On a new generalization of Huff curves

Abdoul Aziz Ciss and Djiby Sow

École doctorale de Mathématiques et d'Informatique,
Université Cheikh Anta Diop de Dakar, Sénégal
BP: 5005, Dakar Fann
abdoul.ciss@ucad.edu.sn,sowdjibab@ucad.sn

Abstract. Recently two kinds of Huff curves were introduced as elliptic curves models and their arithmetic was studied. It was also shown that they are suitable for cryptographic use such as Montgomery curves or Koblitz curves (in Weierstrass form) and Edwards curves.
In this work, we introduce the new generalized Huff curves $ax(y^2 - c) = by(x^2 - d)$ with $abcd(a^2c - b^2d) \neq 0$, which contains the generalized Huff's model $ax(y^2 - d) = by(x^2 - d)$ with $abd(a^2 - b^2) \neq 0$ of Joye-Tibouchi-Vergnaud and the generalized Huff curves $x(ay^2 - 1) = y(bx^2 - 1)$ with $ab(a - b) \neq 0$ of Wu-Feng as a special case.
The addition law in projective coordinates is as fast as in the previous particular cases. More generally all good properties of the previous particular Huff curves, including completeness and independence of two of the four curve parameters, extend to the new generalized Huff curves. We verified that the method of Joye-Tibouchi-Vergnaud for computing of pairings can be generalized over the new curve.

Keywords: Huff curves, pairing, divisor, Jacobian, Miller algorithm, elliptic curve models, Edwards curves, Koblitz Curves

Introduction

Since their introduction in cryptography by Koblitz [17], Miller [23] and Menezes [19], elliptic curves have been extensively used because they allow small key size and discrete logarithm is much more difficult in elliptic curve than in $(\mathbb{Z}/p\mathbb{Z})^*$ where p is a prime. Furthermore, pairings on elliptic curve have received major interest, due to their use to design cryptographic tools such as cryptanalysis technics or protocols.

It is known that elliptic curves can be represented in different forms. This different forms induces different arithmetic properties, to obtain faster scalar multiplications, various forms of elliptic curves have been extensively studied in the last two decades.

Recently, Joye, Tibouchi and Vergnaud revisits for finite fields, in [16] a model for elliptic curves over $\mathbb{Q}$ introduced in [13] by Huff in 1948 in order to study a diophantine problem.

We have the following list of Huff form elliptic curves.

1) The Huff curves (by Huff in [13]) over a field K, $\mathrm{char}(K) \neq 2$, are of the form:
$$ax(y^2-1) = by(x^2-1) \text{ with } a^2-b^2 \neq 0,$$
2) The first generalized Huff curves (by Joye, Tibouchi and Vergnaud in [16]) over a field K, $\mathrm{char}(K) \neq 2$, are of the form:
$$ax(y^2-d) = by(x^2-d) \text{ with } abd(a^2-b^2) \neq 0,$$
3) The second generalized Huff curves (by Wu and Feng in [11]) over a field K, $\mathrm{char}(K) \neq 2$, are of the form:
$$x(ay^2-1) = y(bx^2-1) \text{ with } ab(a-b) \neq 0,$$
4) The third generalized Huff curves (presented in this paper) over a field K, $\mathrm{char}(K) \neq 2$, are of the form:
$$ax(y^2-c) = by(x^2-d) \text{ with } abcd(a^2c-b^2d) \neq 0,$$
5) The binary Huff curves (by Joye, Tibouchi and Vergnaud [16]) over a field K, $\mathrm{char}(K) = 2$, are of the form:
$$ax(y^2+y+1) = by(x^2+x+1) \text{ with } abcd(a^2c-b^2d) \neq 0,$$
6) The generalized binary Huff curves (by Devigne and Joye [7]) over field K, $\mathrm{char}(K) = 2$, are of the form:
$$ax(y^2+fy+1) = by(x^2+fx+1) \text{ with } abf(a-b) \neq 0.$$

The main contribution of this paper is to prove the the new generalized Huff curves have all the good properties for arithmetics and pairing known for the particular Huff curves studied by Joye, Tibouchi and Vergnaud in [16] and by Wu and Feng in [11].

This paper is organized as follows:
In section1: First, we racall the main results of Joye, Tibouchi and Vergnaud in [16] and also those of Wu and Feng in [11].
In section2: We studie the arithmetic of the new generalized Huff curves
In section3: We prove that the method of Joye, Tibouchi and Vergnaud in [16] for computing pairing can be extending to our new generalized Huff curves.

For elliptic and hyperelliptic curves tools and cryptography background, we refer to [19], [20], [24], [6], [17], etc.

1 Basic properties of $ax(y^2-c) = by(x^2-d)$

In this section, we prove that the curve $\mathcal{H}^{(c,d)}_{(a,b)}$: $ax(y^2-c) = by(x^2-d)$ is an affine variety of dimension 1 (which is hence defined by a single irreducible polynomial over the algebraic closure $\overline{K}$ of K) and smooth (which means that there exists no singular points).

1.1 Affine smooth variety

Proposition 1. *Let K be a field with* $\mathrm{char}(K) \neq 2$ *and a, b, c, d be in K. Define the multivariate polynomial $H(x,y) = ax(y^2-c) = by(x^2-d)$ in $K[x,y]$. If $abcd(a^2c - b^2d \neq 0$, then $H(x,y)$ is irreducible in $\overline{K}[x,y]$ where $\overline{K}$ is the algebraic closure of K.*

Proof. Let $f(x)$, $g(x)$, $f'(x)$ and $g'(x)$ be in $\overline{K}[x]^*$ such that

$$H(x,y) = (f(x)y + g(x))(f'(x)y + g'(x)).$$

Then, by identification we have

$\alpha_1)$ $ff' = ax$
$\alpha_2)$ $fg' + f'g = -b(x^2-d)$
$\alpha_3)$ $gg' = -acx$

By equation (α_1) we can assume that $\deg(f') = 0 \Leftrightarrow f' \in \overline{K}$. Then using (α_2) and (α_3) we see that necessary $\deg(g') \neq 0$ hence (α_3) implies that $\deg(g') = 1$ and $\deg(g) = 0 \Leftrightarrow f' \in \overline{K}$. Now we can write $f = \frac{ax}{f'}$ and $g' = \frac{-acx}{g}$ thus $fg' = \frac{-a^2cx^2}{f'g}$.
Therefore by (α_2) we have, $fg' + f'g = \frac{-a^2cx^2}{f'g} + f'g = -bx^2 + bd$. Now by identification, we have $f'g = bd$ and thus $\frac{-a^2c}{bd} = -b \Leftrightarrow (a^2c - b^2d) = 0$ which contradicts the hypothesis.
We conclude that $H(x,y)$ is irreducible over $\overline{K}$ as desired.

Proposition 2. *Let K be a field* $\mathrm{char}(K) \neq 2$ *and a, b, c, d in K. The affine variety defined by*

$$\mathcal{H}^{(c,d)}_{(a,b)} : \; ax(y^2-c) = by(x^2-d) \quad \textit{with } abcd(a^2c - b^2d) \neq 0$$

is smooth.

Proof. Suppose that there exists $P(x,y)$ which verifies $H(x,y) = 0$, $\frac{dH(x,y)}{dy} = 0$ and $\frac{dH(x,y)}{dx} = 0$ where $H(x,y) = ax(y^2-c) - by(x^2-d)$. Therefore, we have

$\beta_1)$ $ax(y^2-c) = by(x^2-d)$
$\beta_2)$ $ay^2 - 2byx - ac = 0$
$\beta_3)$ $2axy - b(x^2-d) = 0$

Remark that $x = 0 \Leftrightarrow y = 0$ and $(0,0)$ is not a solution of the previous system. Multiplying (β_3) by y and using (β_1) yields that $ax(y^2+c) = 0$ thus $y^2 = -c$ and by (β_2), we have $ac + bxy = 0$.
Similarly, by symmetry, we have also: $bd + axy = 0$. Combining these last two equations we have $b^2d = a^2c$ which contradicts the hypothesis.

1.2 Projective closures

We denote by $[X : Y : Z]$ a point on the projective plan $\mathcal{P}^2(K)$, where $[X : Y : Z]$ is the equivalence class $[X : Y : Z] = \{(\lambda X, \lambda Y, \lambda Z), \lambda \in \bar{K}\}$.
If we homogenize the affine previous curve, on the projective plane $\mathcal{P}^2(K)$, we have the projective closure of $\mathcal{H}^{(c,d)}_{(a,b)}$:

$$\overline{\mathcal{H}}^{(c,d)}_{(a,b)} : \ aX(Y^2 - cZ^2) = bY(X^2 - dZ^2) \ \text{ with } \ abcd(a^2c - b^2d) \neq 0$$

The points at infinity are the points of $\overline{\mathcal{H}}^{(c,d)}_{(a,b)}$ which do not lie in $\mathcal{H}^{(c,d)}_{(a,b)}$, in other words the points at infinity are all points of the form $[X : Y : 0] \in \overline{\mathcal{H}}^{(c,d)}_{(a,b)}$. And $Z = 0$ yields that $aXY^2 = bYX^2$. hence we have three infinite points $[1 : 0 : 0]$, $[0 : 1 : 0]$ and $[a : b : 0]$. Moreover this three infite points are not singular as one can see it in the following.

1. To study the curve around $[1 : 0 : 0]$ or $[a : b : 0] = [1 : \frac{b}{a} : 0]$ we consider the affine curve defined by

   $$T(Y, Z) = a(Y^2 - cZ^2) - bY(1 - dZ^2) = 0.$$

   The partial derivatives

   $$(\textbf{Eq1}) \ \frac{dT}{dZ} = 2aY - b(1 - dZ^2) \text{ and } (\textbf{Eq2}) \ \frac{dT}{dY} = -2acZ + 2bdYZ$$

   both vanish at $(0, 0)$ if and only if $b = 0$ by (**Eq1**). Since $b \neq 0$, then the point $[1 : 0 : 0]$ is not singular.
   We see also that this both equations vanish at $(\frac{b}{a}, 0)$ if and only if $b = 0$ by (**Eq1**). Since $b \neq 0$, then the point $[a : b : 0]$ is not singular.
2. As above, by symmetry the point $[0 : 1 : 0]$ is not singular.

1.3 Inflexion points

Since general Huff curve is smooth, the inflection points of $\overline{\mathcal{H}}^{(c,d)}_{(a,b)}$ are the intersections points of $\overline{\mathcal{H}}^{(c,d)}_{(a,b)}$ and his Hessian $\text{Hessian}\big(\overline{\mathcal{H}}^{(c,d)}_{(a,b)}\big)$. Put $H(X, Y, Z) = aX(Y^2 - cZ^2) - bY(X^2 - dZ^2)$. We have

$$\text{Hessian}\big(\mathcal{H}^{(c,d)}_{(a,b)}\big) = \begin{vmatrix} \frac{dH}{dXdX} & \frac{dH}{dXdY} & \frac{dH}{dXdZ} \\ \frac{dH}{dYdX} & \frac{dH}{dYdY} & \frac{dH}{dYdZ} \\ \frac{dH}{dZdX} & \frac{dH}{dZdY} & \frac{dH}{dZdZ} \end{vmatrix} = 8 \begin{vmatrix} -bY & aY - bX & -acZ \\ aY - bX & aX & bdZ \\ -acZ & bdZ & -acX + bdY \end{vmatrix}.$$

Hence, it is clear that $[0 : 0 : 1]$ is an inflection point. If $Z = 0$ we have

$$(-acX + bdY)(-a^2Y^2 - b^2X^2 + abYX) = 0$$

and this equation is not verified by each of the two infinite points $[1 : 0 : 0]$ and $[0 : 1 : 0]$. Moreover the point $[a : b : 0]$ verifies the equation if and only if $(-a^2c + b^2d)(-2a^2b^2) = 0$, which is impossible.
We conclude that $[0 : 0 : 1]$ is an inflexion point and there infinite point which is an inflexion point. .

1.4 Birrational equivalence and Universality of the model

Here, we have the projective version of the birrational equivalence.

Proposition 3. *Let K be a field $charc(K) \neq 2$ and a, b, c, d in K. The affine projective variety defined by $\overline{\mathcal{H}}^{(c,d)}_{(a,b)}: aX(Y^2-cZ^2) = bY(X^2-dZ^2)$ with $abcd(a^2c-b^2d) \neq 0$ is birrationaly equivalent to the elliptic curve defined by $\overline{\mathcal{E}}^{(c,d)}_{(a,b)}: WV^2 = U(U+a^2cW)(U+b^2dW)$ with $abcd(a^2c-b^2d) \neq 0$ via the transformation:*
$\Psi : \mathbb{P}^2(K) \to \mathbb{P}^2(K) : [X:Y:Z] \mapsto [U:V:W]$ and
$\Psi^{-1} : \mathbb{P}^2(K) \to \mathbb{P}^2(K) : [U:V:W] \mapsto [X:Y:Z]$, with

$$\begin{cases} U = abcd(bX - aY) \\ V = abcd(b^2d - a^2c)Z \\ W = -acX + bdY \end{cases} \Leftrightarrow \begin{cases} X = bd(U + a^2cW) \\ Y = ac(U + b^2dW) \\ Z = V \end{cases}$$

Proof.
1) suppose that $WV^2 - U(Za - bU)(acU + bdZ) = 0$. We have the following,

$$\begin{aligned} & aX(Y^2 - cZ^2) - bY(X^2 - dZ^2) \\ &= abd(U+a^2cW)\left[a^2c^2(U + b^2dW)^2 - cV^2\right] - abc(U+b^2dW)\left[b^2d^2(U + a^2cW)^2 - dV^2\right] \\ &= abcd(b^2d-a^2c)WV^2 - abcd(U+b^2dW)(U+a^2cW)\left[a^2c(U + b^2dW)^2 - b^2d(U + a^2cW)^2\right] \\ &= abcd(b^2d - a^2c)\left[WV^2 - U(U + b^2dW)(U + a^2cW)\right] = 0 \end{aligned}$$

2) suppose that $aX(Y^2 - cZ^2) - bY(X^2 - dZ^2) = 0$. Put $\alpha = abcd$ and $\beta = abcd(b^2d - a^2c)$, we have the following:

$$\begin{aligned} & WV^2 - U(U + b^2dW)(U + a^2cW) \\ &= (-acX+bdY)\beta^2Z^2 - \alpha(bX-aY)\left[\alpha(bX - aY) + b^2d(-acX + bdY)\right]\left[\alpha(bX - aY) + a^2c(-acX + bdY)\right] \\ &= (-acX+bdY)\beta^2Z^2 - \alpha(bX-aY)\left[(\alpha b - b^2dac)X + (-\alpha b + b^3d^2)Y\right]\left[(\alpha b - a^3c^2)X + (-\alpha a + a^2bdc)Y\right] \\ &= (-acX+bdY)\left[abcd(b^2d - a^2c)\right]^2 Z^2 - abcd(bX-aY)\left[bd(b^2d - a^2c)Y\right]\left[ac(b^2d - a^2c)X\right] \\ &= \left[abcd(b^2d - a^2c)\right]^2\left[-acXZ^2 + bdYZ^2 - bX(XY) + aY(XY)\right] \\ &= \left[abcd(b^2d - a^2c)\right]^2\left[aX(Y^2 - cZ^2) - bY(X^2 - dZ^2)\right] \end{aligned}$$

We have the following theorem for the universality of this new model.

Theorem 1. *Let $\mathcal{H}^{(c,d)}_{(a,b)}: ax(y^2 - c) = by(x^2 - d)$ with $abcd(a^2c - b^2d) \neq 0$ be a Generalized Huff curve.*

1. *Any elliptic curve $(E;O)$ over a perfect field K of characteristic $\neq 2$ such that $E(K)$ contains a subgroup G isomorphic to $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ is birationally equivalent over K to a New Generalized Huff curve forme $\mathcal{H}^{(\frac{1}{a},d)}_{(a,-1)}$ with $ad(a-d) \neq 0$.*
2. *Any elliptic curve $(E;O)$ over a perfect field K of characteristic $\neq 2$ such that $E(K)$ contains a subgroup G isomorphic to $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ is birationally equivalent over K to a New Generalized Huff curve of the particular forme $\mathcal{H}^{(1,1)}_{(a,b)}$ with $ab(a^2 - b^2) \neq 0$.*

Proof. Follows from the theorems in [16], [11] and [12].

2 Arithmetic of the Generalized Huff Curves

2.1 Addition law

Group structure. The group law on NGHC is the same than classical Huff curves, but we recall the following for the shake of completeness.
- By the above birrational equivalence, we have $\Psi^{-1}([0:1:0]) = [0:0:1]$, and Ψ^{-1} is a line preserving then the group law $\left(\mathcal{H}_{(a,b)}^{(c,d)}, \oplus, \mathcal{O}\right)$ on a NGHC, use the chord-and-tangent rule [24] (with $\mathcal{O} = [0:0:1]$ as neutral element) as follows: for any line intersecting the cubic curve $\mathcal{H}_{(a,b)}^{(c,d)}$ at the three points P_1, P_2 and P_3 (counting multiplicities), we have $P_1 \oplus P_2 \oplus P_3 = \mathcal{O}$ and $P \oplus (\ominus P) = \mathcal{O}$ where $P = [X:Y:Z]$ and $\ominus P = [X:Y:-Z]$, therefore a point at infinity is its own inverse. Furthermore, the 3 infinite points are exactly the three primitive 2-torsion points of $\mathcal{H}_{(a,b)}^{(c,d)}$.
- If c and d are square, $(\pm\sqrt{c} : \pm\sqrt{d} : 1]$ are 4-torsion points.

Formulæ for addition law
Let $y = \alpha x + \beta$ denote the line (P_1P_2) passing through P_1 and P_2, where $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are in the curve $\mathcal{H}_{(a,b)}^{(c,d)}$. We define $P_1 + P_2 = P_3$ where $P_3 = (x_3, y_3)$ and $-P_3 = (-x_3, -y_3)$ is third intersection point between the line and the curve.
We have $ax[(y = \alpha x + \beta)^2 - c] - b(y = \alpha x + \beta)[x^2 - d] = 0$, thus

$$(a\alpha^2 - \alpha b)x^3 + (2a\alpha\beta - b\beta)x^2 + [a(\beta^2 - c) + \alpha bd]x - \beta db = 0.$$

Therefore

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

Hence we have

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

with $\alpha = \dfrac{y_2 - y_1}{x_2 - x_1}$ and $\beta = y_1 - \alpha x_1$.
After some computations, we have

$$x_3 = x_1 + x_2 + \frac{[y_1x_2 - x_1y_2][2a(y_2 - y_1) - b(x_2 - x_1)]}{(y_2 - y_1)[a(y_2 - y_1) - b(x_2 - x_1)]}.$$

Putting $A = y_1y_2(x_2 + x_1)[a(y_2 - y_1) - b(x_2 - x_1)]$, we have the following by calculations and curve equation

$$\begin{aligned}
A &= y_1y_2(x_2 + x_1)[a(y_2 - y_1) - b(x_2 - x_1)] \\
&= a(x_1y_1y_2^2 - x_2y_2y_1^2) + a(x_2y_1y_2^2 - x_1y_2y_1^2) - by_1y_2x_2^2 + by_1y_2x_1^2 \\
&= a(x_1y_1y_2^2 - x_2y_2y_1^2) + a(x_2y_1y_2^2 - x_1y_2y_1^2) - y_1by_2[(x_2^2 - d) + d] + y_1by_2[(x_1^2 - d) + d] \\
&= a(x_1y_1y_2^2 - x_2y_2y_1^2) + a(x_2y_1y_2^2 - x_1y_2y_1^2) - y_1ax_2(y_2^2 - c) + y_2ax_1(y_1^2 - c) \\
&= a(x_1y_1y_2^2 - x_2y_2y_1^2) + acy_1x_2) - acy_2x_1 \\
&= a(x_1y_2 - x_2y_1)(y_1y_2 - c)
\end{aligned}$$

Putting this value in x_3 yields that

$$x_3 = x_1 + x_2 - \frac{[2a(y_2 - y_1) - b(x_2 - x_1)](x_1 + x_2)y_1y_2}{(y_2 - y_1)a(y_1y_2 - c)}.$$

Hence

$$\begin{aligned}
x_3 &= x_1 + x_2 - \frac{[2a(y_2 - y_1) - b(x_2 - x_1)](x_1 + x_2)y_1y_2}{(y_2 - y_1)a(y_1y_2 - c)} \\
x_3 &= x_1 + x_2 - \frac{[a(y_2 - y_1)](x_1 + x_2)y_1y_2 + [a(y_2 - y_1) - b(x_2 - x_1)](x_1 + x_2)y_1y_2}{(y_2 - y_1)a(y_1y_2 - c)} \\
&= x_1 + x_2 - \frac{(x_2 + x_1)y_1y_2}{(y_2y_1 - c)} + \frac{y_1x_2 - x_1y_2}{(y_2 - y_1)} \\
&= \frac{x_2y_2 - x_1y_1}{(y_2 - y_1)} - \frac{(x_2 + x_1)y_1y_2}{(y_2y_1 - c)}
\end{aligned}$$

Put $B = b(x_2y_2 - x_1y_1)(x_2x_1 + d)$, we have the following by calculations and curve equation:

$$\begin{aligned}
B &= y_1y_2(x_2 + x_1)[a(y_2 - y_1) - b(x_2 - x_1)] \\
&= bx_1y_2x_2^2 - bx_2y_1x_1^2 + bdx_2y_2 - bdx_1y_1 \\
&= bx_1y_2[(x_2^2 - d) + d] - bx_2y_1[(x_1^2 - d) + d] + bdx_2y_2 - bdx_1y_1 \\
&= bx_1y_2[(x_2^2 - d) + d] - bx_2y_1[(x_1^2 - d) + d] + bdx_2y_2 - bdx_1y_1 \\
&= ax_2x_1(y_2 - y_1)(y_2 + y_1) + bd(x_2 + x_1)(y_2 - y_1) \\
&= (y_2 - y_1)[ax_2x_1(y_2 + y_1) + bd(x_2 + x_1)]
\end{aligned}$$

Putting this value in

$$x_3 = \frac{x_2y_2 - x_1y_1}{(y_2 - y_1)} - \frac{(x_2 + x_1)y_1y_2}{(y_2y_1 - c)}$$

yields that (after simplification)

$$\begin{aligned}
x_3 &= \frac{(x_2y_2 - x_1y_1)(x_1x_2 + d)b}{(y_2 - y_1)(x_1x_2 + d)b} - \frac{(x_2 + x_1)y_1y_2}{(y_2y_1 - c)} \\
x_3 &= \frac{ax_2x_1(y_2 + y_1) + bd(x_2 + x_1)}{(x_1x_2 + d)b} - \frac{(x_2 + x_1)y_1y_2}{(y_2y_1 - c)}
\end{aligned}$$

$$x_3 = \frac{ax_2x_1(y_2+y_1)(y_2y_1-c)+bd(x_2+x_1)(y_2y_1-c)-(x_2+x_1)y_1y_2(x_1x_2+d)b}{(x_1x_2+d)b(y_2y_1-c)}$$

Put $C = ax_2x_1(y_2+y_1)(y_2y_1-c)$, we have the following by calculations and curve equation:

$$\begin{aligned} C &= ax_1x_2y_1y_2^2 + ax_1x_2y_2y_1^2 - acx_1x_2y_2 - acx_1x_2y_1 \\ &= ax_1y_1x_2[(y_2^2-c)+c] + ax_2y_2x_1[(y_1^2-c)+c] - acx_1x_2y_2 - acx_1x_2y_1 \\ &= bx_1y_1y_2(x_2^2-d) + bx_2y_2y_1(x_1^2-d) \\ &= by_1y_2(x_2+x_1)(x_1x_2-d) \end{aligned}$$

Putting this value in the numerator of x_3, ie in

$$N_{x_3} = ax_2x_1(y_2+y_1)(y_2y_1-c)+bd(x_2+x_1)(y_2y_1-c)-(x_2+x_1)y_1y_2(x_1x_2+d)b,$$

yields that $N_{x_3} = (x_1+x_2)(-dy_2y_2-dc)$ which implies that

$$x_3 = \frac{(x_1+x_2)(y_1y_2+c)(-d)}{(x_1x_2+d)(y_1y_2-c)}.$$

We conclude that

$$x_3 = \frac{d(x_1+x_2)(c+y_1y_2)}{(d+x_1x_2)(c-y_1y_2)}$$

And by symmetry, we have $y_3 = \dfrac{c(y_1+y_2)(d+x_1x_2)}{(c+y_1y_2)(d-x_1x_2)}$

Adding points. If $x_1x_2 \neq \pm c$ and $y_1y_2 \neq \pm d$, we can always add, and we have the following formulae:

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

Doubling points. If $x_1^2 \neq \pm c$ and $y_1^2 \neq \pm d$ and in particular if c and d are not square in K, we can always double, and we have the following formulae:

$$x_3 = \frac{2dx_1(c+y_1^2)}{(d+x_1^2)(c-y_1^2)} \text{ and } y_3 = \frac{2cy_1(d+x_1^2)}{(c+y_1^2)(d-x_1^2)}$$

2.2 Efficiency

Adding rational points. Recall that in affine coordinates we have (whenever defined) $(x_1,y_1)+(x_2,y_2)=(x_3,y_3)$ with

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

In projective coordinates, we have: $[X_1:Y_1:Z_1]+[X_2:Y_2:Z_2]=[X_3:Y_3:Z_3]$ with

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

Let **m**, **s** and **c** denote respectively multiplication, squaring and constant multiplication, then direct counting shows that one can perform addition in projective coordinates with $11\mathbf{m} + 5\mathbf{s} + 4\mathbf{c}$.
But it is possible to reduce the number of multiplications as follows:
let $M_1 = X_1X_2$, $M_2 = Y_1Y_2$, $M_3 = Z_1Z_2$, $C_1 = cM_3$ and $C_2 = dM_3$, then

1. $M_4 = (X_1 + Z_1)(X_2 + Z_2) - M_1 - M_3$, $\quad M_5 = (Y_1 + Z_1)(Y_2 + Z_2) - M_2 - M_3$
2. $M_6 = (C_1 + M_2)(C_2 - M_1)$, $\quad M_7 = (C_2 + M_1)(C_1 - M_2)$,
3. $M_8 = M_4(C_1 + M_2)$, $\quad M_9 = M_5(C_2 + M_1)$
4. thus $X_3 = dM_8M_6$, $\quad Y_3 = cM_9M_7$ and $Z_3 = M_6M_7$

Hence, we have $12\mathbf{m} + 4\mathbf{c}$ instead of $11\mathbf{m} + 5\mathbf{s} + 4\mathbf{c}$.

□

Doubling rational points. In the case of doubling, we have the following:
Let $P_1 = [X_1 : Y_1 : Z_1]$, then $2P = [X_3 : Y_3 : Z_3]$ with

$$\begin{cases} X_3 = 2dX_1(cZ_1^2 + Y_1^2)^2(dZ_1^2 - X_1^2), \\ Y_3 = 2cY_1(dZ_1^2 + X_1^2)^2(cZ_1^2 - Y_1^2), \\ Z_3 = (cZ_1^2 + Y_1^2)(cZ_1^2 - Y_1^2)(dZ_1^2 + X_1^2)(dZ_1^2 - X_1^2). \end{cases}$$

If **m**, **s** and **c** are respectively the costs of multiplication, squaring and multiplication by a constant, then the doubling of a projective point can be performed in $7\mathbf{m} + 5\mathbf{s} + 4\mathbf{c}$.

2.3 Completeness of the addition law

Theorem 2. *Let K be a field of characteristic $\neq 2$. Let $P_1 = [X_1 : Y_1 : Z_1]$ and $P_1 = [X_2 : Y_2 : Z_2]$ be two points on a the New Generalized Huff curve over K. Then the addition formula $P_1 \oplus P_2 = P_3$ given by*

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

where $P_3 = [X_3 : Y_3 : Z_3]$, is valid provided that $X_1X_2 \neq dZ_1Z_2$ and $Y_1Y_2 \neq cZ_1Z_2$.

Proof. Similar to those of [16], Theorem 1. If P_1 and P_2 are finite, we can write $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. The above affine formula for (x_3, y_3) as given by the above equations, is defined whenever $x_1x_2 \neq \pm d$ and $y_1y_2 \neq \pm c$. This translates into $X_1X_2 \neq dZ_1Z_2$ and $Y_1Y_2 \neq cZ_1Z_2$ for projective coordinates.
The infinite points are $[1 : 0 : 0], [0 : 1 : 0]$ and $[a : b : 0]$. If $P_1, P_2 \in \{[1 : 0 : 0], [0 : 1 : 0]\}$, then the conditions $X_1X_2 \neq dZ_1Z_2$ and $Y_1Y_2 \neq cZ_1Z_2$ are not satisfied. If $P_2 = [a : b : 0]\}$, then the condition becomes $X_1 \neq 0$ and $Y_1 \neq 0$, which corresponds to $P_1 \notin \{[1 : 0 : 0], [0 : 1 : 0]\}$

Proposition 4. *Let E be a New Generalized Huff curve over a field K of odd characteristic. Let also $P \in E(K)$ be a point of odd order. Then the addition law in the subgroup generated by P is complete.*

Proof. Similar to those of [16], Corollary 1. All points in the subgroup generated by P (denoted by $\langle P \rangle$) 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 $P_1 = (x_1; y_1)$; $P_2 = (x_2; y_2) \in \langle P \rangle$, we have $x_1 x_2 \neq \pm d$ and $y_1 y_2 \neq \pm c$. Note that $x_1^2; x_2^2 \neq d$ and $y_1^2; y_2^2 \neq c$ since this corresponds to points of order 4 (which are not in $\langle P \rangle$). Suppose that $x_1 x_2 = \pm d$. Then $ax_1(y_1^2 - c) = by_1(x_1^2 - d) \Longrightarrow a\frac{1}{x_1}(y_1^2 - c) = by_1(1 - \frac{d}{x_1^2}) \Longrightarrow \frac{\pm a x_2}{d}(y_1^2 - c) = by_1(1 - \frac{x_2^2}{d}) \Longrightarrow \mp a x_2(y_1^2 - c) = by_1(x_2^2 - d)$. Since $ax_2(y_2^2 - c) = by_2(x_2^2 - d)$ we have $\mp\frac{(y_2^2 - c)}{(y_1^2 - c)} = \frac{y_2}{y_1} \Longrightarrow \mp y_1(y_2^2 - c) = y_2(y_1^2 - c)$, thus $(y_2 \pm y_1)(y_2 y_1 \mp c) = 0$. Therefore, if $x_1 x_2 = \pm d$, we have $(x_2, y_2) \in \left\{ (\frac{d}{x_1}, -y_1); (\frac{d}{x_1}, \frac{c}{y_1}); (\frac{-d}{x_1}, y_1); (\frac{-d}{x_1}, \frac{-c}{y_1}) \right\}$. 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, which is a contradiction. Similarly, it can be verified that the case $y_1 y_2 \neq \pm c$ leads also to a contradiction.

3 Parings in the New Generalized Huff curves

3.1 The Tate Pairing

Definition 1. *Let G_1 and G_2 be finite abelian groups written additively, and let G_3 be a multiplicatively written finite group. A cryptographic pairing is a map*

$$e : G_1 \times G_2 \longrightarrow G_3$$

that satisfies the following properties:

1. *it is non-degenerate, ie for all $0 \neq P \in G_1$, there is a $Q \in G_2$ with $e(P, Q) \neq 1$, and for all $0 \neq Q \in G_2$, there is a $P \in G_1$ with $e(P, Q) \neq 1$*
2. *it is bilinear, ie for all $P_1, P_2 \in G_1$ and for all $Q_1, Q_2 \in G_2$ we have*

$$e(P_1 + P_2, Q_1) = e(P_1, Q_1)e(P_2, Q_1)$$

$$e(P_1, Q_1 + Q_2) = e(P_1, Q_1)e(P_1, Q_2)$$

3. *it is efficiently computable*

An important property that is used in most applications and that follows immediately from the bilinearity is $e([a]P, [b]Q) = e(P, Q)^{ab} = e([b]P, [a]Q)$ for all $a, b \in \mathbb{Z}$ and for all $(P, Q) \in G_1 \times G_2$.

The Tate pairing can be defined on an ordinary abelian variety. It induces a pairing on the r-torsion subgroup of the abelian variety for a prime order r.
Let $\mathcal{C}$ be a hyperelliptic curve of genus g defined over a finite field $\mathbb{F}_q$ of characteristic p. Let $J_{\mathcal{C}}$ be the jacobian variety of $\mathcal{C}$. Elements of $J_{\mathcal{C}}$ can be considered as divisor classes represented by a divisor of degree 0. Let $n = \#J_{\mathcal{C}}(\mathbb{F}_q)$ and $r > 5$ be a prime different from p and $r|n$.

Definition 2. *The smallest integer k with $r|(q^k-1)$ is called the embedding degree of $\mathcal{C}$ with respect to r*

Remark 1. If k is the smallest integer with $r|(q^k-1)$, the order of q modulo r is k. Furthermore, the smallest field extension of $\mathbb{F}_q$ that contains the group μ_r of all r-th roots of unity is $\mathbb{F}_{q^k}$.

Definition 3. *Let $\mathcal{C}$ be a hyperelliptic curve of genus g over the finite field $\mathbb{F}_q$ of characteristic p and let $r \neq p$ be a prime dividing $\#J_{\mathcal{C}}(\mathbb{F}_q)$. Let k be the embedding degree of $\mathcal{C}$ with respect to r. The Tate pairing is a map*

$$T_r : J_{\mathcal{C}}(\mathbb{F}_{q^k})[r] \times J_{\mathcal{C}}(\mathbb{F}_{q^k})/[r]J_{\mathcal{C}}(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$$

defined as follows.

Let $P \in J_{\mathcal{C}}(\mathbb{F}_{q^k})[r]$ be an $\mathbb{F}_{q^k}$-rational divisor class of order dividing r represented by the divisor D_p, and let $Q \in J_{\mathcal{C}}(\mathbb{F}_{q^k})$ be an an $\mathbb{F}_{q^k}$-rational divisor class represented by a divisor D_Q such that its support is disjoint from the support of D_P. Let $f_{r,P} \in \overline{\mathbb{F}_{q^k}}(C)$ be a function on $\mathcal{C}$ with $div(f_{r,P}) = rD_P$. Then,

$$T_r(P, Q + [r]J_{\mathcal{C}}(\mathbb{F}_{q^k})) = f_{r,P}(D_Q)(\mathbb{F}_{q^k}^*)^r$$

The evaluation of the function $f_{r,P}$ at a divisor $D = \sum_{R \in \mathcal{C}} n_R(R)$ is given as

$$f_{r,P}(D) = \prod_{R \in C} f_{r,P}(R)^{n_R}$$

Proposition 5. *The Tate pairing is well defined, bilinear, non-degenerate and can be computed in $\mathcal{O}(log_2(r))$ operations in $\mathbb{F}_{q^k}$.*

Lemma 1. *Let G be a finite abelian group written additively, and let r be a prime dividing $\#G$. Let $G[r]$ be the subgroup of all points of order dividing r and rG be the set of all r-fold sums of elements of G. If there is no element of order r^2 in G, then*

$$G[r] \cong G/rG$$

Corollary 1. *If there are no points of order r^2 in $J_{\mathcal{C}}(\mathbb{F}_{q^k})$, we have*

$$J_{\mathcal{C}}(\mathbb{F}_{q^k})[r] \cong J_{\mathcal{C}}(\mathbb{F}_{q^k})/[r]J_{\mathcal{C}}(\mathbb{F}_{q^k})$$

Remark 2. Since $r|\#J_{\mathcal{C}}(\mathbb{F}_q)$, there are r-torsion points in $J_{\mathcal{C}}(\mathbb{F}_q)[r]$ and we may restrict the first argument to be taken from this set. Thus, we can also define the Tate pairing as a map

$$T_r : J_{\mathcal{C}}(\mathbb{F}_q)[r] \times J_{\mathcal{C}}(\mathbb{F}_{q^k})/[r]J_{\mathcal{C}}(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$$

From now, we assume that $J_{\mathcal{C}}(\mathbb{F}_{q^k})$ does not contain any point of order r^2. In this case the Tate pairing can be given as

$$T_r : J_{\mathcal{C}}(\mathbb{F}_q)[r] \times J_{\mathcal{C}}(\mathbb{F}_{q^k})[r] \longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$$

Values of the Tate pairing are classes in $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$. By applying the multiplicative version of the lemma, we see that $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r \cong \mu_r$, the subgroup of all rth roots of unity in $\mathbb{F}_{q^k}^*$. The isomorphism is made explicit by computing

$$\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r \longrightarrow \mu_r, \quad a(\mathbb{F}_{q^k}^*)^r \longrightarrow a^{(q^k-1)/r}$$

This map is called the final exponentiation.

Definition 4. *The reduced Tate pairing is the map*

$$\begin{aligned} e_r : J_{\mathcal{C}}(\mathbb{F}_q)[r] \times J_{\mathcal{C}}(\mathbb{F}_{q^k})[r] &\longrightarrow \mu_r \subseteq \mathbb{F}_{q^k} \\ (P,Q) &\longmapsto Tr(P,Q)^{(q^k-1)/r} = f_{r,P}(D_Q)^{(q^k-1)/r} \end{aligned}$$

induced by the Tate pairing.

3.2 Pairing computation on elliptic curves in Weierstrass form

.

Let E be an elliptic curve over $\mathbb{F}_q$ of characteristic $p > 3$ given by a short Weierstrass equation

$$E : y^2 = x^3 + ax + b \quad a, b \in \mathbb{F}_q.$$

Let $r \neq p$ be a prime such that $r|n = \#E(\mathbb{F}_q)$ and let $k > 1$ be the embedding degree of E with respect to r.

Theorem 3. *Let* $D = \sum_{P \in E} n_P(P) \in Div(E)$. *Then* D *is a principal divisor if and only if* $deg(D) = 0$ *and* $\sum_{P \in E} [n_P](P) = 0$, *where the latter sum describes the addition on* E.

Reduced Tate pairing

$$\begin{aligned} e_r : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})[r] &\longrightarrow \mu_r \subseteq \mathbb{F}_{q^k} \\ (P,Q) &\longmapsto f_{r,P}(D_Q)^{(q^k-1)/r} \end{aligned}$$

When computing $f_{r,P}(Q)$, ie when rD_P is supposed to be the divisor of the function $f_{r,P}$, we can choose $D_P = (P) - (O)$. The divisor $D_Q \sim (Q) - (O)$ needs to have a support disjoint from $\{O, P\}$. To achieve that, one may choose a suitable point $S \in E(\mathbb{F}_{q^k})$ and represent D_Q as $(Q + S) - S$.
We need to compute $f_{r,P}$ having divisor $div(f_{r,P}) = r(P) - r(O)$. Note that **Theorem 1** shows that for $m \in \mathbb{Z}$, the divisor $m(P) - ([m]P) - (m-1)(O)$ is principal, such that there exists a function $f_{m,P} \in \overline{\mathbb{F}_q}(E)$ with $div(f_{m,P}) = m(P) - ([m]P) - (m-1)(O)$. Since P is a r-torsion point, we see that $div(f_{r,P}) = r(P) - r(O)$, and $f_{r,P}$ is a function we are looking for.

Definition 5. *Given $m \in \mathbb{Z}$ and $P \in E(\mathbb{F}_{q^k})[r]$, a function $f_{m,P} \in \overline{\mathbb{F}_{q^k}}(E)$ with divisor $div(f_{m,P}) = m(P) - ([m]P) - (m-1)(O)$ is called a Miller function*

Lemma 2. *Let $P_1, P_2 \in E$. Let l_{P_1,P_2} be the homogeneous polynomial defining the line through P_1 and P_2, being the tangent to the curve if $P_1 = P_2$. The function $L_{P_1,P_2} = l_{P_1,P_2}(X,Y,Z)/Z$ has the divisor*

$$div(L_{P_1,P_2}) = (P_1) + (P_2) + (-(P_1+P_2)) - 3(O).$$

Lemma 3. *Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $Q = (x_Q, y_Q) \in E$. For $P_1 \neq -P_2$ define*

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } P_1 \neq P_2, \\ (3x_1^2 + a)/(2y_1) & \text{if } P_1 = P_2. \end{cases}$$

Then, the dehomogenization $(l_{P_1,P_2})_*$ of l_{P_1,P_2} evaluated at Q is given by

$$(l_{P_1,P_2})_*(Q) = \lambda(x_Q - x_1) + (y_1 - y_Q).$$

If $P_1 = -P_2$, then $(l_{P_1,P_2})_*(Q) = x_Q - x_1$.

Lemma 4. *Let $P_1, P_2 \in E$. The function $g_{P_1,P_2} := L_{P_1,P_2}/L_{P_1+P_2,-(P_1+P_2)}$ has the divisor*

$$div(g_{P_1,P_2}) = (P_1) + (P_2) - (P_1+P_2) - (O).$$

The function g can be used to compute the Miller function recursively as shown in the next lemma.

Lemma 5. *The Miller function $f_{r,P}$ can be chosen such that $f_{1,P} = 1$ and such that for $m_1, m_2 \in \mathbb{Z}$, it holds*

$$f_{m_1+m_2,P} = f_{m_1,P} f_{m_2,P} g_{[m_1]P,[m_2]P},$$

$$f_{m_1 m_2,P} = f_{m_1,P}^{m_2} f_{m_2,[m_1]P} = f_{m_2,P}^{m_1} f_{m_1,[m_2]P}$$

Remark 3. Special cases from the previous lemma
Let $m \in \mathbb{Z}$, then

1. $f_{m+1,P} = f_{m,P} g_{[m]P,P}$,
2. $f_{2m,P} = f_{m,P}^2 g_{[m]P,[m]P}$,
3. $f_{-m,P} = (f_{m,P} g_{[m]P}, -[m]P)^{-1}$.

Note that $f_{0,P} = 1$ for all $P \in E$ and $g_{P_1,P_2} = 1$ if P_1 or P_2 equals the point at infinity O. These formulas show that any function $f_{m,P}$ can be computed recursively as a product line functions. The functions are defined over the field of definition of P.

Lemma 6. *Let $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})[r]$, $\notin E(\mathbb{F}_q)$, then the reduced Tate pairing can be computed as $e_r(P,Q) = f_{r,P}(Q)^{(q^k-1)/r}$.*

The following algorithm, well known as the Miller's algorithm, can be used to compute $f_{r,P}(Q)$ for $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})[r]$ and $r = (r_l, r_{l-1}, \ldots, r_0)_2$ up to irrelevant factors lying a proper subfield of $\mathbb{F}_{q^k}$. Since $k > 1$, these factors are mapped to 1 by the final exponentiation.

Algorithm 1 Miller's Algorithm

1: $R \leftarrow P$, $f \leftarrow 1$
2: **for** $(i = l - 1; i \geq 0; i - -)$ **do**
3: $f \leftarrow f^2.g_{R,R}(Q)$
4: $R \leftarrow 2R$
5: **if** $(r_i = 1)$ **then**
6: $f \leftarrow f.g_{R,P}(Q)$
7: $R \leftarrow R + P$
8: **end if**
9: **end for**
10: **return** $f^{(q^k-1)/r}$

3.3 Pairing computation in generalized Huff curves

Generalized Huff curves are represented as plane cubics. This makes Miller's algorithm directly applicable to the computation of pairings over generalized Huff curves.

As above, for generalized Huff curve, the following lemma will be useful to compute the equation line used in Miller algorithm.

Lemma 7. *Let* $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $Q = (x_Q, y_Q) \in \overline{\mathcal{H}}^{(c,d)}_{(a,b)}$. *For* $P_1 \neq -P_2$ *define*

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } P_1 \neq P_2, \\ \dfrac{ay_1^2 - 2bx_1y_1 - ac}{bx_1^2 - 2bx_1y_1 - bd} & \text{if } P_1 = P_2. \end{cases}$$

where λ *is the* (x, y)*-slope of the line through* $P_1 = (x_1, y_1)$ *and* $P_2 = (x_2, y_2)$.

Proof: obvious!

□

It is common to represent the point $Q \in E(\mathbb{F}_{q^k}) \backslash E(\mathbb{F}_q)$ in affine coordinates since in the Miller's algorithm the function is always evaluated at the same point Q. Let's choose the coordinates of Q as $Q = (y, z) = (1 : y : z)$. Suppose the embedding degree k is even, then Q can be choosen of the form $Q = (y_Q, z_Q\alpha)$, with $y_Q, z_Q \in \mathbb{F}_{q^{k/2}}$, $\mathbb{F}_{q^k} = \mathbb{F}_{q^{k/2}}(\alpha)$ where α is any quadratic non-residue in $\mathbb{F}_{q^{k/2}}$.
Let $P, R \in E(\mathbb{F}_q)$ and let $l_{R,P}$ denote the rational function vanishing on the line through P and R. We have

$$l_{R,P}(Q) = \frac{(zX_p - Z_p) - \lambda(yX_p - Y_P)}{X_P}$$

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

$$div(l_{R,P}) = R + P + T - (1 : 0 : 0) - (0 : 1 : 0) - (a : b : 0)$$

where T is the third point of intersection of the line through P and R with the curve. If U is the neutral element of the group law $\oplus$, the line function can be

written as

$$g_{R,P} = \frac{l_{R,P}}{l_{R\oplus P,U}}$$

Let $U = O = (0 : 0 : 1)$ be the neutral element. Then, for any $Q = (y_Q, z_Q\alpha)$, we have

$$l_{R\oplus P,O} = y_Q - \frac{Y_{R\oplus P}}{X_{R\oplus P}} \in \mathbb{F}_{q^{k/2}}$$

Since this quantity lies on 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. Similary, divisions by X_P can be omitted, and denominators int the expression of λ can be cancelled. In other words, if $\lambda = \frac{A}{B}$, the line function can be computed as

$$g_{R,P}(Q) = (z_Q\alpha.X_p - Z_p)B - (yX_p - Y_P)A$$

We are now able to give precise fromulæfor the addition and the doubling steps in the Miller loop.

Addition step. In the addition step, the (y, z)-slope of the line through $P = (X_P : Y_P : Z_P)$ and $R = (X_R : Y_R : Z_R)$ est is given by

$$\lambda = \frac{Z_R X_P - Z_P X_R}{Y_R X_P - Y_P X_R}.$$

Thus, the line function is of the form

$$g_{R,P}(Q) = (z_Q\alpha.X_P - Z_P)(Y_R X_P - Y_P X_R) - (y_Q.X_P - Y_P)(Z_R X_P - Z_P X_R).$$

The quantities depending on P and Q, ie $y'_Q = y_Q.X_P - Y_P$ and $z'_Q = z_Q\alpha.X_P$ can be precomputed since the points P and Q ramain constant during the execution of the for loop. Hence, each addition step in the Miller's algorithm requires the computation of $R \oplus P$ (une addition sur $E(\mathbb{F}_q)$), the evaluation of the function $g_{R,P}(Q)$, and the computation of $f.g_{R,P}(Q)$.
The operation $R \oplus P$ can be performed in $12\mathbf{m} + 4\mathbf{c}$ including all intermediate results $m_1, m_2, \ldots m_9$. Compute also $m_{10} = (X_R + Y_R)(X_P - Y_P)$ and $m_{11} = (X_P + Z_P)(Z_R - X_R)$. Then,

$$g_{R,P}(Q) = (z'_Q - Z_P)(m_{10} - m_1 + m_2) - y'_Q(m_{11} + m_1 - m_3),$$

where the firsrt term requires $(\frac{k}{2} + 1)\mathbf{m}$, and the second $\frac{k}{2}\mathbf{m}$. With the final multiplication in $\mathbb{F}_{q^k}$, the total cost of the addition is $1\mathbf{M} + (k + 15)\mathbf{m} + 4\mathbf{c}$, where $\mathbf{M}$ is the cost of a multiplication in $\mathbb{F}_q^k$.

Doubling step. When doubling a point $R = (X_R : Y_R : Z_R)$, the (y, z)-slope of the tangent line at R is given by

$$\lambda = \frac{aZ_R^2 - 2bY_R Z_R - acX_R^2}{bY_R^2 - 2aY_R Z_R - bdX_R^2} = \frac{A}{B}.$$

Therefore,

$$g_{R,R}(Q) = z_Q\alpha.X_RB - Z_RB - y_Q.X_RA + Y_RA.$$

In Miller's algorithm, we need to compute the point $2R$. This computation can be performed in $7\mathbf{m}+5\mathbf{s}$. The quotients A and B can be evaluated in $1\mathbf{m}$, namely Y_RZ_R since the other squares were computed when doubling the point R. The function $g_{R,R}$ can be evaluated in $4\mathbf{m}$ (X_RB, Z_RB, X_RA and Y_RA), $\frac{k}{2}\mathbf{m}$ for $z_Q\alpha.X_RB$ and $\frac{k}{2}\mathbf{m}$ for $y_Q.X_RA$. Then, the full doubling can be performed in $1\mathbf{M} + 1\mathbf{S} + (k + 12)\mathbf{m} + 5\mathbf{s} + 6\mathbf{c}$ by keeping in count the multiplication, the suqaring and the multiplication by constants.

Conclusion

We successfully introduce a new generalization of existing Huff models of elliptic curves. We show that the arithmetic in the new generalized Huff curves is as fast as in the previous models. The addition formulæ on this curve is complete when considered in a subgroup generated by a finite point and is independant from the two of the four parameters of the curve. We also prove that the pairing computation on the new generalized Huff curves extends also those done by Joye, Tibouchi and Vergnaud.

References

1. Daniel J. Bernstein, Peter Birkner, Tanja Lange, Christiane Peters, *Optimizing double-base elliptic-curve single-scalar multiplication*, in Indocrypt 2007 [23] (2007), 167-182. URL: http://cr.yp.to/papers.html.
2. Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, Christiane Peters, *Twisted Edwards Curves,* in Africacrypt [25] (2008), 389-405. URL: http:// eprint.iacr.org/2008/013.
3. Daniel J. Bernstein, Tanja Lange, *Explicit-formulas* database (2007). URL: http:// hyperelliptic.org/EFD.
4. Daniel J. Bernstein, Tanja Lange, *Faster addition and doubling on elliptic curves*, in Asiacrypt 2007 [16] (2007), 29-50. URL: http://cr.yp.to/papers. html.
5. Daniel J. Bernstein, Tanja Lange, *Inverted Edwards coordinates*, in AAECC 2007 [9] (2007), 20-27. URL: http://cr.yp.to/papers.html.
6. Cohen, H., Frey, G. (eds.), *Handbook of elliptic and hyperelliptic curve cryptography*, CRC Press, 2005. ISBN 1-58488-518-1. MR 2007:14020. See [9], [25].
7. J Devigne and M. Joye *Binary Huff Curves* A. Kiayias, Ed., Topics in Cryptology .. CT-RSA 2011, vol. 6558 of Lecture Notes in Computer Science, pp. 340-355, Springer, 2011.
8. Diao, O. Camara, M. Sow, D. Sow, D. *Introduction on Generalized Edwards Form Hyperelliptic curves*, preprint
9. Doche, C., Lange, T., Arithmetic of elliptic curves, in [7] (2005), 267-302. MR 2162729.
10. Edwards, H.M., *A normal form for elliptic curves*, Bulletin of the American Mathematical Society 44 (2007), 393-422. URL: http://www.ams.org/bull/ 2007-44-03/S0273-0979-07-01153-6/home.html.

11. H. Wu, R. Feng *Elliptic curves in Huff's model* eprint.iacr.org/2010/390.pdf
12. G. Fung, H. Stroher, H. Williams and H. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over pure cubic fields*, Journal of Number Theory, Volume 36, Issue 1, September 1990, Pages 12-45
13. G. B. Huff. *Diophantine problems in geometry and elliptic ternary forms.* Duke Math. J., 15:443-453, 1948.
14. Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, Ed Dawson, *Twisted Edwards curves revisited,* in Asiacrypt 2008 [21] (2008). URL: http://eprint.iacr.org/2008/522
15. Sorina Ionica and Antoine Joux *Another Approach to Pairing Computation in Edwards Coordinates* Lecture notes in computer sciences Volume 5365/2008, Book Progress in Cryptology - INDOCRYPT 2008, pge 400-413
16. M. Joye, M. Tibouchi, and D. Vergnaud *Huff's Model for Elliptic Curves* 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
17. N. Koblitz. *Elliptic curve cryptosystems.* Math. Comp., 48:203-209, 1987.
18. N. Koblitz *Guide to Elliptic Curve Cryptography* Springer Verlag,(2004)
19. A.J. Menezes. *Elliptic curve public key cryptosystems.* Kluwer Academic Publishers, 1993
20. A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone. *Handbookof Applied Cryptography.* CRC Press, 1996.
21. V. S. Miller. *The Weil pairing and its efficient implementation.* J. Cryptology, 17(1), pages 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. 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.
24. J. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics 106, 1986 (THE, introduction to elliptic curves)