content Protection Labs
1 avenue de Belle Fontaine, 35576 Cesson-Sévigné Cedex, France
{julien.devigne, marc.joye}@technicolor.com

Abstract. This paper describes the addition law for a new form for elliptic curves over fields of characteristic 2. Specifically, it presents explicit formulæ for adding two different points and for doubling points. The case of differential point addition (that is, point addition with a known difference) is also addressed. Finally, this paper presents unified point addition formulæ; i.e., point addition formulæ that can be used for doublings. Applications to cryptographic implementations are discussed.

Keywords: Elliptic curves, Huff curves, binary fields, cryptography.

1 Introduction

Elliptic curve cryptography, introduced in the mid-eighties [10, 15], is a technology of choice for the implementation of secure systems. Its main advantage is the absence of sub-exponential algorithms to solve the underlying hard problem, the elliptic curve discrete logarithm problem (ECDLP). Elliptic curve cryptosystems therefore feature smaller key sizes, which results in smaller memory and processor requirements. They are especially well suited to memory-constrained devices like smart cards.

Two types of finite fields are mainly used to implement elliptic curve cryptosystems: large prime fields and fields of characteristic 2. This paper focuses on the binary case. Further, to prevent the so-called MOV reduction [14], only non-supersingular elliptic curves are considered.

An elliptic curve over a field $\mathbb{K}$ is a smooth projective algebraic curve of genus 1 with a specified $\mathbb{K}$-rational point. More explicitly, when $\mathbb{K} = \mathbb{F}_{2^m}$, a (non-supersingular) elliptic curve can be written as the locus in the affine plane of the Weierstraß equation

$$E_{/\mathbb{F}_{2^m}} : y^2 + xy = x^3 + a_2x^2 + a_6 \qquad (a_6 \neq 0)$$

together with the extra point at infinity $\boldsymbol{O} = (0 : 1 : 0)$. It is well known that the points on an elliptic curve given by a Weierstraß equation over any field of definition form a group under the 'chord-and-tangent' addition [19, Chapter III]. The identity element is $\boldsymbol{O}$. The inverse of a point $\boldsymbol{P_0} = (x_0, y_0) \in E \setminus \{\boldsymbol{O}\}$ is given by $-\boldsymbol{P_0} = (x_0, y_0 + x_0)$. Hence, $(0, \sqrt{a_6})$ is a rational point of order 2. (Remember that square roots always exist and are unique in characteristic two.)

Now let $\boldsymbol{P_1} + \boldsymbol{P_2} = \boldsymbol{P_3}$ with $\boldsymbol{P_i} = (x_i, y_i) \in E \setminus \{\boldsymbol{O}\}$ and $\boldsymbol{P_1} \neq -\boldsymbol{P_2}$. Then

$$x_3 = \lambda^2 + \lambda + a_2 + x_1 + x_2 \quad \text{and} \quad y_3 = \lambda(x_1 + x_3) + x_3 + y_1$$

where

$$\begin{cases} \lambda = \dfrac{y_1 + y_2}{x_1 + x_2}, & \text{if } x_1 \neq x_2 \\ \lambda = x_1 + \dfrac{y_1}{x_1}, & \text{if } x_1 = x_2 \end{cases} .$$

There are other known models to represent elliptic curves (see e.g. [4, 5]). Having different models at one's disposal is useful as this gives rise to a different arithmetic, with different properties. An expected outcome is of course an improved efficiency. This can be observed at different levels: speed, memory and processor requirements, bandwidth, etc. Another possible benefit, which should not be overlooked, is the ease of implementation. Of particular interest are the unified and complete addition laws, which reduce the number of cases to handle. Furthermore, this can help to prevent certain attacks, including those based on side-channel analysis [11] or exceptional procedure attacks [8]. Yet another application is batch computing [1].

We study in this paper a special model of elliptic curves known as *Huff's model* and generalizations thereof. More precisely, we detail the arithmetic on an extension of Huff's model to binary fields, as recently introduced in [9]. Almost all formulæ required for implementing modern discrete-log based cryptographic protocols with state-of-the-art scalar multiplication algorithms are considered: addition, doubling, special cases of addition, unified point addition formulæ, all in affine and projective versions, differential point addition. We also present a generalized form of the curve that allows for more flexibility in choosing the coefficients — in particular, every ordinary elliptic curve over $\mathbb{F}_{2^m}$ $(m \geq 4)$ is birationally equivalent over $\mathbb{F}_{2^m}$ to a generalized binary Huff curve.

As a result, we obtain that (generalized) binary Huff curves can even perform better than binary Edwards curves in some cases, with the only problem that the unified formulæ do *not* really apply to all cases, and there are exceptional situations. Nevertheless, we show that one has *complete* (i.e., fully unified) addition formulæ in certain proper subgroups, which can be used for most cryptographic applications.

The rest of this paper is organized as follows. In the next section, we detail the group law on binary Huff curves. In Section 3, we provide unified addition formulæ for doubling and adding points. Section 4 presents differential point addition formulæ. In Section 5, we propose a generalized model for binary Huff curves. Finally, we conclude the paper in Section 6.

2 Binary Huff Curves

While studying a diophantine problem, Huff introduced a new model for elliptic curves [7] (see also [18]). Huff's model was recently revisited in [9]. The case of fields of odd characteristic is fully covered. For binary fields, an extended model is also proposed but no details are provided. In this section, we fill the gap. In particular, we specify the group law on binary Huff curves.

We start with the definition.

Definition 1 ([9]). *A* binary Huff curve *is the set of projective points* $(X : Y : Z) \in \mathbb{P}^2(\mathbb{F}_{2^m})$ *satisfying the equation*

$$E_{/\mathbb{F}_{2^m}} : \; aX(Y^2 + YZ + Z^2) = bY(X^2 + XZ + Z^2)\,, \tag{1}$$

where $a, b \in \mathbb{F}_{2^m}^*$ *and* $a \neq b$.

There are three points at infinity satisfying the curve equation, namely $(a : b : 0)$, $(1 : 0 : 0)$, and $(0 : 1 : 0)$. The affine model corresponding to the binary Huff curve given by Eq. (1) is

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

As stated in [9, § 3.4], this curve is birationally equivalent to the Weierstraß elliptic curve

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

under the inverse maps

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

The set of points on a binary Huff curve forms a group. The identity element is $\boldsymbol{o} = (0, 0)$. While the above maps are not line-preserving, the group law on a binary Huff curve satisfies the chord-and-tangent rule. Let $\ell_{\boldsymbol{P},\boldsymbol{Q}}$ be the line joining points $\boldsymbol{P}$ and $\boldsymbol{Q}$. This line intersects the curve in a third point (counting multiplicities) that we denote by $\boldsymbol{P} * \boldsymbol{Q}$. Let also $\ell_{\boldsymbol{R},\boldsymbol{o}}$ be the line through $\boldsymbol{R} := \boldsymbol{P} * \boldsymbol{Q}$ and $\boldsymbol{o}$. The addition of $\boldsymbol{P}$ and $\boldsymbol{Q}$ is defined as the third point of intersection of $\ell_{\boldsymbol{R},\boldsymbol{o}}$ with the curve, that is, $\boldsymbol{P} + \boldsymbol{Q} = \boldsymbol{R} * \boldsymbol{o}$. The correctness follows by observing that $\operatorname{div}(\ell_{\boldsymbol{R},\boldsymbol{o}}/\ell_{\boldsymbol{P},\boldsymbol{Q}}) = (\boldsymbol{R} * \boldsymbol{o}) + (\boldsymbol{R}) + (\boldsymbol{o}) - (\boldsymbol{R}) - (\boldsymbol{P}) - (\boldsymbol{Q}) \sim 0$, which implies $(\boldsymbol{P}) + (\boldsymbol{Q}) \sim (\boldsymbol{R} * \boldsymbol{o}) + (\boldsymbol{o})$.

Point inverse Identity element $\boldsymbol{o}$ is not an inflection point. The inverse of a point $\boldsymbol{P}$ is therefore not defined as $\boldsymbol{P} * \boldsymbol{o}$. From the previous description, we have that $-\boldsymbol{P} = \boldsymbol{P} * \boldsymbol{A}$, where $\boldsymbol{A} = \left(\frac{b}{a+b}, \frac{a}{a+b}\right)$ is the third point of intersection of the tangent line at $\boldsymbol{o}$ with the curve.

Another way to get the inverse is to use the birational equivalence with the Weierstraß form. Let $\boldsymbol{P} = (x_1, y_1) \in E$ be a finite point. Then, whenever defined, we so obtain $-\boldsymbol{P} = (\bar{x_1}, \bar{y_1})$ with

$$\bar{x_1} = \frac{y_1(b + ax_1y_1)}{a + bx_1y_1} \quad \text{and} \quad \bar{y_1} = \frac{x_1(a + bx_1y_1)}{b + ax_1y_1} \enspace . \tag{3}$$

If $a + bx_1y_1 = 0$ (i.e., $\boldsymbol{P} = \left(\frac{a+b}{b}, \frac{a}{a+b}\right)$) then $-\boldsymbol{P} = (1 : 0 : 0)$. If $b + ax_1y_1 = 0$ (i.e., $\boldsymbol{P} = \left(\frac{b}{a+b}, \frac{a+b}{a}\right)$) then $-\boldsymbol{P} = (0 : 1 : 0)$.

For the points at infinity, we obtain $-(a : b : 0) = (a : b : 0)$, $-(1 : 0 : 0) = \left(\frac{a+b}{b}, \frac{a}{a+b}\right)$, and $-(0 : 1 : 0) = \left(\frac{b}{a+b}, \frac{a+b}{a}\right)$. Observe that $(a : b : 0)$ is of order 2.

Point doubling Here too, the birational equivalence could be used to derive the doubling formula. The calculation, however, quickly becomes tricky. We instead directly rely on the geometric interpretation of the addition law.

Let $\boldsymbol{P} = (x_1, y_1) \in E$ be a finite point. The third point of intersection of the tangent line to the curve at $\boldsymbol{P}$ is $\boldsymbol{S} = \boldsymbol{P} * \boldsymbol{P}$. Then $[2]\boldsymbol{P} = \boldsymbol{S} * \boldsymbol{o}$. After some algebra, whenever defined, we get $[2]\boldsymbol{P} = (x_3, y_3)$ with

$$x_3 = \frac{(a+b){x_1}^2(1+y_1)^2}{b(1+x_1)^2(1+x_1y_1)^2} \quad \text{and} \quad y_3 = \frac{(a+b){y_1}^2(1+x_1)^2}{a(1+y_1)^2(1+x_1y_1)^2} \ . \tag{4}$$

If $x_1 = 1$ then $[2]\boldsymbol{P} = (1:0:0)$. If $y_1 = 1$ then $[2]\boldsymbol{P} = (0:1:0)$. If $x_1y_1 = 1$ (i.e., $\boldsymbol{P} = (\zeta, \zeta^{-1})$ with $\zeta^2 + \zeta + 1 = 0$) then $[2]\boldsymbol{P} = (a:b:0)$. (Note that $(1,1)$ is not a point on E.)

Remark 1. Since a solution to $\zeta^2 + \zeta + 1 = 0$ is a non-trivial cubic root of unity, (ζ, ζ^{-1}) is a rational point if and only the curve is defined over a binary extension field of even degree (i.e., over $\mathbb{F}_{2^m}$ with m even). Note also that (ζ, ζ^{-1}) is of order 4.

For the points at infinity, we have $[2](a:b:0) = \boldsymbol{o}$ (since $(a:b:0)$ is of order 2) and $[2](1:0:0) = [2](0:1:0) = \boldsymbol{A}$, where $\boldsymbol{A} = \left(\frac{b}{a+b}, \frac{a}{a+b}\right)$. Indeed, we have $[2](1:0:0) = -[2]\left(\frac{a+b}{b}, \frac{a}{a+b}\right) = -\left(\frac{b^3}{a^2(a+b)}, \frac{a^3}{b^2(a+b)}\right) = \left(\frac{b}{a+b}, \frac{a}{a+b}\right)$. This can also be seen from $\operatorname{div}(\ell_{\boldsymbol{o},\boldsymbol{o}}/y) = 2(\boldsymbol{o}) + (\boldsymbol{A}) - (\boldsymbol{o}) - 2(\boldsymbol{T_1}) = (\boldsymbol{o}) + (\boldsymbol{A}) - 2(\boldsymbol{T_1}) \sim 0$ and so $[2]\boldsymbol{T_1} = \boldsymbol{A}$, where $\ell_{\boldsymbol{o},\boldsymbol{o}}$ is the tangent line at $\boldsymbol{o}$, $\boldsymbol{A} = \boldsymbol{o} * \boldsymbol{o}$ and $\boldsymbol{T_1} = (1:0:0)$. Similarly, for $[2](0:1:0)$, the result follows from $\operatorname{div}(\ell_{\boldsymbol{o},\boldsymbol{o}}/x) = (\boldsymbol{o}) + (\boldsymbol{A}) - 2(\boldsymbol{T_2}) \sim 0$, where $\boldsymbol{T_2} = (0:1:0)$.

Dedicated point addition Let $\boldsymbol{P} = (x_1, y_1)$ and $\boldsymbol{Q} = (x_2, y_2) \in E$ be two finite points with $\boldsymbol{P} \neq \boldsymbol{Q}$. As afore explained, the addition of $\boldsymbol{P}$ and $\boldsymbol{Q}$ is given by $\boldsymbol{P} + \boldsymbol{Q} = (\boldsymbol{P} * \boldsymbol{Q}) * \boldsymbol{o}$. Then, whenever defined, we obtain $\boldsymbol{P} + \boldsymbol{Q} = (x_3, y_3)$ with

$$x_3 = \frac{(x_1y_1 + x_2y_2)(1 + y_1y_2)}{(y_1 + y_2)(1 + x_1x_2y_1y_2)} \quad \text{and} \quad y_3 = \frac{(x_1y_1 + x_2y_2)(1 + x_1x_2)}{(x_1 + x_2)(1 + x_1x_2y_1y_2)} \ . \tag{5}$$

If $x_1 = x_2$ then $\boldsymbol{P} + \boldsymbol{Q} = (0:1:0)$. If $y_1 = y_2$ then $\boldsymbol{P} + \boldsymbol{Q} = (1:0:0)$.

Remark 2. When $x_1 = x_2$, we can assume that $y_1 \neq 0$ (as otherwise we would have $x_1 = x_2 = 0$ and thus $\boldsymbol{P} = \boldsymbol{Q} = \boldsymbol{o}$). We then have $(x_1, y_1) + \left(x_1, \frac{1}{y_1}\right) = (0:1:0)$. Similarly, for $x_1 \neq 0$, we have $(x_1, y_1) + \left(\frac{1}{x_1}, y_1\right) = (1:0:0)$.

Suppose now $x_1 \neq x_2$ and $y_1 \neq y_2$. If $x_1x_2y_1y_2 = 1$ and $x_1x_2 = 1$ then $\boldsymbol{P} + \boldsymbol{Q} = [2]\boldsymbol{P} + (a:b:0)$. If $x_1x_2y_1y_2 = 1$ and $x_1x_2 \neq 1$ then $\boldsymbol{P} + \boldsymbol{Q} = (a:b:0)$.

When $\boldsymbol{P} = (x_1, y_1)$ is finite and $\boldsymbol{Q}$ is at infinity, whenever defined, we have

$$\begin{cases} (x_1, y_1) + (a:b:0) = \left(\dfrac{1}{x_1}, \dfrac{1}{y_1}\right) \\ (x_1, y_1) + (1:0:0) = \left(\dfrac{a + bx_1y_1}{y_1(b + ax_1y_1)}, \dfrac{x_1(a + bx_1y_1)}{b + ax_1y_1}\right) \\ (x_1, y_1) + (0:1:0) = \left(\dfrac{y_1(b + ax_1y_1)}{a + bx_1y_1}, \dfrac{b + ax_1y_1}{x_1(a + bx_1y_1)}\right) \end{cases} ,$$

and similarly when $\boldsymbol{P}$ is at infinity and $\boldsymbol{Q}$ is finite. If $x_1 = 0$ or $y_1 = 0$ (i.e., $\boldsymbol{P} = \boldsymbol{o}$) then $(x_1, y_1) + \boldsymbol{Q} = \boldsymbol{Q}$. If $a + bx_1y_1 = 0$ (i.e., $\boldsymbol{P} = \big(\frac{a+b}{b}, \frac{a}{a+b}\big)$) then $(x_1, y_1) + (0 : 1 : 0) = (a : b : 0)$. If $b + ax_1y_1 = 0$ (i.e., $\boldsymbol{P} = \big(\frac{b}{a+b}, \frac{a+b}{a}\big)$) then $(x_1, y_1) + (1 : 0 : 0) = (a : b : 0)$.

We also have $(a : b : 0) + (1 : 0 : 0) = (0 : 1 : 0)$, $(a : b : 0) + (0 : 1 : 0) = (1 : 0 : 0)$, and $(1 : 0 : 0) + (0 : 1 : 0) = (\frac{a+b}{b}, \frac{a+b}{a})$.

The correctness of the addition law for the exceptional cases (i.e., when the addition formula is not defined) is easily verified. We start with the points at infinity. As before, define $\boldsymbol{A} = \big(\frac{b}{a+b}, \frac{a}{a+b}\big)$, $\boldsymbol{T_1} = (1 : 0 : 0)$, and $\boldsymbol{T_2} = (0 : 1 : 0)$. Define also $\boldsymbol{T_0} = (a : b : 0)$. From $\operatorname{div}(x) = (\boldsymbol{o}) + (\boldsymbol{T_2}) - (\boldsymbol{T_0}) - (\boldsymbol{T_1}) \sim 0$, we get $\boldsymbol{T_2} = \boldsymbol{T_0} + \boldsymbol{T_1}$, that is, $(a : b : 0) + (1 : 0 : 0) = (0 : 1 : 0)$. Since $\boldsymbol{T_0}$ is of order 2, we also get $\boldsymbol{T_1} = \boldsymbol{T_2} - \boldsymbol{T_0} = \boldsymbol{T_0} + \boldsymbol{T_2}$, that is, $(a : b : 0) + (0 : 1 : 0) = (1 : 0 : 0)$. Letting $\ell_{\boldsymbol{o},\boldsymbol{o}}$ the tangent line at $\boldsymbol{o}$, since $\boldsymbol{A} = \boldsymbol{o} * \boldsymbol{o}$, we have $\operatorname{div}(\ell_{\boldsymbol{o},\boldsymbol{o}}) = 2(\boldsymbol{o}) + (\boldsymbol{A}) - (\boldsymbol{T_0}) - (\boldsymbol{T_1}) - (\boldsymbol{T_2}) \sim 0$, which yields $\boldsymbol{T_1} + \boldsymbol{T_2} = \boldsymbol{A} - \boldsymbol{T_0} = \boldsymbol{A} + \boldsymbol{T_0}$, that is, $(1 : 0 : 0) + (0 : 1 : 0) = \big(\frac{b}{a+b}, \frac{a}{a+b}\big) + (a : b : 0) = \big(\frac{a+b}{b}, \frac{a+b}{a}\big)$. The last equality holds because for a finite point $(x_1, y_1) \neq \boldsymbol{o}$, we have $(x_1 : y_1 : 1) + (a : b : 0) = (y_1 : x_1 : x_1y_1)$, that is, $(x_1, y_1) + (a : b : 0) = \big(\frac{1}{x_1}, \frac{1}{y_1}\big)$. Furthermore, for a finite point $(x_1, y_1) \neq \boldsymbol{o}, \big(\frac{a+b}{b}, \frac{a}{a+b}\big)$, the dedicated addition formula yields $\big(\frac{a+bx_1y_1}{y_1(b+ax_1y_1)}, \frac{x_1(a+bx_1y_1)}{b+ax_1y_1}\big) - (1 : 0 : 0) = \big(\frac{a+bx_1y_1}{y_1(b+ax_1y_1)}, \frac{x_1(a+bx_1y_1)}{b+ax_1y_1}\big) + \big(\frac{a+b}{b}, \frac{a}{a+b}\big) = (x_1, y_1)$, that is, $(x_1, y_1) + (1 : 0 : 0) = \big(\frac{a+bx_1y_1}{y_1(b+ax_1y_1)}, \frac{x_1(a+bx_1y_1)}{b+ax_1y_1}\big)$. The relation $(x_1, y_1) + (0 : 1 : 0)$, for a finite point $(x_1, y_1) \neq \boldsymbol{o}, \big(\frac{b}{a+b}, \frac{a+b}{a}\big)$, is obtained from $(x_1, y_1) + (a : b : 0) + (1 : 0 : 0) = \big(\frac{1}{x_1}, \frac{1}{y_1}\big) + (1 : 0 : 0) = \big(\frac{y_1(b+ax_1y_1)}{a+bx_1y_1}, \frac{b+ax_1y_1}{x_1(a+bx_1y_1)}\big)$. If $(x_1, y_1) = \big(\frac{a+b}{b}, \frac{a}{a+b}\big)$ then $(x_1, y_1) + (1 : 0 : 0) = (a : b : 0)$ since $(x_1, y_1) = -\boldsymbol{T_2} = \boldsymbol{T_0} - \boldsymbol{T_1}$. If $(x_1, y_1) = \big(\frac{b}{a+b}, \frac{a+b}{a}\big)$ then $(x_1, y_1) + (0 : 1 : 0) = (a : b : 0)$ since $(x_1, y_1) = -\boldsymbol{T_1} = \boldsymbol{T_0} - \boldsymbol{T_2}$.

The next cases consider finite points. Suppose that $x_1 = x_2$, that is, $\boldsymbol{P} = (x_1, y_1)$ and $\boldsymbol{Q} = (x_1, y_2)$. We can write $\operatorname{div}((x - x_1)/x) = (\boldsymbol{P}) + (\boldsymbol{Q}) + (\boldsymbol{T_2}) - (\boldsymbol{o}) - 2(\boldsymbol{T_2}) = (\boldsymbol{P}) + (\boldsymbol{Q}) - (\boldsymbol{T_2}) - (\boldsymbol{o}) \sim 0$. Therefore, we get $(x_1, y_1) + (x_1, y_2) = (0 : 1 : 0)$. The case $y_1 = y_2$ is similar by considering $\operatorname{div}((y - y_1)/y)$. Lastly, suppose that $\boldsymbol{P} = (x_1, y_1)$ and $\boldsymbol{Q} = (x_2, y_2)$ with $x_1 \neq x_2$ and $y_1 \neq y_2$. If $x_1x_2y_1y_2 = 1$ and $x_1x_2 = 1$ then $y_1y_2 = 1$; we thus have $\boldsymbol{P} = (x_1, y_1)$ and $\boldsymbol{Q} = \big(\frac{1}{x_1}, \frac{1}{y_1}\big)$. (Note that $x_1x_2 = 1$ implies $\boldsymbol{P} \neq \boldsymbol{o}$.) As already shown, we then have $\boldsymbol{Q} = \big(\frac{1}{x_1}, \frac{1}{y_1}\big) = (x_1, y_1) + (a : b : 0)$. We so obtain $\boldsymbol{P} + \boldsymbol{Q} = (x_1, y_1) + \big(\frac{1}{x_1}, \frac{1}{y_1}\big) = [2]\boldsymbol{P} + (a : b : 0)$. If $x_1x_2y_1y_2 = 1$ and $x_1x_2 \neq 1$ then $y_1y_2 \neq 1$ and also $x_1y_1 \neq x_2y_2$. Indeed, $x_1y_1 = x_2y_2$ and $x_1x_2y_1y_2 = 1$ would imply $x_1y_1 = x_2y_2 = 1$, that is, $\boldsymbol{P} = \big(x_1, \frac{1}{x_1}\big)$ and $\boldsymbol{Q} = \big(x_2, \frac{1}{x_2}\big)$. This in turn would imply $x_1 = \zeta$ and $x_2 = \zeta^{-1}$ (since $\boldsymbol{P} \neq \boldsymbol{Q}$) and so $x_1x_2 = 1$, a contradiction. Consequently, if $x_1x_2y_1y_2 = 1$ and $x_1x_2 \neq 1$, the result follows since then $(x_1, y_1) + (x_2, y_2) = \big((x_1y_1 + x_2y_2)(1 + y_1y_2)(x_1 + x_2) : (x_1y_1 + x_2y_2)(1 + x_1x_2)(y_1 + y_2) : 0\big) = (a : b : 0)$, provided that $x_1 \neq x_2$ and $y_1 \neq y_2$.

Projective formulæ We now present the projective version of the addition formulæ. It is useful to introduce some notation. When analyzing the performance, we will let M and D respectively denote the cost of a multiplication and of a multiplication by a constant, in $\mathbb{F}_{2^m}$. The cost of additions and squarings in $\mathbb{F}_{2^m}$ will be neglected.

For the point doubling (Eq. (4)) of $\boldsymbol{P} = (X_1 : Y_1 : Z_1)$, we get

$$\begin{cases} X_3 = \alpha \cdot {X_1}^2 {Z_1}^2 (Y_1 + Z_1)^4 \\ Y_3 = \beta \cdot {Y_1}^2 {Z_1}^2 (X_1 + Z_1)^4 \\ Z_3 = (X_1 Y_1 + {Z_1}^2)^2 (X_1 + Z_1)^2 (Y_1 + Z_1)^2 \end{cases} ,$$

where $\alpha = \frac{a+b}{b}$ and $\beta = \frac{a+b}{a}$. In more detail, this can be evaluated as

$$m_1 = X_1 Y_1 + {Z_1}^2, \quad m_2 = X_1 Z_1, \quad m_3 = Y_1 Z_1,$$
$$X_3 = \alpha \cdot [m_2 (Y_1 + Z_1)^2]^2, \quad Y_3 = \beta \cdot [m_3 (X_1 + Z_1)^2]^2,$$
$$Z_3 = [m_1 (m_1 + m_2 + m_3)]^2,$$

that is, with $6\mathsf{M} + 2\mathsf{D}$ (here $2\mathsf{D}$ represents the cost of the two multiplications by constants α and β).

For the dedicated point addition (Eq. (5)) of $\boldsymbol{P} = (X_1 : Y_1 : Z_1)$ and $\boldsymbol{Q} = (X_2 : Y_2 : Z_2)$, we get

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

This can be evaluated with $15\mathsf{M}$ as

$$m_1 = X_1 X_2, \quad m_2 = Y_1 Y_2, \quad m_3 = Z_1 Z_2,$$
$$m_4 = (X_1 + Z_1)(X_2 + Z_2) + m_1 + m_3, \quad m_5 = (Y_1 + Z_1)(Y_2 + Z_2) + m_2 + m_3,$$
$$m_6 = m_4 (m_2 + m_3), \quad m_7 = m_5 (m_1 + m_3), \quad m_8 = m_1 m_2 + {m_3}^2,$$
$$m_9 = m_8 + (X_1 Y_1 + {Z_1}^2)(X_2 Y_2 + {Z_2}^2),$$
$$X_3 = m_6 m_9, \quad Y_3 = m_7 m_9, \quad Z_3 = m_4 m_5 m_8 \ .$$

The cost can be reduced to $14\mathsf{M}$ with extended coordinates (X_i, Y_i, Z_i, T_i) where $T_i = X_i Y_i$ $(i = 1, 2, 3)$:

$$m_1 = X_1 X_2, \quad m_2 = Y_1 Y_2, \quad m_3 = Z_1 Z_2,$$
$$m_4 = (X_1 + Z_1)(X_2 + Z_2) + m_1 + m_3, \quad m_5 = (Y_1 + Z_1)(Y_2 + Z_2) + m_2 + m_3,$$
$$m_6 = m_4 (m_2 + m_3), \quad m_7 = m_5 (m_1 + m_3), \quad m_8 = m_1 m_2 + {m_3}^2,$$
$$m_9 = m_8 + (T_1 + {Z_1}^2)(T_2 + {Z_2}^2),$$
$$X_3 = m_6 m_9, \quad Y_3 = m_7 m_9, \quad Z_3 = m_4 m_5 m_8, \quad T_3 = X_3 Y_3 \ .$$

3 Unified Point Addition

The formulæ presented in the previous section for evaluating $\boldsymbol{P}+\boldsymbol{Q}$ distinguish two cases: $\boldsymbol{P}=\boldsymbol{Q}$ (doubling) and $\boldsymbol{P}\neq\boldsymbol{Q}$ (dedicated addition). In this section, we develop addition formulæ that can be used in both cases. The corresponding operation is referred to as *unified point addition*.

The starting point is our formula for the dedicated point addition. Let $\boldsymbol{P}=(x_1,y_1)$ and $\boldsymbol{Q}=(x_2,y_2)\in E$ be two finite points, with $\boldsymbol{P}\neq\boldsymbol{Q}$. Equation (5) says that, whenever defined, $\boldsymbol{P}+\boldsymbol{Q}=(x_3,y_3)$ where

$$x_3=\frac{(x_1y_1+x_2y_2)(1+y_1y_2)}{(y_1+y_2)(1+x_1x_2y_1y_2)}\quad\text{and}\quad y_3=\frac{(x_1y_1+x_2y_2)(1+x_1x_2)}{(x_1+x_2)(1+x_1x_2y_1y_2)}\ .$$

The point addition is defined up to the curve equation. Using the additional relations $ax_i({y_i}^2+y_i+1)=by_i({x_i}^2+x_i+1)$, $i\in\{1,2\}$, we get after a lengthy and tedious calculation:

$$\begin{cases}x_3=\dfrac{b(x_1+x_2)(1+x_1x_2y_1y_2)+(a+b)x_1x_2(1+y_1y_2)}{b(1+x_1x_2)(1+x_1x_2y_1y_2)}\\ y_3=\dfrac{a(y_1+y_2)(1+x_1x_2y_1y_2)+(a+b)y_1y_2(1+x_1x_2)}{a(1+y_1y_2)(1+x_1x_2y_1y_2)}\end{cases}. \tag{6}$$

The following Sage script [21] verifies that the two formulations for x_3 are equivalent. The equivalence for y_3 follows by symmetry.

```
R.<a,b,x1,y1,x2,y2>=GF(2)[]
S=R.quotient([
  a*x1*(y1^2+y1+1)+b*y1*(x1^2+x1+1),
  a*x2*(y2^2+y2+1)+b*y2*(x2^2+x2+1)
])
verif = b*(x1*y1+x2*y2)*(1+x1*x2)*(1+y1*y2)+
      (y1+y2)*((a+b)*x1*x2*(1+y1*y2)+b*(x1+x2)*(1+x1*x2*y1*y2))
0 == S(verif)
```

Remarkably, this new expression works for doubling a point $\boldsymbol{P}=(x_1,y_1)$. Indeed, if we replace (x_2,y_2) with (x_1,y_1) in Eq. (6), we obtain

$$x_3=\frac{(a+b){x_1}^2(1+{y_1}^2)}{b(1+{x_1}^2)(1+{x_1}^2{y_1}^2)}\quad\text{and}\quad y_3=\frac{(a+b){y_1}^2(1+{x_1}^2)}{a(1+{y_1}^2)(1+{x_1}^2{y_1}^2)}\ ,$$

namely, our previous doubling formula (Eq. (4)).

The unified addition law given by Eq. (6) is defined when the denominators $b(1+x_1x_2)(1+x_1x_2y_1y_2)$ and $a(1+y_1y_2)(1+x_1x_2y_1y_2)$ are non-zero. If $x_1x_2y_1y_2=1$, $x_1x_2\neq 1$ and $y_1y_2\neq 1$ then $\boldsymbol{P}+\boldsymbol{Q}=(a:b:0)$. If $x_1x_2=1$ or $y_1y_2=1$ —namely, $\boldsymbol{P}=(x_1,y_1)$ $(\neq\boldsymbol{o})$ and $\boldsymbol{Q}\in\big\{\big(\frac{1}{x_1},y_1\big),\big(x_1,\frac{1}{y_1}\big),\big(\frac{1}{x_1},\frac{1}{y_1}\big)\big\}$, then

$$\boldsymbol{P}+\boldsymbol{Q}=\begin{cases}(1:0:0) & \text{if } x_1x_2=1 \text{ and } y_1=y_2\\ (0:1:0) & \text{if } y_1y_2=1 \text{ and } x_1=x_2\\ \big(\frac{b(1+{x_1}^2)(1+{x_1}^2{y_1}^2)}{(a+b){x_1}^2(1+{y_1}^2)},\frac{a(1+{y_1}^2)(1+{x_1}^2{y_1}^2)}{(a+b){y_1}^2(1+{x_1}^2)}\big) & \text{otherwise}\end{cases}.$$

Proof. Observe that since $\boldsymbol{Q} = (x_2, y_2)$ belongs to the curve so do $\big(\frac{1}{x_2}, y_2\big)$, $\big(x_2, \frac{1}{y_2}\big)$, and $\big(\frac{1}{x_2}, \frac{1}{y_2}\big)$. Suppose first that $x_1 x_2 = 1 \iff x_2 = \frac{1}{x_1}$. Now using the fact that (x_1, y_1) and $\big(\frac{1}{x_1}, y_2\big)$ are on the curve implies that $(y_1 + y_2)(y_1 + y_2 + 1) = (y_1 + y_2)\big(y_1 + 1 + \frac{1}{y_1}\big) \iff (y_1 + y_2)(\frac{1}{y_1} + y_2) = 0$. This means that $(x_2, y_2) \in \big\{\big(\frac{1}{x_1}, y_1\big), \big(\frac{1}{x_1}, \frac{1}{y_1}\big)\big\}$.

Analogously, it can be shown that $y_1 y_2 = 1$ implies $(x_1 + x_2)\big(\frac{1}{x_1} + x_2\big) = 0$, that is, $(x_2, y_2) \in \big\{\big(x_1, \frac{1}{y_1}\big), \big(\frac{1}{x_1}, \frac{1}{y_1}\big)\big\}$. □

The cases where the points $\boldsymbol{P}$ and/or $\boldsymbol{Q}$ are at infinity are detailed in the previous section.

To sum up, noting that the case $\boldsymbol{P} = (x_1, y_1)$ and $\boldsymbol{Q} \in \big\{\big(\frac{1}{x_1}, y_1\big), \big(x_1, \frac{1}{y_1}\big), \big(\frac{1}{x_1}, \frac{1}{y_1}\big)\big\}$ corresponds to $\boldsymbol{P}+\boldsymbol{Q} = (1:0:0)$, $\boldsymbol{P}+\boldsymbol{Q} = (0:1:0)$ or $\boldsymbol{Q} = \boldsymbol{P} + (a : b : 0)$, we see that the exceptional cases always involve the points at infinity. This leads to the following result.

Proposition 1. *Let E be a binary Huff curve over $\mathbb{F}_{2^m}$ and let $\mathbb{G} \subset E(\mathbb{F}_{2^m})$ be a subgroup such that $(a : b : 0), (1 : 0 : 0), (0 : 1 : 0) \notin \mathbb{G}$. Then the unified addition formula given by Eq.* (6) *is complete.* □

In particular, the addition formula is complete in a subgroup of odd order, provided that $(1 : 0 : 0)$ and $(0 : 1 : 0)$ are both of even order.

Projective version Here we give the projective version of Eq. (6). For $\boldsymbol{P} = (X_1 : Y_1 : Z_1)$ and $\boldsymbol{Q} = (X_2 : Y_2 : Z_2)$, we get $\boldsymbol{P} + \boldsymbol{Q} = (X_3 : Y_3 : Z_3)$ with

$$\begin{cases} X_3 = (Z_1Z_2 + Y_1Y_2)\big((X_1Z_2 + X_2Z_1)({Z_1}^2{Z_2}^2 + X_1X_2Y_1Y_2) + \\ \qquad\qquad\qquad \alpha X_1X_2Z_1Z_2(Z_1Z_2 + Y_1Y_2)\big) \\ Y_3 = (Z_1Z_2 + X_1X_2)\big((Y_1Z_2 + Y_2Z_1)({Z_1}^2{Z_2}^2 + X_1X_2Y_1Y_2) + \\ \qquad\qquad\qquad \beta Y_1Y_2Z_1Z_2(Z_1Z_2 + X_1X_2)\big) \\ Z_3 = (Z_1Z_2 + X_1X_2)(Z_1Z_2 + Y_1Y_2)({Z_1}^2{Z_2}^2 + X_1X_2Y_1Y_2) \end{cases} \tag{7}$$

where $\alpha = \frac{a+b}{b}$ and $\beta = \frac{a+b}{a}$. This can be evaluated as

$$\begin{gathered} m_1 = X_1X_2, \quad m_2 = Y_1Y_2, \quad m_3 = Z_1Z_2, \\ m_4 = (X_1 + Z_1)(X_2 + Z_2) + m_1 + m_3, \quad m_5 = (Y_1 + Z_1)(Y_2 + Z_2) + m_2 + m_3 \\ m_6 = m_1m_3, \quad m_7 = m_2m_3, \quad m_8 = m_1m_2 + {m_3}^2, \\ m_9 = m_6(m_2 + m_3)^2, \quad m_{10} = m_7(m_1 + m_3)^2, \\ m_{11} = m_8(m_2 + m_3), \quad m_{12} = m_8(m_1 + m_3), \\ X_3 = m_4m_{11} + \alpha \cdot m_9, \quad Y_3 = m_5m_{12} + \beta \cdot m_{10}, Z_3 = m_{11}(m_1 + m_3), \end{gathered}$$

that is, with $15\mathsf{M} + 2\mathsf{D}$ (again $2\mathsf{D}$ represents the cost of the two multiplications by constants α and β).

More formulæ There are other unified addition formulæ similar to Eq. (6). For instance, whenever defined, we also have

$$\begin{cases} x_3 = \dfrac{(1+y_1y_2)\big(b(x_1+x_2)+x_1x_2(a+b+ay_1+ay_2)\big)}{b(1+x_1x_2)(1+x_1x_2y_1y_2)} \\ y_3 = \dfrac{(1+x_1x_2)\big(a(y_1+y_2)+y_1y_2(a+b+bx_1+bx_2)\big)}{a(1+y_1y_2)(1+x_1x_2y_1y_2)} \end{cases} .$$

Alternate unified formulæ can be obtained by selecting another neutral element. This results in translating the group law. For instance, defining $\boldsymbol{o}' = (a : b : 0)$ as the neutral element yields, whenever defined, the following unified point addition formula:

$$\begin{cases} x_3 &= \dfrac{b(1+x_1x_2)(1+x_1x_2y_1y_2)}{b(x_1+x_2)(1+x_1x_2y_1y_2)+(a+b)x_1x_2(1+y_1y_2)} \\ &= \dfrac{b(1+x_1x_2)^2(1+x_1x_2y_1y_2)y_1y_2}{\big[b(x_1+x_2)(1+x_1x_2y_1y_2)+(a+b)x_1x_2(1+y_1y_2)\big](1+x_1x_2)y_1y_2} \\ y_3 &= \dfrac{a(1+y_1y_2)(1+x_1x_2y_1y_2)}{a(y_1+y_2)(1+x_1x_2y_1y_2)+(a+b)y_1y_2(1+x_1x_2)} \\ &= \dfrac{a(1+y_1y_2)^2(1+x_1x_2y_1y_2)x_1x_2}{\big[b(x_1+x_2)(1+x_1x_2y_1y_2)+(a+b)x_1x_2(1+y_1y_2)\big](1+x_1x_2)y_1y_2} \end{cases} .$$

Advantageously, the corresponding projective version can be evaluated with $13\mathsf{M}+2\mathsf{D}$ as

$$\begin{gathered} m_1 = X_1X_2, \quad m_2 = Y_1Y_2, \quad m_3 = Z_1Z_2, \quad m_4 = m_1m_2, \\ m_5 = m_2m_3, \quad m_6 = (X_1+Z_1)(X_2+Z_2)+m_1+m_3 \\ X_3 = (m_1+m_3)(m_4+m_5)({m_3}^2+m_4), \quad Y_3 = \rho m_1(m_2+m_3)^2({m_3}^2+m_4), \\ Z_3 = (m_4+m_5)\big[(\alpha m_1({m_3}^2+m_5)+m_6(m_4+{m_3}^2)\big], \end{gathered}$$

where $\alpha = \frac{a+b}{b}$ and $\rho = \frac{a}{b}$.

4 Differential Point Addition

The so-called Montgomery representation was developed in [16] in order to speed up the implementation of the elliptic curve factoring method (ECM) [12]. It was subsequently adapted to (ordinary) Weierstraß elliptic curves over binary fields in [13, 20] (see also [6]). The idea stems from the observation that the x-coordinate of the sum of two points can be evaluated from two x-coordinates of the input points and the x-coordinate of their difference. More generally, a *differential point addition* consists in calculating $w(\boldsymbol{P}+\boldsymbol{Q})$ from $w(\boldsymbol{P})$, $w(\boldsymbol{Q})$ and $w(\boldsymbol{Q}-\boldsymbol{P})$, for a certain coordinate function w. When such an operation is available, the value of $w([k]\boldsymbol{P})$ can be efficiently computed from the binary expansion of scalar k, $k = \sum_{i=0}^{\ell-1} k_i\, 2^i$ with $k_i \in \{0,1\}$ and $k_{\ell-1} = 1$. Defining $\kappa_j = \sum_{i=j}^{\ell-1} k_i\, 2^i$, $\boldsymbol{P_j} = [\kappa_j]\boldsymbol{P}$, and $\boldsymbol{Q_j} = \boldsymbol{P_j} + \boldsymbol{P}$, we have

$$\big(w(\boldsymbol{P_{\ell-1}}), w(\boldsymbol{Q_{\ell-1}})\big) = \big(w(\boldsymbol{P}), w(\boldsymbol{P}+\boldsymbol{P})\big)$$

and

$$\big(w(\boldsymbol{P_j}), w(\boldsymbol{Q_j})\big) = \begin{cases} \big(w(\boldsymbol{P_{j+1}} + \boldsymbol{P_{j+1}}), w(\boldsymbol{P_{j+1}} + \boldsymbol{Q_{j+1}})\big) & \text{if } k_j = 0 \\ \big(w(\boldsymbol{P_{j+1}} + \boldsymbol{Q_{j+1}}), w(\boldsymbol{Q_{j+1}} + \boldsymbol{Q_{j+1}})\big) & \text{if } k_j = 1 \end{cases} ,$$

for $j = \ell - 2, \ldots, 0$. Remarking that $\kappa_0 = k$, the value of $w([k]\boldsymbol{P})$ is obtained at the end of the recursion as $w(\boldsymbol{P_0})$.

As shown in Section 2, the inverse of a point $\boldsymbol{P} = (x_1, y_1)$ on a binary Huff curve is given by $-\boldsymbol{P} = (\bar{x_1}, \bar{y_1})$ with $\bar{x_1} = \frac{y_1(b+ax_1y_1)}{a+bx_1y_1}$ and $\bar{y_1} = \frac{x_1(a+bx_1y_1)}{b+ax_1y_1}$. A natural choice for coordinate function $w : \boldsymbol{P} \mapsto w(\boldsymbol{P})$ is therefore to define it as the product of the x- and y-coordinates, or as a function thereof. Doing so, we see that $w(\boldsymbol{P}) = w(-\boldsymbol{P})$.

Specifically, for a finite point $\boldsymbol{P} = (x_1, y_1)$, we define $w(\boldsymbol{P}) = x_1y_1$. For the points at infinity, we define $w(1 : 0 : 0) = \frac{a}{b}$, $w(0 : 1 : 0) = \frac{b}{a}$, and $w(a : b : 0) =$ "∞" $= (1 : 0)$. Hence, for the differential doubling, we immediately obtain from Eq. (4),

$$w([2]\boldsymbol{P}) = \frac{\gamma \cdot {w_1}^2}{(1 + w_1)^4} \quad \text{with } \gamma = \tfrac{(a+b)^2}{ab} \,, \tag{8}$$

and where $w_1 = w(\boldsymbol{P})$, provided that $w_1 \neq 1$. If $w_1 = 1$ then $w([2]\boldsymbol{P}) = (1 : 0)$.

Let $\boldsymbol{Q}$ be a second point, different from $\boldsymbol{P}$. We let w_1, w_2, and $\bar{w}$ denote the w-coordinate of $\boldsymbol{P}$, $\boldsymbol{Q}$, and $\boldsymbol{Q} - \boldsymbol{P}$, respectively. In principle, it could be possible to derive the formula for the differential addition from Eq. (5). A much simpler way is to rely on the connection between our choice of the w-coordinate and the birational map with the Weierstraß equation; cf. Eq. (2).

Montgomery representation comes in two flavors: additive method and multiplicative method. From the additive formula in [13, Lemma 1] (slightly generalized), whenever defined, we get

$$w(\boldsymbol{P} + \boldsymbol{Q}) = \frac{\bar{w} \cdot (w_1 + w_2)^2}{(w_1 + w_2)^2 + (\gamma\bar{w}) \cdot w_1w_2} \quad \text{with } \gamma = \tfrac{(a+b)^2}{ab} \;.$$

An application of the multiplicative formula in [20, § 3.2] yields after simplification

$$w(\boldsymbol{P} + \boldsymbol{Q}) = \frac{(w_1 + w_2)^2}{\bar{w} \cdot (1 + w_1w_2)^2} \,, \tag{9}$$

provided that $w_1w_2 \neq 1$. (Note that $\bar{w} \neq 0$ since $\boldsymbol{P} \neq \boldsymbol{Q}$.) The case $w_1w_2 = 1$ corresponds to the case $x_1x_2y_1y_2 = 1$; see Section 2. If $w_1w_2 = 1$ then $w(\boldsymbol{P} + \boldsymbol{Q}) = (1 : 0)$.

Projective version To have projective formulæ, we represent the w-coordinate of a point $\boldsymbol{P}$ by the pair $(W : Z) = (\theta\, w(\boldsymbol{P}) : \theta)$ if $\boldsymbol{P} \neq (a : b : 0)$, and

$(W : Z) = (\theta : 0)$ if $\boldsymbol{P} = (a : b : 0)$, for some non-zero $\theta \in \mathbb{F}_{2^m}$. Letting $w_i = (W_i : Z_i)$ for $i = 1, 2$, and $\bar{w} = (\bar{W} : \bar{Z})$, we obtain from Eqs (8) and (9)

$$\begin{cases} W([2]\boldsymbol{P}) = \gamma \cdot (W_1 Z_1)^2 \\ Z([2]\boldsymbol{P}) = (W_1 + Z_1)^4 \end{cases}$$

and

$$\begin{cases} W(\boldsymbol{P}+\boldsymbol{Q}) = \bar{Z}(W_1 Z_2 + W_2 Z_1)^2 \\ Z(\boldsymbol{P}+\boldsymbol{Q}) = \bar{W}(W_1 W_2 + Z_1 Z_2)^2 \end{cases} .$$

The differential point doubling requires 1M + 1D (where D is the cost of a multiplication by γ) and, by computing $W_1Z_2 + W_2Z_1$ as $(W_1 + Z_1)(W_2 + Z_2) + (W_1W_2 + Z_1Z_2)$, the differential point addition requires 5M. The cost of the differential point addition reduces to 4M when $\bar{Z} = 1$. Using the above scalar multiplication algorithm, the computation of $w([k]\boldsymbol{P})$ can therefore be evaluated with 5M + 1D per bit of scalar k. Furthermore, we note that over a binary field of even extension (i.e., over $\mathbb{F}_{2^m}$ with m even), selecting the ratio $a/b = \zeta$ (with $\zeta^2 + \zeta + 1 = 0$) leads to $\gamma = 1$ and so reduces the cost of the differential point doubling to 1M.

5 Generalized Binary Huff Curves

The transformations given by Eq. (2) show how to express any binary Huff curve as a Weierstraß curve. The reverse direction is however not always possible. Not all ordinary elliptic curves over $\mathbb{F}_{2^m}$ can be expressed in the Huff form as defined by Eq. (1). Worse, none of the NIST-recommended curves [17] can be written in this model. In this section, we generalize the definition of binary Huff curves to cover all isomorphism classes of ordinary curves over $\mathbb{F}_{2^m}$, for $m \geq 4$.

In [9, Section 3], Huff's model is generalized to $ax\mathcal{P}(y) = by\mathcal{P}(x)$ for some monic polynomial $\mathcal{P} \in \mathbb{F}_{2^m}[t]$, of degree 2, with non-zero discriminant, and such that $\mathcal{P}(0) \neq 0$. Binary Huff curves correspond to the choice $\mathcal{P}(t) = t^2 + t + 1$. We consider below a more general polynomial, namely, $\mathcal{P}(t) = t^2 + ft + 1$ with $f \neq 0$.

Definition 2. *A* generalized binary Huff curve *is the locus in* $\mathbb{P}^2(\mathbb{F}_{2^m})$ *of the equation*

$$aX(Y^2 + fYZ + Z^2) = bY(X^2 + fXZ + Z^2)\,, \tag{10}$$

where $a, b, f \in \mathbb{F}_{2^m}^*$ *and* $a \neq b$.

Remark 3. There are other suitable generalizations of binary Huff curves, like $\mathcal{P}(t) = t^2 + t + e$ with $e \neq 0$. We selected $\mathcal{P}(t) = t^2 + ft + 1$ since the arithmetic looked slightly simpler. Note also that polynomial $\mathcal{P}(t) = t^2 + ft + e$ (with $e, f \neq 0$) is not more general since the change of variables $(x, y) \leftarrow (\sqrt{e}\,\bar{x}, \sqrt{e}\,\bar{y})$ transforms the equation $ax(y^2 + fy + e) = by(x^2 + fx + e)$ into $a\bar{x}(\bar{y}^2 + f'\bar{y} + 1) = b\bar{y}(\bar{x}^2 + f'\bar{x} + 1)$ where $f' = f/\sqrt{e}$.

The affine model of Eq. (10) is $ax(y^2+fy+1) = by(x^2+fx+1)$. It is birationally equivalent to the Weierstraß elliptic curve

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

under the inverse maps

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

The points at infinity are $(a:b:0)$, $(1:0:0)$ and $(0:1:0)$. Point $\boldsymbol{A}$, namely the point of intersection of the tangent line at $\boldsymbol{o}$ with the curve, becomes $\boldsymbol{A} = \left(\frac{bf}{a+b}, \frac{af}{a+b}\right)$.

Before stating the universality of the generalized model, we summarize some elementary results on binary fields that are needed to understand the proof. We let Tr denote the trace function defined as the linear function given by $\mathrm{Tr} : \mathbb{F}_{2^m} \to \mathbb{F}_2, \theta \mapsto \sum_{j=0}^{m-1} \theta^{2^j}$. We recall that the quadratic equation $x^2+Ax+B=0$ with $A \neq 0$ has a solution in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}(B/A^2) = 0$. If x_0 is a solution then the other solution is $x_0 + A$. Finally, it is easy to see that $\mathrm{Tr}(A^2) = \mathrm{Tr}(A)$ for $A \in \mathbb{F}_{2^m}$.

Proposition 2. *Let $m \geq 4$. Each ordinary elliptic curve over $\mathbb{F}_{2^m}$ is birationally equivalent over $\mathbb{F}_{2^m}$ to a generalized binary Huff curve.*

Proof. Each ordinary elliptic curve over $\mathbb{F}_{2^m}$ is isomorphic to $v^2+uv = u^3 + a_2u^2 + a_6$ for some $a_2, a_6 \in \mathbb{F}_{2^m}$, $a_6 \neq 0$. Further, from [19, Proposition 3.1(b) and Table 1.2], the Weierstraß curves $v^2+uv = u^3+a_2u^2+a_6$ and $v(v+(a+b)fu) = u(u+a^2)(u+b^2)$ are isomorphic under the admissible change of variables $(u,v) \leftarrow (\mu^2u, \mu^3(v+su+\sqrt{a_6}))$ with $\mu = (a+b)f$ if and only if the curve parameters satisfy

$$s^2+s+a_2+f^{-2} = 0 \quad \text{and} \quad (a+b)^4f^4\sqrt{a_6} = a^2b^2$$

for some s. The equation $s^2+s+a_2+f^{-2} = 0$ has a solution $s \in \mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}(a_2+f^{-2}) = 0 \iff \mathrm{Tr}(f^{-1}) = \mathrm{Tr}(a_2)$. Dividing the second equation by b^4 and letting $t = \frac{a^2}{b^2}$ yields $t^2 + \frac{1}{f^4\sqrt{a_6}}t + 1 = 0$, which has a solution $t \in \mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}(f^8a_6) = \mathrm{Tr}(f\sqrt[8]{a_6}) = 0$. Consequently, given an ordinary binary elliptic curve $v^2+uv = u^3+a_2u^2+a_6$, one can obtain an isomorphic curve $v(v+(a+b)fu) = u(u+a^2)(u+b^2)$ —and so the birationally equivalent generalized binary Huff curve $ax(y^2+fy+1) = by(x^2+fx+1)$, by choosing parameter f such that $\mathrm{Tr}(f^{-1}) = \mathrm{Tr}(a_2)$ and $\mathrm{Tr}(f\sqrt[8]{a_6}) = 0$, and parameters a and b such that $\frac{a^2}{b^2}$ is a solution to $t^2 + \frac{1}{f^4\sqrt{a_6}}t + 1 = 0$.

It remains to show that such an f always exists. The proof proceeds analogously to the one offered in [2, Theorem 4.3]. Fix $a_2 \in \mathbb{F}_{2^m}$ and $a_6 \in \mathbb{F}_{2^m}^*$. For each $\delta, \epsilon \in \mathbb{F}_2$, define

$$D_{\delta,\epsilon} = \{f \in \mathbb{F}_{2^m}^* : \mathrm{Tr}(f^{-1}) = \delta, \mathrm{Tr}(f\sqrt[8]{a_6}) = \epsilon\} \ .$$

We have to show that the set $D_{\mathrm{Tr}(a_2),0}$ is non-empty.

We have $\#D_{0,0} + \#D_{1,0} = 2^{m-1} - 1$. Indeed, as f runs through $\mathbb{F}_{2^m}^*$, so does $f\sqrt[8]{a_6}$. Hence, $\#D_{0,0} + \#D_{1,0}$ is the number of $f \in \mathbb{F}_{2^m}^*$ with $\mathrm{Tr}(f) = 0$. We also have $\#D_{1,0} + \#D_{1,1} = 2^{m-1}$. Indeed, for the same reason, $\#D_{1,0} + \#D_{1,1}$ is the number of $f \in \mathbb{F}_{2^m}^*$ with $\mathrm{Tr}(f) = 1$.

We compute $\#D_{0,0} + \#D_{1,1}$, which is equal to the number of $f \in \mathbb{F}_{2^m}^*$ with $\mathrm{Tr}(f^{-1} + f\sqrt[8]{a_6}) = 0$. For each f with $\mathrm{Tr}(f^{-1} + f\sqrt[8]{a_6}) = 0$, there are exactly two choices of $x \in \mathbb{F}_{2^m}$ such that $x^2 + x + f^{-1} + f\sqrt[8]{a_6} = 0 \iff f^2x^2 + f^2x = f + f^3\sqrt[8]{a_6}$, producing two points (f, fx) on the elliptic curve $v^2 + uv = \sqrt[8]{a_6}u^3 + u$. Hasse's theorem says that this curve has $2^m + 1 + \tau$ points for some integer τ in the interval $[-2\sqrt{2^m}, 2\sqrt{2^m}]$. Since all points of this curve but $(0,0)$ and the point at infinity appear as (f, fx), it follows that $\#D_{0,0} + \#D_{1,1} = 2^{m-1} + (\tau - 1)/2$. Finally, we have $4\#D_{1,0} = 2(\#D_{0,0} + \#D_{1,0}) + 2(\#D_{1,0} + D_{1,1}) - 2(\#D_{0,0} + \#D_{1,1}) = 2^m - (\tau + 1)$ and $4\#D_{0,0} = 4(2^{m-1} - 1) - 4\#D_{1,0} = 2^m + (\tau - 3)$. Since $\tau \in [-2\sqrt{2^m}, 2\sqrt{2^m}]$, this implies $\#D_{1,0} \geq \frac{2^m - 2\sqrt{2^m} - 1}{4}$ and $\#D_{0,0} \geq \frac{2^m - 2\sqrt{2^m} - 3}{4}$. The result now follows by remarking that $2^m - 2\sqrt{2^m} - 1 > 2^m - 2\sqrt{2^m} - 3 > 0$ for $m \geq 4$. This is true since $(\sqrt{2^m} - 1)^2 \geq (\sqrt{2^4} - 1)^2 > 4$, which yields $2^m - 2\sqrt{2^m} + 1 > 4 \iff 2^m - 2\sqrt{2^m} - 3 > 0$. □

The arithmetic on generalized binary Huff curves is easily derived from the formulæ given in Section 2. Let $E^\dagger$ be a generalized binary Huff curve as per Eq. (10). Let also $\boldsymbol{P} = (x_1, y_1)$ and $\boldsymbol{Q} = (x_2, y_2) \in E^\dagger$ be two finite points. The formula given by Eq. (3) remains valid for computing the inverse of $\boldsymbol{P}$. An alternate expression for $-\boldsymbol{P} = (\bar{x_1}, \bar{y_1})$ is, whenever defined,

$$\bar{x_1} = \frac{y_1(\hat{\alpha}x_1 + 1)}{\hat{\beta}y_1 + 1} \quad \text{and} \quad \bar{y_1} = \frac{x_1(\hat{\beta}y_1 + 1)}{\hat{\alpha}x_1 + 1} \quad . \tag{11}$$

where $\hat{\alpha} = \frac{a+b}{bf}$ and $\hat{\beta} = \frac{a+b}{af}$. The exceptional points of Eq. (11) are $\boldsymbol{P} = \left(\frac{a+b}{bf}, \frac{af}{a+b}\right)$, $\boldsymbol{P} = \left(\frac{bf}{a+b}, \frac{af}{a+b}\right)$, $\boldsymbol{P} = \left(\frac{bf}{a+b}, \frac{a+b}{af}\right)$, and $\boldsymbol{P} = \left(\frac{a+b}{bf}, \frac{a+b}{af}\right)$, the inverses of which are $-\boldsymbol{P} = (1:0:0)$, $-\boldsymbol{P} = \left(\frac{bf(a+b+af)^2}{(a+b)(a+b+bf)^2}, \frac{af(a+b+bf)^2}{(a+b)(a+b+af)^2}\right)$, $-\boldsymbol{P} = (0:1:0)$, and $-\boldsymbol{P} = \left(\frac{(a+b)(a+b+bf)^2}{bf(a+b+af)^2}, \frac{(a+b)(a+b+af)^2}{af(a+b+bf)^2}\right)$, respectively.

The doubling formula (Eq. (4)) becomes $[2]\boldsymbol{P} = (x_3, y_3)$ with

$$x_3 = \frac{f(a+b){x_1}^2(1+y_1)^2}{b(1+x_1)^2(1+x_1y_1)^2} \quad \text{and} \quad y_3 = \frac{f(a+b){y_1}^2(1+x_1)^2}{a(1+y_1)^2(1+x_1y_1)^2} \quad . \tag{12}$$

The exceptional cases are handled in the same way as in Section 2. We note that the condition $x_1y_1 = 1$ is only possible when $\mathrm{Tr}(f^{-1}) = 0$.

The formula for dedicated point addition (Eq. (5)) is unchanged. For the unified point addition, we get, whenever defined, $\boldsymbol{P} + \boldsymbol{Q} = (x_3, y_3)$ with

$$\begin{cases} x_3 = \dfrac{b(x_1+x_2)(1+x_1x_2y_1y_2) + f(a+b)x_1x_2(1+y_1y_2)}{b(1+x_1x_2)(1+x_1x_2y_1y_2)} \\ y_3 = \dfrac{a(y_1+y_2)(1+x_1x_2y_1y_2) + f(a+b)y_1y_2(1+x_1x_2)}{a(1+y_1y_2)(1+x_1x_2y_1y_2)} \end{cases} \quad . \tag{13}$$

The exceptional cases are the same as for the (regular) binary Huff curves. In particular, Proposition 1 remains valid for generalized binary Huff curves: unified addition is complete in any subgroup that does not contain the points at infinity.

Furthermore, the performance is unchanged. This is easily seen by comparing the generalized formulæ of this section with the previous ones (i.e., for $f = 1$). The cost of a point doubling, dedicated point addition, and unified point addition is of $6\mathsf{M} + 2\mathsf{D}$, $15\mathsf{M}$ (or $14\mathsf{M}$ with extended coordinates), and $15\mathsf{M} + 2\mathsf{D}$, respectively. This is better than with binary Edwards curves [5] but, contrary to Edwards' form, unified addition is guaranteed to be complete only in certain proper subgroups.

To sum up, the generalized model presented in this section can be used to represent any ordinary elliptic curve over a finite field of characteristic two; this includes all NIST-recommended curves. It offers a competitive arithmetic leading to efficient implementations. Further, they can be made secure against certain side-channel attacks [11] for cryptographic applications. When the operations of point addition and point doubling make use of different formulæ, they may produce different power traces revealing the secret value of scalar k in the computation of $\boldsymbol{Q} = [k]\boldsymbol{P}$. There are basically three known approaches to circumvent the leakage: *(i)* unifying the addition formulæ, *(ii)* inserting dummy operations, and *(iii)* using regular scalar multiplication algorithms [3, Chapter V]. We note that with the second approach the resulting implementations become vulnerable to safe-error attacks [22]. The so-called Montgomery ladder [16] is an example of a regular scalar multiplication algorithm (third approach). It can be used with the differential point addition formulæ given in Section 4. Given their connection with those of the Weierstraß model, the so-obtained, Huff-based, implementations are equally efficient as the fastest implementations of the Montgomery ladder. But the main advantage of (generalized) Huff curves is that they are equipped with unified point addition formulæ: the same formulæ can be used for doubling or adding points, as required by the first approach against side-channel leakage. The formulæ are even complete — in a subgroup that does not contain the points at infinity. Very few models are known to feature a complete addition law. The Edwards model, as introduced by Bernstein *et al.* in [2], has a such addition law and without any restriction. But this comes at a price: $18\mathsf{M} + 7\mathsf{D}$ (or $21\mathsf{M} + 4\mathsf{D}$) are needed for the complete addition of two points on a binary Edwards curve. Therefore, whenever applicable, the (generalized) binary Huff model should be preferred since it offers faster complete addition formulæ. Other cryptographic applications of complete addition law include protection against exceptional procedure attacks [8] and batch computing [1].

6 Conclusion

This paper studied in detail the addition law for a new model for elliptic curves. While much attention has been paid to elliptic curves over fields of large characteristic, fewer models are known for elliptic curves over binary fields. Our results add the Huff model to the cryptographer's toolbox for the implementation of elliptic curve cryptography in characteristic two. Its distinct arithmetic features may offer an interesting alternative in a number of applications.

Acknowledgments

We are very grateful to the anonymous referees for their useful comments and suggestions.

References

1. Bernstein, D.J.: Batch binary Edwards. In: Halevi, S. (ed.) Advances in Cryptology − CRYPTO 2009. Lecture Notes in Computer Science, vol. 5677, pp. 317–336. Springer (2009)
2. Bernstein, D.J., Lange, T., Farashahi, R.R.: Binary Edwards curves. In: Oswald, E., Rohatgi, P. (eds.) Cryptographic Hardware and Embedded Systems − CHES 2008. Lecture Notes in Computer Science, vol. 5154, pp. 244–265. Springer (2008)
3. Blake, I.F., Seroussi, G., Smart, N.P. (eds.): Advances in Elliptic Curve Cryptography, London Mathematical Society Lecture Note Series, vol. 317. Cambridge University Press (2005)
4. Chudnovsky, D.V., Chudnovsky, G.V.: Sequences of numbers generated by addition in formal groups and new primality and factorization tests. Advances in Applied Mathematics 7(4), 385–434 (1986)
5. Explicit-formulas database (EFD). `http://www.hyperelliptic.org/EFD/`
6. Gaudry, P., Lubicz, D.: The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines. Finite Fields and Applications 15, 246–260 (2009)
7. Huff, G.B.: Diophantine problems in geometry and elliptic ternary forms. Duke Math. J. 15, 443–453 (1948)
8. Izu, T., Takagi, T.: Exceptional procedure attack on elliptic curve cryptosystems. In: Desmedt, Y. (ed.) Public Key Cryptography − PKC 2003. Lecture Notes in Computer Science, vol. 2567, pp. 224–239. Springer (2003)
9. Joye, M., Tibouchi, M., Vergnaud, D.: Huff's model for elliptic curves. In: Hanrot, G., Morain, F., Thomé, E. (eds.) Algorithmic Number Theory (ANTS-IX). Lecture Notes in Computer Science, vol. 6197, pp. 234–250. Springer (2010)
10. Koblitz, N.: Elliptic curve cryptosystems. Mathematics of Computation 48, 203–209 (1987)
11. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) Advances in Cryptology − CRYPTO '99. Lecture Notes in Computer Science, vol. 1666, pp. 388–397. Springer-Verlag (1999)
12. Lenstra, Jr., H.W.: Factoring integers with elliptic curves. Annals of Mathematics 126(2), 649–673 (1987)
13. López, J., Dahab, R.: Fast multiplication on elliptic curves over $GF(2^m)$ without precomputation. In: Koç, Ç., Paar, C. (eds.) Cryptographic Hardware and Embedded Systems − CHES '99. Lecture Notes in Computer Science, vol. 1717, pp. 316–327. Springer (1999)
14. Menezes, A., Okamoto, T., Vanstone, S.: Reducing elliptic curve discrete logaritms to a finite field. IEEE Transactions on Information Theory 39(5), 1639–1646 (1993)
15. Miller, V.S.: Use of elliptic curves in cryptography. In: Williams, H.C. (ed.) Advances in Cryptology − CRYPTO '85. Lecture Notes in Computer Science, vol. 218, pp. 417–426. Springer (1986)

16. Montgomery, P.L.: Speeding up the Pollard and elliptic curve methods of factorization. Mathematics of Computation 48(177), 243–264 (1987)
17. National Institute of Standards and Technology: Recommended elliptic curves for federal government use. `http://csrc.nist.gov/CryptoToolkit/dss/ecdsa/NISTReCur.pdf` (July 1999)
18. Peeples, Jr., W.D.: Elliptic curves and rational distance sets. Proc. Am. Math. Soc. 5, 29–33 (1954)
19. Silverman, J.H.: The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, vol. 106, chap. III. Springer-Verlag (1986)
20. Stam, M.: On Montgomery-like representations for elliptic curves over $GF(2^k)$. In: Desmedt, Y. (ed.) Public Key Cryptography − PKC 2003. Lecture Notes in Computer Science, vol. 2567, pp. 240–253. Springer (2003)
21. Stein, W.A., et al.: Sage Mathematics Software (Version 4.5.1). The Sage Development Team (2010), `http://www.sagemath.org`
22. Yen, S.M., Joye, M.: Checking before output may not be enough against fault-based cryptanalysis. IEEE Transactions on Computers 49(9), 967–970 (2000)