EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 10, No. 2, 2017, 363-391
ISSN 1307-5543 – www.ejpam.com
Published by New York Business Global

On Indifferentiable Deterministic Hashing into Elliptic Curves

Nafissatou Diarra[1], Djiby Sow[1,*], Ahmed Youssef Ould Cheikh Khlil[1]

[1] *Laboratoire d'Algèbre, de Cryptographie, de Géométrie Algébrique et Aplications (LACGAA, Cheikh Anta Diop University, Dakar, Senegal*

Abstract. In this paper, we give new deterministic encodings based on Elligator's model, for some families of elliptic curves. These encodings are *almost*-injective and easily invertible. This allows to make points in the image set of the encoding indistinguishable from uniform string of bits, which is useful for applications in censorship circumvention. Following the idea of Farashahi *et al.*, we show that our encodings are well-distributed. And thus they give rise to hash functions constructions indifferentiable from random oracles.

Key Words and Phrases: deterministic encodings, elliptic curves, random oracle, indifferentiable hashing

1. Introduction

In Elliptic Curve Cryptography, many protocols [18] and encryption schemes (like the the identity based-encryption of Boneh and Franklin [2]) need to hash into the group of points of an elliptic curve. The main idea is the following: the image of a message (a random string) m by the hash function F is $F(m) = f(h(m))$, where h is a classical hash function and f is an encoding function that maps a point of $\mathbb{F}_q$ to an element of the elliptic curve. As discussed by Brier *et al.* in [6], the construction $H(m) = f(h(m))$, where f is a constant-time encoding and h is a classical hash function modeled as a random oracle, can not replace a random oracle to the group of points of the elliptic curve (excepted for some special encodings, such as Boneh and Franklin's one [2]). In 2013, Farashahi *et al.* [14] defined the notion of *admissible encodings*, which allow them to give a sufficient condition for an encoding f to be indifferentiable from a random oracle. But this is not applicable to the constant-time encodings (such as Icart's encoding) since they are not admissible. Hence, Farashahi *et al.* [14] proposed a more general construction $H(m) = f(h_1(m)) + \ldots + f(h_s(m))$, which preserves the indifferentiability notion if the h_i are modeled as random oracles and s is strictly greater than the genus of the curve.

*Corresponding author.

Email addresses: fifiramatou@gmail.com (N. Diarra), sowdjibab@yahoo.fr (D. Sow), ahmed.youssef@ucad.edu.sn (A.Y.O.C. Khlil)

On another side, ECC has many applications on Internet (SSL/TLS, SSH, Tor [10], Bitcoin,...); but it presents at least one drawback: for applications in censorship circumvention, points of elliptic curves are easy to distinguish from uniform random strings if a suitable implementation is not used. The problem of making points of elliptic curves indistinguishable from uniform random strings was investigated by Möller [11], Bernstein *et al.* [4], Tibouchi [17].

The first approach is Möller's one. In 2004 [11], Möller proposed to modify protocols so that transmitted points lie either on the given elliptic curve or in its quadratic twist [5]. But this approach imposes twist-security. The second approach, called Elligator, is the one proposed by Bernstein *et al.* in [4]. It is based on the construction of an efficient injective and invertible encoding ψ that maps a subset $S \subseteq \mathbb{F}_q$ (where q prime and $S \cap -S = \{0\}$), to the group $E(\mathbb{F}_q)$ of an elliptic curve E over $\mathbb{F}_q$. Since the map is injective and invertible, Bernstein *et al.* consider that a point $P \in \mathrm{Im}(\psi)$ of the curve can be viewed as the string representation of the unique $\psi^{-1}(P)$. Moreover, if q is chosen such that $\#S$ is relatively close to a power of 2, then a uniform $P \in \mathrm{Im}(\psi)$ will have a close to uniform bit string representation. This method has the advantage to not impose additional security requirements on the quadratic twist of the curve, but it relies on the existence of the injective encoding ψ.

Recently [17], Tibouchi proposed a new method, called Elligator-Squared, which supports more elliptic curves than Elligator. While Elligator is used to represent a point P in the curve by a preimage under an injective encoding, in Elligator-Squared, a point P in the curve is represented by a randomly sampled preimage under a surjective map.

In Binary-Elligator-Squared [5], a comparison between Elligator and Elligator-Squared is done. Elligator is better for protocols using a fixed base point (such as static ECDH), but Elligator-Squared is better for protocols using a variable base point (such as ElGamal encryption). Even if Elligator-Squared constructs a surjective map, it uses an injective encoding as Elligator. To our knowledge, only a few examples of such encodings exist [5, 4, 13, 12]. This is one of the motivations of this paper.

Organization of the paper:

- Section **2** recalls some definitions about square roots in finite fields (**2.1**) and gives an overview of existing encodings into elliptic curves (**2.2**).
- Sections **3** and 4 present the contributions of this paper as follows:
  - In section **3**, we revisit Elligator's methods for constructing *almost*-injective and invertible encodings for some models of curves: (**3.1**) generalized Huff curves $x(ay^2 - 1) = y(bx^2 - 1)$, (**3.2**) classical Huff curves $\alpha x(y^2 - 1) = \beta y(x^2 - 1)$, (**3.3**) Edwards curves $x^2 + y^2 = 1 + dx^2y^2$ and (**3.4**) Weierstrass model $y^2 = x^3 + ax^2 + c$.
  - Section **4** begins by a review of well-distributed encodings (**4.1**), as defined in [6, 14]. Then we show (**4.3**) how one can obtain a hash function indifferentiable from a random oracle using one of the previous encodings and following the methodology in [6, 14].

2. Preliminaries

2.1. Squares and square roots

Let q be an odd prime power.

(i) The **quadratic character** is the function χ defined by $\chi : \mathbb{F}_q \to \mathbb{F}_q : u \mapsto \chi(u) = u^{(q-1)/2}$ and verifying: $\chi(u) = 1$ if u is a non-zero square; $\chi(u) = -1$ if u is a non-square; and $\chi(u) = 0$ if $u = 0$. The following properties are also verified: $\chi(uv) = \chi(u) \cdot \chi(v)$ for any $u, v \in \mathbb{F}_q$; $\chi(a^2) = 1$ for any $a \in \mathbb{F}_q^*$; and if $q \equiv 3 \mod 4$, $\chi(-1) = -1$, $\chi(\chi(u)) = \chi(u)$, for any $u \in \mathbb{F}_q$. If $q \equiv 1 \mod 4$, then $\chi(-1) = 1$.

(ii) Define $\mathbb{F}_q^2 = \{a^2 : a \in \mathbb{F}_q\}$ (see [4]). A square root function $\sqrt{\ }$ for $\mathbb{F}_q$ is defined by: $\sqrt{\ } : \mathbb{F}_q^2 \to \mathbb{F}_q : a^2 \mapsto \sqrt{a^2} = \pm a$. For $q \equiv 3 \mod 4$, $a^{\frac{q+1}{4}}$ is called the principal square root of a; therefore one can take the principal square root as a square-root function, i.e., take $\sqrt{\mathbb{F}_q^2} = \mathbb{F}_q^2$. For an odd prime q, one can take $\sqrt{\mathbb{F}_q^2} = \{0, 1, ..., \frac{q-1}{2}\}$.

2.2. An overview of existing encodings into elliptic curves

We give here an overview of main existing encodings for elliptic curves.

2.2.1. Trivial encoding

For an elliptic curve $E_{a,b} : y^2 = x^3 + ax + b$, the simplest way to construct a point of $E_{a,b}$ is to use the trivial encoding, also known as the *try-and-increment* method. The idea is to pick a x-coordinate and try to deduce the y-coordinate by computing a square root: choose a random element $u \in \mathbb{F}_q^*$ and compute $u^3 + au + b$; and then test whether $u^3 + au + b$ is a square in $\mathbb{F}_q$. If it's the case, then returns $(x, y) = (u, \pm\sqrt{u^3 + au + b})$ as a point of the curve. Otherwise, one can choose another u in $\mathbb{F}_q$ and try again. But this method has at least one drawback, that is it cannot run in constant time: the number of operations depends on the input u. In practice the input u is the message m we want to hash; thus running this algorithm can allow the attacker to guess some information about m.

2.2.2. Encoding for supersingular curves

A *supersingular* curve over $\mathbb{F}_q$ is an elliptic curve E such that $|E(\mathbb{F}_q)| = q + 1$. For $q \equiv 2 \mod 3$, the curve defined by $E_b : y^2 = x^3 + b$ is a supersingular one. In their identity-based scheme[2], Boneh and Franklin proposed the function $f : u \mapsto ((u^2 - b)^{\frac{1}{3}}, u)$ that constructs a point of E_b, given any $u \in \mathbb{F}_q$. This function allows them to construct the public key Q_{id}(a point on the supersingular curve) corresponding to the identity id $\in \{0, 1\}^*$. But it is well-known that supersingular curves are useless for cryptographic concerns because of the MOV attack[1]: that is the DLP on E_b can be reduced to the DLP in $\mathbb{F}_q$. To avoid these attack, a large q should be used.

2.2.3. The SWU algorithm

In 2006[15], Shallue and van de Woestjine proposed an algorithm that generates, in polynomial time, a point of an elliptic curve $E_{a,b}$ given by its Weierstrass equation.
Let $\mathbb{F}_q$ be a finite field of characteristic at least 5, and $g(x) = x^3 + ax + b$ be a polynomial in $\mathbb{F}_q[x]$, with $a \neq 0$. We know from the Skalba's theorem [16] that there exist four non-constant rational functions $X_1(t), X_2(t), X_3(t), X_4(t) \in \mathbb{F}_q(x)$ such that:

$$g(X_1(t^2)) \cdot g(X_2(t^2)) \cdot g(X_3(t^2)) = (X_4(t))^2 \tag{1}$$

It follows that at less one one the $g(X_i(u^2))$ must be a quadratic residue in the finite field $\mathbb{F}_q$, given any $u \in \mathbb{F}_q$ such that u^2 is not a pole of the X_i's, $i = 1, 2, 3$.
From identity (1), one can deduce an encoding function to the curve $E_{a,b} : \ y^2 = g(x)$. It suffices to set $(x, y) = (X_i(u^2), \sqrt{g(X_i(u^2))})$, where i is the smallest indice such that $g(X_i(u^2))$ is a quadratic residue.
Even if this construction defines a constant-time encoding, it presents at least one drawback. In fact, the rational functions $X_i(t)$ are large and complex enough to make them difficult to implement. And there is no deterministic polynomial time for computing a square root in $\mathbb{F}_q$, unless making additional hypotheses on q. For example, when $q \equiv 3 \mod 4$, then computing a square root is simply an exponentiation.

2.2.4. Icart's function

Let $q = 2 \mod 3$; so the map $x \mapsto x^3$ is a bijection and then computation of a cubic root can be done as an exponentiation. In [9], Icart defined a new encoding function, based on the following idea: intersect the line $y = ux + v$ with the Weierstrass curve $E_{a,b} : \ y^2 = x^3 + ax + b$, with $a, b \in \mathbb{F}_q$. He defined the encoding function:

$$\begin{aligned} f_{a,b} : \mathbb{F}_q &\to E_{a,b} \\ x &\mapsto f_{a,b}(u) = \left((v^2 - b - \frac{u^6}{27})^{1/3} + \frac{u^2}{3}, ux + v \right) \end{aligned}$$

where $v = (3a - u^4)/6u$. As shown in the paper, this function presents many interesting properties. In fact, it can be implemented in polynomial time with $O(\log^3 q)$ operations. The inverse function $f_{a,b}^{-1}$ is also computable in polynomial time. Icart also showed that $|f_{a,b}^{-1}(P)| \leq 4$, given a point P on the elliptic curve. This results from the fact that to compute $f_{a,b}^{-1}(P)$, it's sufficient to solve the degree 4 polynomial over $\mathbb{F}_q$:

$$u^4 - 6u^2x + 6uy - 3a = 0$$

Moreover, Icart showed that the cardinal of the image set $\mathrm{Im}(f_{a,b})$ is greater than $q/4$ and made the following conjecture(proved later by Tibouchi and Fouque in [8]): the size of $\mathrm{Im}(f_{a,b})$ is approximately $\frac{5}{8}$ of the size of the curve $E_{a,b}$.

2.2.5. Encoding and extraction for Hessian curves

Let $d \in \mathbb{F}_q$ with $d^3 \neq 1$. A **Hessian curve**(a curve with a point of order 3) H_d over $\mathbb{F}_q$ is given by the equation $x^3 + y^3 + 1 = 3dxy$. For $q \equiv 2 \mod 3$, Farashahi[7] applied Icart's method to the set $H_d(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points of H_d. He obtained the function:

$$\begin{aligned} h_d : \mathbb{F}_q &\mapsto H_d(\mathbb{F}_q) \\ u &\mapsto h_d(u) = (x, y) \end{aligned}$$

defined by

- $h_d(u) = (x, y)$ if $u \neq -1$, where $x = -u\left(\frac{d^3u^3+}{u^3+1}\right)^{1/3}$, $v = -\left(\frac{d^3u^3+}{u^3+1}\right)^{1/3} + du$;
- and $h_d(u) = \mathcal{O}$ if $u = -1$, where $\mathcal{O}$ is the point at infinity.

The map h_d is well-defined since $h_d(u)$ is a point of $H_d(\mathbb{F}_q)$, for $u \in \mathbb{F}_q$. This encoding function for Hessian curves is less general than Icart's one, but has many other interesting properties. In fact, Farashahi showed that the size of the image set $h_d(\mathbb{F}_q)$ is at least $q/2$ an that the inverse function h_d^{-1} can be easily described. He also studied the possibility to extract random bits from the image $h_d(u)$ of an element $u \in \mathbb{F}_q$.

2.2.6. Injective encoding for Edwards curves: Elligator-1

An Edwards curve E_d defined over $\mathbb{F}_q$ is a model of elliptic curve given by the equation: $E_d : \ x^2 + y^2 = 1 + dx^2y^2$ with $d \notin \{0, 1\}$ and d is not a square.

In [4], Bernstein *et al.* defined an encoding that maps an element of $\mathbb{F}_q$ to a point of the curve E_d. Their work used the general method proposed by Fouque *et al.* in [13]. Note that, in their updated paper [12], Fouque *et al.* have also proposed an explicit encoding for Edwards curves, based on their previous work [13]. The encoding process of Bernstein *et al.* in [4] is described in the following theorem:

Theorem 1. *Let q be a prime power congruent to 3 modulo 4. Let s be a nonzero element of $\mathbb{F}_q$ with $(s^2 - 2)(s^2 + 2) \neq 0$. Define $c = 2/s^2$. Then $c(c - 1)(c + 1) \neq 0$. Define $r = c + 1/c$ and $d = -(c+1)^2/(c-1)^2$. Then $r \neq 0$, and d is not a square. The following elements of $\mathbb{F}_q$ are defined for each $t \in \mathbb{F}_q \setminus \{0, 1\}$:*

$$\begin{aligned} u = (1 - t)/(1 + t), \qquad & v = u^5 + (r^2 - 2)u^3 + u; \\ X = \chi(v)u, \qquad & Y = (\chi(v)v)^{(q+1)/4}\chi(v)\chi(u^2 + 1/c^2); \\ x = (c - 1)sX(1 + X)/Y, \qquad & y = (rX - (1 + X)^2)/(rX + (1 + X)^2). \end{aligned}$$

Furthermore $x^2 + y^2 = 1 + dx^2y^2$; $uvXYx(y + 1) \neq 0$ and $Y^2 = X^5 + (r^2 - 2)X^3 + X$.

The authors also showed that the image set of the map can be easily described. Furthermore, this map can be used for injective encoding into the curve, considering only half of the points of $\mathbb{F}_q$.

3. Elligator's methods revisited for various curves

In this section, we investigate the problem of constructing *Almost*-Injective and Invertible Encodings (AIIE) for some forms of curves, such as generalized Huff curves $x(ay^2-1)=y(bx^2-1)$, classical Huff curves $\alpha x(y^2-1)=\beta y(x^2-1)$, Edwards curves $x^2+y^2=1+dx^2y^2$ and the Weierstrass model $y^2=x^3+ax^2+c$. Our encodings are based on the Elligator method due to Bernstein *et al.* [4], and their *almost*-injectivity means that their restriction to a large enough subset of $\mathbb{F}_q$ is injective.

3.1. An AIEE for the generalized Huff model $x(ay^2-1)=y(bx^2-1)$

Fouque, Joux and Tibouchi proposed a method in [13], to construct an injective encoding for an elliptic curve, viewed as a quotient of an odd hyperelliptic curve. The elliptic curves compatible with their encoding are of the form: $y^2=x^3\pm 4x^2+Ax$ (see [13], pages 11-12). They have updated their work in [12]. Bernstein *et al.*, based on the work in [13], have proposed in [4], an injective encoding for the Edward's curve $E_d: x^2+y^2=1+dx^2y^2$, where d is not a square. In [13] and [12], an explicit encoding was not proposed for the special case of generalized Huff curve $x(ay^2-1)=y(bx^2-1)$, with $ab(a-b)\neq 0$. As in [4], our main contribution in this section is to adapt Elligator-1's method (as well as those of Fouque *et al.*) to generalized Huff curves.

Theorem 2. *Let $q\equiv 3 \mod 4$. Let $c\in\mathbb{F}_q$ such that $c(c-1)(c+1)\neq 0$. Let $A=-(c-\frac{1}{c})^2$; then $A\neq 0$ and A is not a square. Let $s=\dfrac{c+1}{c-1}$; then $s\neq\pm 1$. Let $\lambda\in\mathbb{F}_q^*$; define $b=\dfrac{\lambda^2}{1-s^2}$ and $a=-bs^2$. Then $a+b$ is a square, ab is not a square and $ab(a-b)\neq 0$. Under the previous hypotheses, for each element $z\in\mathbb{F}_q\setminus\{-1,1\}$, the following elements are well-defined:*

$$u=(1-z)/(1+z); \qquad v=-u^5+(c^2+1/c^2)u^3-u; \qquad X=\chi(v)u;$$
$$Y=\chi(v\cdot(c^2u^2-1))\sqrt{\chi(v)v}; \qquad \alpha=\frac{\lambda}{2}=\frac{\sqrt{a+b}}{2};$$
$$x=\frac{(1+X)(bX-\alpha^2(1+X)^2)}{b\alpha Y} \qquad \text{and} \qquad y=\frac{(1+X)(aX-\alpha^2(1+X)^2)}{a\alpha Y}.$$

Moreover, we have: $Y^2=-X^5+(2-A)X^3-X$ and $x(ay^2-1)=y(bx^2-1)$.

Proof.

(i) Let us show that $A\neq 0$ and A is not a square.

- If $A=0$ then $c=1/c$ so we have $c^2=1$ and $c=\pm 1$ which is a contradiction.
- If A is a square, then we have $-1=A(c/c^2-1)^2$ is a square which is a contradiction since $q=3 \mod 4$.

(ii) Let us show that $s\neq\pm 1$ and b is well-defined.

- $s = 1 \Rightarrow c - 1 = c + 1$ which is impossible.
- $s = -1 \Rightarrow c - 1 = -c - 1 \Rightarrow 2c = 0$ which is impossible since $c \neq 0$.

(iii) Let us show that $a + b$ is a square and $ab(a - b) \neq 0$.

- In fact, we have $a + b = -bs^2 + b = b(1 - s^2) = \lambda^2$ which is a square.
- $ab \neq 0$ since a and b are both non-zero. We have $a - b = 0 \Rightarrow -b(s^2 + 1) = 0$, which is impossible.

(iv) By hypothesis, u is well-defined and $u \neq 0$. Suppose that $v = 0$; so $u(-u^4 + (c^2 + 1/c^2)u^2 - 1) = 0$. Since $u \neq 0$, then we have $-u^4 + (c^2 + 1/c^2)u^2 - 1 = 0$. Thus $u^2 = -c^2$ or $u^2 = -1/c^2$ contradicting the fact that -1 is not a square.

(v) Since $uv \neq 0$ by above results, then $X \neq 0$.

(vi) Let us show that $1 + X \neq 0$. If $1 + X = 0$ then we have $u = -\chi(v)$ and $v = (\chi(v))^5 - (c^2 + 1/c^2)(\chi(v))^3 + \chi(v) = \chi(v) - (c^2 + 1/c^2 - 1)\chi(v) = -\chi(v)(c^2 + 1/c^2 - 2)$. So we find $v = -\chi(v)(c - 1/c)^2$, then $\chi(v) = -\chi(v)$, which is a contradiction.

(vii) Since $X \neq 0$ and $Y^2 = -X^5 + (c^2 + 1/c^2)X^3 - X$, similarly as 4, we have $Y \neq 0$.

(viii) We have $-X^5 + (c^2 + 1/c^2)X^3 - X = -(\chi(v)u)^5 + (c^2 + 1/c^2)(\chi(v)u)^3 - \chi(v)u = \chi(v)[-u^5 + (c^2 + 1/c^2)u^3 - u] = \chi(v)v = Y^2$.

(ix) x and y are well-defined since $Y \neq 0$.

(x) (x, y) verifies $x(ay^2 - 1) = y(bx^2 - 1)$?
At first we show that $\alpha^4(X^4 - (2 - A)X^2 + 1) = (bX - \alpha^2(1 + X)^2)(aX - \alpha^2(1 + X)^2)$. In fact, we have:
$(bX - \alpha^2(1 + X)^2)(aX - \alpha^2(1 + X)^2) = abX^2 - b\alpha^2X(X^2 + 2X + 1) - a\alpha^2(X^3 + 2X^2 + X) + \alpha^4(1 + 4X + 6X^2 + 4X^3 + X^4) = X^4(\alpha^4) + X^3(4\alpha^4 - (a + b)\alpha^2) + X^2(ab + 6\alpha^4 - 2\alpha^2(a + b)) + X(4\alpha^4 - \alpha^2(a + b)) + \alpha^4$. Then using $4 = (a + b)/\alpha^2$ and $A = ab/\alpha^4$ yields that $(bX - \alpha^2(1 + X)^2)(aX - \alpha^2(1 + X)^2) = \alpha^4(X^4 - (2 - A)X^2 + 1)$. Since a and b are not square, thus $(ay^2 - 1)(bx^2 - 1) \neq 0$. Now, we have:

$$\frac{bx^2 - 1}{ay^2 - 1} = \frac{a}{b} \cdot \frac{(1 + X)^2(bX - \alpha^2(1 + X)^2)^2 - b\alpha^2Y^2}{(1 + X)^2(aX - \alpha^2(1 + X)^2)^2 - a\alpha^2Y^2}$$

$$= \frac{a}{b} \cdot \left(\frac{bX - \alpha^2(1 + X)^2}{aX - \alpha^2(1 + X)^2}\right) \cdot \left[\frac{(1 + X)^2(bX - \alpha^2(1 + X)^2) - \frac{b\alpha^2Y^2}{bX - \alpha^2(1+X)^2}}{(1 + X)^2(aX - \alpha^2(1 + X)^2) - \frac{a\alpha^2Y^2}{aX - \alpha^2(1+X)^2}}\right]$$

$$= \frac{a}{b} \cdot \left(\frac{bX - \alpha^2(1 + X)^2}{aX - \alpha^2(1 + X)^2}\right) \cdot \left[\frac{(1 + X)^2(bX - \alpha^2(1 + X)^2) + \frac{b\alpha^2X(X^4 - (2-A)X^2 + 1)}{bX - \alpha^2(1+X)^2}}{(1 + X)^2(aX - \alpha^2(1 + X)^2) + \frac{a\alpha^2X(X^4 - (2-A)X^2 + 1)}{aX - \alpha^2(1+X)^2}}\right]$$

$$= \frac{a}{b} \cdot \left(\frac{bX - \alpha^2(1 + X)^2}{aX - \alpha^2(1 + X)^2}\right) \cdot \left[\frac{\alpha^2(1 + X)^2(bX - \alpha^2(1 + X)^2) + bX(aX - \alpha^2(1 + X)^2)}{\alpha^2(1 + X)^2(aX - \alpha^2(1 + X)^2) + aX(bX - \alpha^2(1 + X)^2)}\right]$$

$$= \frac{a}{b} \cdot \left(\frac{bX - \alpha^2(1 + X)^2}{aX - \alpha^2(1 + X)^2}\right) \cdot \left(\frac{abX^2 - \alpha^4(1 + X)^4}{abX^2 - \alpha^4(1 + X)^4}\right)$$

$$= \frac{a}{b} \cdot \left(\frac{bX - \alpha^2(1 + X)^2}{aX - \alpha^2(1 + X)^2}\right) = \frac{x}{y}$$

In the situation of the previous theorem, we can write $x = \dfrac{(1+X)(bX-\alpha^2(1+X)^2)}{b\alpha Y}$ $= g(z)$ and $y = \dfrac{(1+X)(aX-\alpha^2(1+X)^2)}{a\alpha Y} = h(z)$. Therefore, we can define the encoding function as follows.

Definition 1. *The encoding function for the generalized Huff curve* $E: x(ay^2-1) = y(bx^2-1)$ *with* $ab(a-b) \neq 0$ *is the function* $\phi_{a,b} : \mathbb{F}_q \to E(\mathbb{F}_q)$ *defined as follows:* $\phi_{a,b}(\pm 1) = (0,0)$*; and* $\phi_{a,b}(z) = (x,y) = (g(z), h(z))$ *if* $z \neq \pm 1$.

NB: Our encoding function for generalized Huff curves does not include classical Huff curves, because in our algorithm, ab is not a square, hence a and b cannot be square simultaneously.

Proposition 1. *In the situation of definition (1), if* $z \in \mathbb{F}_q$ *then* $-z \in \phi_{a,b}^{-1}(\phi_{a,b}(z))$.

Proof. Let $z \in \mathbb{F}_q$; if $z = \pm 1$ then $\phi_{a,b}(z) = (0,0) = \phi_{a,b}(-z)$ by definition. So we can suppose that $z \neq 1, -1$. Let $z' = -z$ and define u', v', X', Y', x', y' from z', with $(x', y') = \phi_{a,b}(z')$. To show that $(x,y) = (x', y')$, as in [4], we will compare u' to u, v' to v, X' to X, Y to Y' and finally compute $(x', y') = \phi_{a,b}(z')$.

(i) $u' = \frac{1-z'}{1+z'} = \frac{1+z}{1-z} = \frac{1}{u}$.

(ii) $v' = -u'^5 + (c^2 + 1/c^2)u'^3 - u' = -\frac{1}{u^5} + (c^2+1/c^2)\frac{1}{u^3} - \frac{1}{u} = \frac{v}{u^6}$. Note that $\chi(v') = \chi(v)$.

(iii) $X' = \chi(v')u' = \chi(v)u' = \frac{\chi(v)}{u} = \frac{1}{u\chi(v)} = \frac{1}{X}$.

(iv) $Y' = \chi(v' \cdot (c^2u'^2 - 1)/c)\sqrt{\chi(v')v'} = \chi(v') \cdot \chi(u'^2 - 1/c^2)\sqrt{\chi(v')v'}$. For the second factor of Y', recall that $v' = v/u^6$ and $\chi(v') = \chi(v)$; so $\sqrt{\chi(v')v'} = \sqrt{\frac{\chi(v)v}{u^6}} = \sqrt{\frac{\chi(v)v}{\chi(u)^2u^6}} = \frac{\chi(u)\sqrt{\chi(v)v}}{u^3}$.
Since $\chi((u^2 - 1/c^2)^2c^2u^4) = 1$, we have $\chi(u'^2 - 1/c^2) = \chi((u'^2 - 1/c^2)(u^2 - 1/c^2)^2c^2u^4)$. Thus, we have: $\chi(u'^2 - 1/c^2) = \chi(u^2(c^2 - u^2)(u^2 - 1/c^2)^2)$.
Since $v = -u^5 + (c^2 + 1/c^2)u^3 - u = -u(u^2 - c^2)(u^2 - 1/c^2)$, we then have $\chi(u'^2 - 1/c^2) = \chi(uv(u^2 - 1/c^2))$.
Finally, $Y' = \chi(v') \cdot \chi(u'^2 - 1/c^2)\sqrt{\chi(v')v'} = \frac{1}{u^3}\left(\chi(u^2)\chi(v^2)\chi(u^2 - 1/c^2)\sqrt{\chi(v')v'}\right) = \dfrac{Y}{\chi(v)u^3} = \dfrac{Y}{(\chi(v)u)^3} = \dfrac{Y}{X^3}$.

(v) Since $y' = \frac{(1+X')(aX' - \alpha^2(1+X')^2)}{a\alpha Y'}$, $X' = 1/X$ and $Y' = Y/X^3$, then we have $y' = X^3\left(\dfrac{(1+1/X)(a/X - \alpha^2(1+1/X)^2}{a\alpha Y}\right) = \dfrac{X(X+1)(aX - \alpha^2(1+X)^2)}{a\alpha Y} = y$, as desired.

(vi) As for y', one can show that $x' = x$.

Hence we conclude that $\phi_{a,b}(-z) = \phi_{a,b}(z)$, for every $z \in \mathbb{F}_q$.

Proposition 2. *In the situation of definition 1, if* $(x, y) \in \phi_{a,b}(\mathbb{F}_q)$ *then:* $x \neq y$ *and* $1 - 4\alpha^2\eta$ *is a square, where* $\eta = \dfrac{bx - ay}{ab(x - y)}$ *with* $\alpha^2 = \dfrac{a + b}{4}$.

Proof. Let $(x, y) \in \phi_{a,b}(\mathbb{F}_q)$; by theorem 2, we know that $x = \dfrac{(1 + X)(bX - \alpha^2(1 + X)^2)}{b\alpha Y}$ and $y = \dfrac{(1 + X)(aX - \alpha^2(1 + X)^2)}{a\alpha Y}$.

- $x = y \Rightarrow a = b$ which is impossible.
- We have $\dfrac{x}{y} = \dfrac{a}{b}\left(\dfrac{bX - \alpha^2(1 + X)^2}{aX - \alpha^2(1 + X)^2}\right)$ and we obtain the equation $X^2 + X(2 - \dfrac{1}{\eta\alpha^2}) + 1 = 0$, where $\eta = \dfrac{bx - ay}{ab(x - y)}$. The discriminant $\delta = \dfrac{1}{(\eta\alpha^2)^2}(1 - 4\eta\alpha^2)$ of this equation has to be a square. This leads to $1 - 4\eta\alpha^2$ is a square, as desired.

Proposition 3. *For* $z \in \mathbb{F}_q \setminus \{\pm 1\}$*, the set of preimages of* $\phi_{a,b}(z)$ *is* $\{-z, z\}$.

Proof.

- $\{z, -z\} \subseteq \phi_{a,b}^{-1}(\phi_{a,b}(z))$ follows from proposition 1.
- Let $z \in \mathbb{F}_q$ and $z' \in \mathbb{F}_q$ such that $\phi_{a,b}(z') = \phi_{a,b}(z)$. Define, as in the proof of theorem 1 and in proposition 2, the following elements:
  - for z: u, v, X, Y, x, y;
  - for $z_1 = -z$: $u_1, v_1, X_1, Y_1, x_1 = x, y_1 = y$;
  - for z': $u', v', X', Y', x' = x, y' = y$.

  By the previous proposition and since $x = x' = x_1$, $y = y' = y_1$, we have $\eta = \eta' = \eta_1$. So X, as well as X_1 and X' are solutions of the equation $F^2 + F(2 - \frac{1}{\eta\alpha^2}) + 1 = 0$.

  Since $X = 1/X_1$ then $X \neq X_1$. In fact $X = X_1$ implies that $X^2 = 1 \Rightarrow X = \pm 1 \Rightarrow \chi(v)u = \pm 1$; thus $u = \pm 1$ and $\frac{1-z}{1+z} = \pm 1$, which is impossible if $z \neq 0$.

  Now let us discuss the following cases.

  - If $X' = X$: let us prove that $\chi(v) = \chi(v')$, $u' = u$ and $z' = z$. Now we have $x = \dfrac{(1 + X)(bX - \alpha^2(1 + X)^2)}{b\alpha Y} = \dfrac{(1 + X)(bX - \alpha^2(1 + X)^2)\chi(v)}{b\alpha\chi(c^2u^2 - 1)\sqrt{\chi(v)v}}$; but $u = \chi(v)X$ so $x = \dfrac{(1 + X)(bX - \alpha^2(1 + X)^2)\chi(v)}{b\alpha\chi(c^2X^2 - 1)\sqrt{\chi(v)v}}$ and thus $\chi(v) = \chi\left(b\alpha(1 + X)(bX - \alpha^2(1 + X)^2)(c^2X^2 - 1)\right)$. Similarly we have $\chi(v') = \chi\left(b\alpha(1 + X')(bX' - \alpha^2(1 + X')^2)(c^2X'^2 - 1)\right)$. Since $x = x'$ and $X = X'$, we have $\chi(v) = \chi(v')$; therefore $u' = u$ and $z' = z$.

– If $X' = X_1$: as above we have $\chi(v') = \chi(v_1)$, $u' = u_1$ and $z' = z_1$.

Proposition 4. *Let $(x, y) \in E(\mathbb{F}_q)$. If $x - y \neq 0$ and $1 - 4\alpha^2\eta$ is a square, with $\eta = \dfrac{bx - ay}{ab(x - y)}$, there exists $\overline{z} \in \mathbb{F}_q$ such that $\phi_{a,b}(\overline{z}) = (x, y)$.*

Proof. Let $(x, y) \in E(\mathbb{F}_q)$ such that $x - y \neq 0$ and $1 - 4\alpha^2\eta$ is a square, where $\eta = \dfrac{bx - ay}{ab(x - y)}$. The discriminant δ of the equation $F^2 + F(2 - \frac{1}{\eta\alpha^2}) + 1 = 0$ is then a square, since $1 - 4\alpha^2\eta$ is a square. So there is at least one solution $X = -\frac{1}{2}(2 - \frac{1}{\eta\alpha^2}) + \frac{1}{2\eta\alpha^2}(1 - 4\alpha^2\eta)^{(q+1)/4}$. Note that the two quantities

$\dfrac{(1 + X)(bX - \alpha^2(1 + X)^2)}{\alpha bx}$ and $\dfrac{(1 + X)(aX - \alpha^2(1 + X)^2)}{\alpha ay}$ are the same. In fact, as a solution of the previous equation, X verifies $X^2 = -X(2 - \frac{1}{\eta\alpha^2}) - 1$; so $bX - \alpha^2(1+X)^2 = \dfrac{X(b\eta - 1)}{\eta}$ and $aX - \alpha^2(1+X)^2 = \dfrac{X(a\eta - 1)}{\eta}$. Thus, we have $\dfrac{bX - \alpha^2(1 + X)^2}{aX - \alpha^2(1 + X)^2} = \dfrac{1 - b\eta}{1 - a\eta}$. From $\eta = \dfrac{bx - ay}{ab(x - y)}$, we deduce that $\dfrac{x}{y} = \dfrac{a(1 - b\eta)}{b(1 - a\eta)}$; so $\dfrac{a(bX - \alpha^2(1 + X)^2)}{b(aX - \alpha^2(1 + X)^2)} = \dfrac{x}{y}$ and $\dfrac{(1 + X)(bX - \alpha^2(1 + X)^2)}{\alpha bx} = \dfrac{(1 + X)(aX - \alpha^2(1 + X)^2)}{\alpha ay}$.

Now we define $Y = \dfrac{(1 + X)(bX - \alpha^2(1 + X)^2)}{\alpha bx} = \dfrac{(1 + X)(aX - \alpha^2(1 + X)^2)}{\alpha ay}$.

(i) First, we verify that $Y^2 = -X^5 + (2 - A)X^3 - X$. In fact, x and y are such that $\dfrac{bx^2 - 1}{ay^2 - 1} = \dfrac{x}{y}$; that is $\dfrac{a}{b}(\dfrac{(1 + X)^2(bX - \alpha^2(1 + X)^2)^2 - b\alpha^2Y^2}{(1 + X)^2(aX - \alpha^2(1 + X)^2)^2 - a\alpha^2Y^2}) = \dfrac{a}{b}(\dfrac{bX - \alpha^2(1 + X)^2}{aX - \alpha^2(1 + X)^2})$.
We have $(1+X)^2(bX - \alpha^2(1+X)^2(ax - \alpha^2(1+X)^2)^2 - a\alpha^2Y^2(bX - \alpha^2(1+X)^2) = (1+X)^2(aX - \alpha^2(1+X)^2(bx - \alpha^2(1+X)^2)^2 - b\alpha^2Y^2(aX - \alpha^2(1+X)^2)$.
$\Rightarrow \alpha^4Y^2(1+X)^2(b-a) = X(1+X)^2(a-b)(bX - \alpha^2(1+X)^2)(aX - \alpha^2(1+X)^2)$.**(*)**
But recall from the proof of theorem 2 that $(bX - \alpha^2(1+X)^2)(aX - \alpha^2(1+X)^2) = \alpha^4(X^4 - (2 - A)X^2 + 1)$. So **(*)** yields to:
$\alpha^4Y^2(1 + X)^2(b - a) = \alpha^4X(1 + X)^2(a - b)(X^4 - (2 - A)X^2 + 1)$. Finally we have $Y^2 = -X^5 + (2 - A)X^3 - X$ as desired.

(ii) Define $\beta = \chi\left(Y(c^2X^2 - 1)\right)$ and $u = \beta X$.

(iii) Define $v = -u^5 + (c^2 + 1/c^2)u^3 - u$.
Now, we have $v = \beta\left(-X^5 + (c^2 + 1/c^2)X^3 - X\right)$. Since $Y^2 = -X^5 + (2-A)X^3 - X$ and $q \equiv 3 \mod 4$, then $v = \beta Y^2$ and $\chi(v) = \chi(\beta) = \beta$. From $u = \beta X$ and $\beta = \chi(v)$, we deduce that $X = \chi(v)u$ and $Y^2 = \beta v = \chi(v)v$.

(iv) $\chi(v) = \beta = \chi\left(Y(c^2X^2 - 1)\right) = \chi\left(Y(X^2 - 1/c^2)\right) \Rightarrow \chi(Y) = \chi(v)\chi\left(X^2 - 1/c^2\right)$.
So $Y = (\chi(v)v)^{(q+1)/4}\chi(v)\chi\left(X^2 - 1/c^2\right)$.

(v) Finally let $\overline{z} = \dfrac{1-u}{1+u}$; so $\phi_{a,b}(t) = (x, y)$ by the previous construction. Note that $\overline{z}$ is well-defined since $u = \pm X$ and $X \neq 1$, and $\overline{z} \neq \pm 1$.

Efficiency of $\phi_{a,b}$ and ϕ_3^{-1}: As in Elligator-1 [4], the definitions of u, v, X, Y, x, y in theorem 2 involve divisions by c, $1+c$, $1-c$ and αY, two computations of the quadratic character χ (namely $\chi(v)$ and $\chi(u^2 - 1/c^2)$), a square-root computation and some multiplications. One can reduce the number of multiplications, for example by factoring $v = -u^5 + (c^2 + 1/c^2)u^3 - u$ as $v = -u(u^2 - c^2)(u^2 - 1/c^2)$. And $u^2 - 1/c^2$ can be reused when computing $Y = \chi(v) \cdot \chi(u^2 - 1/c^2) \cdot \sqrt{\chi(v)v}$. The computation of $\chi(v)$ and $\chi(u^2 - 1/c^2)$ can be replaced by exponentiations, and the square-root computation is also replaced by an exponentiation with exponent $a^{(q+1)/4}$ since $q \equiv 3 \mod 4$. For $P = (x, y) \in E_{a,b}$, checking wether or not P is in $\mathrm{Im}(\phi_{a,b})$ requires few multiplications, one inversion and a computation of $\chi(1 - 4\alpha^2\eta)$, where $\eta = (bx - ay)/(ab(x - y))$.

Elligator-Squared approach with Elligator-3 encoding: Recently [17], Tibouchi proposed a new method, called Elligator-Squared, which supports more elliptic curves than Elligator, and uses a surjective map to represent a point in the curve by its preimage under this map. In fact, any $P \in E(\mathbb{F}_q)$ is represented by its randomly sampled preimage under an admissible encoding of the form $f^{\otimes 2} : (u, v) \mapsto f(u) + f(v)$, where $f : \mathbb{F}_q \to E(\mathbb{F}_q)$ is any encoding. In the same paper, Tibouchi gave a list of known encodings that meet the requirements of Elligator-Squared construction, namely *well-bounded encodings*.

As for Elligator-1 encoding [4], the Elligator-squared construction can be applied to our new Elligator-3 encoding. In fact, $\phi_{a,b}$ can be expressed in terms of a degree 2 covering $h : H \to E$ of E by a certain elliptic curve H of genus 2 [17, 13]. Hence, using lemma 3 in [17], one shows that $\phi_{a,b}$ is $2-$well-distributed and is also a $(2, 2)$-well-bounded encoding, since any $P \in E(\mathbb{F}_q)$ has at most 2 preimages (see proposition 3).

Also note that Elligator-3 encoding $\phi_{a,b}$ can be used to build a hash function into the elliptic curve. But it cannot be directly used in the BLS signature scheme [3]. This results from the fact that not all points of the elliptic curve are representable since the image set does not cover the whole curve. And in the BLS signature scheme, which is a full-domain signature scheme, all points need to be representable. Nevertheless, we can overcome this limitation by combining Elligator-3 encoding and Elligator-Squared approach. In fact, the resulting construction $\phi_{a,b}^{\otimes 2} : (u, v) \mapsto \phi_{a,b}(u) + \phi_{a,b}(v)$, which we call *Elligator-3-Squared*, is a surjective one.

3.2. An AIEE for the classical Huff model $\alpha x(y^2 - 1) = \beta y(x^2 - 1)$

The classical Huff model $\alpha x'(y'^2 - 1) = \beta y'(x'^2 - 1)$ is included in the generalized Huff model $x(ay^2 - 1) = y(bx^2 - 1)$. In fact, one can simply set $a = \alpha^2$, $b = \beta^2$ and then use the change of variables $(x, y) \to (x' = \beta x, y' = \alpha y)$. But the previous method is not directly applicable to the classical Huff model, since the product ab has to be a non-square in $\mathbb{F}_q$. This is not the case when $a = \alpha^2$ and $b = \beta^2$. To avoid these problems, one can possibly

use the translation suggested in [12], page 13.
In this section, we propose an encoding function for the classical Huff model $\alpha x(y^2 - 1) = \beta y(x^2 - 1)$ with $\alpha\beta(\alpha^2 - \beta^2)(\alpha^2 + \beta^2) \neq 0$, using Elligator-2 method as in [4]. Elligator-2 method's propose an injective encoding for Weierstrass curves of the form $y^2 = x^3 + Ax^2 + Bx$. With this method, to encode into another form (such as Edwards, Huff,...), it is necessary to use a birational equivalence. We propose the following algorithm which allows to encode directly into Huff curves, without using any birational equivalence.

We begin by giving the following algorithm.

Algorithm 1.

Input: *$\alpha, \beta \in \mathbb{F}_q$ such that $\alpha\beta(\alpha^2-\beta^2)(\alpha^2+\beta^2) \neq 0$, u a non-square in $\mathbb{F}_q$ and $r \in \mathbb{F}_q$ verifying $\alpha^2 + u\beta^2 r^2 \neq 0$;*
Output: *A point $(x, y) \in E_{\alpha,\beta} :\ \alpha x(y^2 - 1) = \beta y(x^2 - 1)$;*

1. $v = \dfrac{\beta(\alpha^2 + u\beta^2 r^2)}{\alpha(\alpha^2 + \beta^2)}$;

2. $\varepsilon = \chi\left(v(\alpha v - \beta)(\alpha - \beta v)\right)$;

3. $t = \dfrac{1}{2}\left(\varepsilon\left(\dfrac{1+v^2}{v} - \dfrac{\alpha}{\beta} - \dfrac{\beta}{\alpha}\right) + \left(\dfrac{\alpha}{\beta} + \dfrac{\beta}{\alpha} + \dfrac{v^2-1}{v}\right)\right)$;

4. $x = -\varepsilon\sqrt{\dfrac{t(\alpha t - \beta)}{\alpha - \beta t}}$;

5. $y = \dfrac{x}{t}$;

6. ***Return*** (x, y);

Theorem 3. *Let q be a prime power, $\alpha, \beta \in \mathbb{F}_q$ such that $\alpha\beta(\alpha^2 - \beta^2)(\alpha^2 + \beta^2) \neq 0$, u a non-square in $\mathbb{F}_q$ and define the set $R = \{r \in \mathbb{F}_q :\ \alpha^2 + u\beta^2 r^2 \neq 0\}$. Let $E_{\alpha,\beta}$ be the elliptic curve defined over $\mathbb{F}_q$ by $\alpha x(y^2 - 1) = \beta y(x^2 - 1)$. Then algorithm 1 defines a deterministic encoding $\phi_{\alpha,\beta} :\ R \to E_{\alpha,\beta},\ r \mapsto \phi_{\alpha,\beta}(r) = (x, y)$.*

Proof.

(i) Let us show that v is well-defined and $v \neq 0$:

By the hypothesis on α and β, we have $\alpha(\alpha^2 + \beta^2) \neq 0$; so v is well-defined. Suppose that $v = 0$; this implies that $\alpha^2 + u\beta^2 r^2 = 0$, which is impossible by the definition of R. Thus $v \neq 0$.

(ii) We show that ε is well-defined and $\varepsilon \neq 0$:

In fact, suppose that $\alpha - \beta v = 0$; this implies that $\alpha^2(\alpha^2+\beta^2) - \beta^2(\alpha^2 + u\beta^2 r^2) = 0$ and then $r^2 = \dfrac{\alpha^4}{u\beta^4}$. This cannot happen since u is not a square in $\mathbb{F}_q$; so ε is well-defined.

Now suppose that $\varepsilon = 0$; so $v(\alpha v - \beta) = 0$ and then $\alpha v - \beta$ since $v \neq 0$. But $\alpha v - \beta = 0 \Rightarrow \alpha\beta(\alpha^2 + u\beta^2 r^2) - \alpha\beta(\alpha^2+\beta^2) = 0 \Rightarrow u\alpha\beta^3 r^2 - \alpha\beta^3 = 0 \Rightarrow r^2 = \frac{1}{u}$; contradiction since u is not a square. Finally we have $\varepsilon \neq 0$, that is $\varepsilon = \pm 1$.

(iii) Let us show that t is well-defined and $t \neq 0$:

First see that $\alpha\beta v \neq 0$; so t is well-defined. To show that $t \neq 0$, we have to consider the cases where $\varepsilon = 1$ and where $\varepsilon = -1$.

- if $\varepsilon = 1$, then $t = v \neq 0$.
- if $\varepsilon = -1$, then $t = \dfrac{v(\alpha^2+\beta^2) - \alpha\beta}{\alpha\beta v}$. Suppose that $v(\alpha^2+\beta^2) - \alpha\beta = 0$; so $\dfrac{\beta(\alpha^2 + u\beta^2 r^2)}{\alpha(\alpha^2+\beta^2)} = v = \dfrac{\alpha\beta}{\alpha^2+\beta^2}$. This implies that $u\beta^2 r^2 = 0$ which is impossible since $r \in R \setminus \{0\}$. Hence $t \neq 0$.

Finally t is well-defined and $t \neq 0$.

(iv) We show that x is well-defined and $x \neq 0$:

For this, we must show that $\dfrac{t(\alpha t - \beta)}{\alpha - \beta t}$ is well-defined and is a non-zero square. As previously, for t, we have to consider the cases where $\varepsilon = 1$ and where $\varepsilon = -1$.

- if $\varepsilon = 1$, then $t = v$ and $\alpha - \beta t = \alpha - \beta v = 0$ which is impossible as previously shown. Moreover we have $\chi\left(\dfrac{t(\alpha t - \beta)}{\alpha - \beta t}\right) = \chi\left(\dfrac{v(\alpha v - \beta)}{\alpha - \beta v}\right) = \varepsilon = 1$. Hence we conclude that x is well-defined when $\varepsilon = 1$.
- if $\varepsilon = -1$, then $t = \dfrac{v(\alpha^2+\beta^2) - \alpha\beta}{\alpha\beta v}$. Suppose that $\alpha - \beta t = 0$; this implies that $\beta v = \alpha$ and then $r^2 = \dfrac{\alpha^4}{u\beta^4}$; contradiction since $\chi(u) = -1$. Thus the quantity $\dfrac{t(\alpha t - \beta)}{\alpha - \beta t}$ is well-defined. Moreover we have:

$$\begin{aligned}
\chi\left(\frac{t(\alpha t - \beta)}{\alpha - \beta t}\right) &= \chi\left(\frac{\alpha(\alpha v - \beta)(v(\alpha^2+\beta^2) - \alpha\beta)}{v\beta^3(\alpha - \beta v)}\right) \\
&= \chi\left(\frac{\alpha v - \beta}{v(\alpha - \beta v)}\right) \cdot \chi\left(\alpha\beta\left(v(\alpha^2+\beta^2) - \alpha\beta\right)\right) \\
&= \varepsilon \cdot \chi\left(\alpha\beta\left(v(\alpha^2+\beta^2) - \alpha\beta\right)\right) = -\chi\left(\alpha\beta\left(v(\alpha^2+\beta^2) - \alpha\beta\right)\right)
\end{aligned}$$

But $\chi\left(\alpha\beta\left(v(\alpha^2+\beta^2)-\alpha\beta\right)\right) = \chi\left(\alpha\beta\left(\frac{u\beta^3r^2}{\alpha}\right)\right) = \chi(u) = -1$. Hence we conclude that $\chi\left(\frac{t(\alpha t-\beta)}{\alpha-\beta t}\right) = 1$ and x is well-defined when $\varepsilon = -1$. Furthermore x is a non-zero element of $\mathbb{F}_q$.

(v) y is well-defined since $t \neq 0$ and $y \neq 0$ since $x \neq 0$.

(vi) We show that $(x,y) \in E_{\alpha,\beta}:\ \alpha x(y^2-1) = \beta y(x^2-1)$:

In fact $\frac{y^2-1}{x^2-1} = \frac{\frac{x^2}{t^2}-1}{x^2-1} = \frac{x^2-t^2}{t^2(x^2-1)} = \frac{1}{t^2}\left(\frac{\frac{t(\alpha t-\beta)}{\alpha-\beta t}-t^2}{\frac{t(\alpha t-\beta)}{\alpha-\beta t}-1}\right) = \frac{\beta}{\alpha t^2}\left(\frac{t^3-t}{t^2-1}\right) = \frac{\beta}{\alpha t} = \frac{\beta y}{\alpha x}$.

Hence we have $\alpha x(y^2-1) = \beta y(x^2-1)$, which ends the proof.

Proposition 5. *For any $r \in R$, the set of preimages of $\phi_{\alpha,\beta}(r)$ is $\{r,-r\}$.*

Proof. It is obvious that $\phi_{\alpha,\beta}(-r) = \phi_{\alpha,\beta}(r)$ since the definition of $\phi_{\alpha,\beta}$ only uses r^2. Now let $r' \in R$ such that $\phi_{\alpha,\beta}(r') = \phi_{\alpha,\beta}(r)$. We want to show that $r' = r$ or $r' = -r$. From r' we define the elements $v', \varepsilon', t', x', y'$ as in theorem 3. So $\phi_{\alpha,\beta}(r') = \phi_{\alpha,\beta}(r) \Rightarrow x' = x$ and $y' = y$. Furthermore we have $t' = t$ and then $-\varepsilon'\sqrt{\frac{t(\alpha t-\beta)}{\alpha-\beta t}} = -\varepsilon\sqrt{\frac{t(\alpha t-\beta)}{\alpha-\beta t}}$. So $\varepsilon' = \varepsilon$; and we have $v' = v$ by replacing ε' by ε in $t' = t$. Finally $v = v'$ implies that $r'^2 = r^2$, that is $r' = \pm r$.

Proposition 6. *In the situation of theorem 3, we have:*

(i) $\mathrm{Im}(\phi_{\alpha,\beta})$ *is the set of* $(x,y) \in E_{\alpha,\beta}$ *such that:*

- $\chi\left(u\alpha\beta xy(\alpha^2+\beta^2-\alpha\beta\frac{y}{x})\right) = 1$ *if* $x \notin \sqrt{\mathbb{F}_q^2}$.
- *and* $\chi\left(u\alpha\beta xy(\alpha^2+\beta^2-\alpha\beta\frac{x}{y})\right) = 1$ *if* $x \in \sqrt{\mathbb{F}_q^2}$;

(ii) For $(x,y) \in \mathrm{Im}(\phi_{\alpha,\beta})$, *define* $t = \frac{x}{y}$ *and* $z = \frac{t(\alpha t-\beta)}{\alpha-\beta t}$; *so* $x \in \{\sqrt{z}, -\sqrt{z}\}$.
Let $\overline{r}$ *defined as follows:*
$\overline{r} = \frac{1}{\beta}\sqrt{\frac{\alpha(x(\alpha^2+\beta^2)-\alpha\beta y)}{u\beta y}}$ *if* $x = -\sqrt{z}$; *and* $\overline{r} = \alpha\sqrt{\frac{\alpha x}{u\beta(y(\alpha^2+\beta^2)-\alpha\beta x)}}$ *if* $x = \sqrt{z}$. *Then* $\overline{r} \in R$ *and* $\phi_{\alpha,\beta}(\overline{r}) = (x,y)$.

Proof.

(i) For this statement, we have to show two things. The first one is that every $(x,y) \in \mathrm{Im}(\phi_{\alpha,\beta})$ verifies the conditions mentioned above; the second is that any point $(x,y) \in E_{a,b}$ verifying these conditions, is in $\mathrm{Im}(\phi_{\alpha,\beta})$.

- Let $(x,y) \in \mathrm{Im}(\phi_{\alpha,\beta})$; so there exists $r \in R \setminus \{0\}$ such that the elements $t = \dfrac{x}{y}$, ε, v are defined as in theorem 3. We consider two cases:
  - if $\varepsilon = 1$, so $x = -\sqrt{\dfrac{t(\alpha t - \beta)}{\alpha - \beta t}} \notin \sqrt{\mathbb{F}_q^2}$ and $\dfrac{x}{y} = t = v = \dfrac{\beta(\alpha^2 + u\beta^2 r^2)}{\alpha(\alpha^2+\beta^2)}$.
    Let us show that $\chi\left(u\alpha\beta xy(\alpha^2+\beta^2-\alpha\beta\dfrac{y}{x})\right) = 1$. In fact, we have:
    $$\begin{aligned} u\alpha\beta xy(\alpha^2+\beta^2-\alpha\beta\frac{y}{x}) =& u\alpha by^2(t(\alpha^2+b^2)-\alpha b) = u\alpha\beta y^2\left(\frac{\beta(\alpha^2+u\beta^2r^2)}{\alpha} - \alpha\beta\right) \\ =& u\alpha\beta y^2\left(\frac{u\beta^3 r^2}{\alpha}\right) = u^2\beta^4 r^2 y^2 \text{ which is a square.} \end{aligned}$$
  - if $\varepsilon = -1$, so $x = \sqrt{\dfrac{t(\alpha t-\beta)}{\alpha-\beta t}} \in \sqrt{\mathbb{F}_q^2}$ and $\dfrac{x}{y} = t = \dfrac{v(a^2+b^2)-ab}{abv}$. Let us show that $\chi\left(u\alpha\beta xy(\alpha^2+\beta^2-\alpha\beta\dfrac{x}{y})\right) = 1$. In fact, we have:
    $$\begin{aligned} u\alpha\beta xy(\alpha^2+\beta^2-\alpha\beta\frac{x}{y}) =& u\alpha\beta x^2\left(\frac{\alpha^2+\beta^2-\alpha\beta t}{t}\right) = u\alpha\beta x^2\left(\frac{\alpha\beta}{vt}\right) \\ =& u\alpha\beta x^2\left(\frac{\alpha^2\beta^2}{v(\alpha^2+\beta^2)-\alpha\beta}\right) = u\alpha\beta x^2\left(\frac{\alpha^3}{u\beta r^2}\right) \\ =& \frac{\alpha^4 x^2}{r^2} \text{ which is a square.} \end{aligned}$$
- Now let $(x,y) \in E_{\alpha,\beta}$ such that $\chi\left(u\alpha\beta xy(\alpha^2+\beta^2-\alpha\beta\dfrac{y}{x})\right) = 1$ if $x \notin \sqrt{\mathbb{F}_q^2}$ and $\chi\left(u\alpha\beta xy(\alpha^2+\beta^2-\alpha\beta\dfrac{x}{y})\right) = 1$ if $x \in \sqrt{\mathbb{F}_q^2}$.
  We define $\overline{r} = \dfrac{1}{\beta}\sqrt{\dfrac{\alpha(x(\alpha^2+\beta^2)-\alpha\beta y)}{u\beta y}}$ if the first condition is verified; and $\overline{r} = a\sqrt{\dfrac{\alpha x}{u\beta(y(\alpha^2+\beta^2)-\alpha\beta x)}}$ otherwise. First see that $\overline{r}$ is well-defined and $\overline{r} \neq 0$ in both cases since $u\alpha\beta xy(\alpha^2+\beta^2-\alpha\beta\dfrac{y}{x})$ and $u\alpha\beta xy(\alpha^2+\beta^2-\alpha\beta\dfrac{x}{y})$ are non-zero squares. Now let us show that $\overline{r} \in R$.
  - if $\overline{r} = \dfrac{1}{\beta}\sqrt{\dfrac{\alpha(x(\alpha^2+\beta^2)-\alpha\beta y)}{u\beta y}}$, then $\alpha^2 + u\beta^2\overline{r}^2 = \alpha^2 + u\beta^2\left(\dfrac{\alpha\left(x(\alpha^2+\beta^2)-\alpha\beta y\right)}{u\beta^3 y}\right)$ $= \dfrac{\alpha x(\alpha^2+\beta^2)}{\beta y} \neq 0$ since $x \neq 0$ and $\alpha(\alpha^2+\beta^2) \neq 0$.
  - if $\overline{r} = \alpha\sqrt{\dfrac{\alpha x}{u\beta(y(\alpha^2+\beta^2)-\alpha\beta x)}}$, then $\alpha^2 + u\beta^2\overline{r}^2 = \alpha^2 + u\beta^2\left(\dfrac{\alpha^2(\alpha x)}{u\beta\left(y(\alpha^2+\beta^2)-\alpha bx\right)}\right)$ $= \dfrac{\alpha^2 y(\alpha^2+\beta^2)}{y(\alpha^2+\beta^2)-\alpha\beta x} \neq 0$ since $y \neq 0$ and $\alpha(\alpha^2+\beta^2) \neq 0$.

Hence we have showed that $\overline{r}$ is well-defined and that $\overline{r} \in R \setminus \{0\}$. Then $\phi_{\alpha,\beta}(\overline{r}) = (x, y)$ follows from the following proof.

(ii) As previously, we consider two cases:

- First case: $x = -\sqrt{z} \notin \sqrt{\mathbb{F}_q^2}$ and $\overline{r} = \dfrac{1}{\beta}\sqrt{\dfrac{\alpha(x(\alpha^2+\beta^2)-\alpha\beta y)}{u\beta y}}$. Since $\overline{r} \in R \setminus \{0\}$, we can define $\overline{v}, \overline{\varepsilon}, \overline{t}, \overline{x}$ and $\overline{y}$ from $\overline{r}$ as in theorem 3. We have:

$$\overline{v} = \frac{\beta(\alpha^2+u\beta^2\overline{r}^2)}{\alpha(\alpha^2+\beta^2)} = \frac{\beta}{\alpha(\alpha^2+\beta^2)}\left(\alpha^2 + \frac{\alpha\left(x(\alpha^2+\beta^2)-\alpha\beta y\right)}{\beta y}\right) = \frac{\alpha x(\alpha^2+\beta^2)}{\alpha y(\alpha^2+\beta^2)} = \frac{x}{y}.$$

$$\overline{\varepsilon} = \chi\left(\frac{\overline{v}(\alpha\overline{v}-\beta)}{\alpha-\beta\overline{v}}\right) = \chi\left(\frac{\frac{x}{y}(\alpha\frac{x}{y}-\beta)}{\alpha-\beta\frac{x}{y}}\right) = \chi\left(\frac{x(\alpha x-\beta y)}{y(\alpha y-\beta x)}\right)$$

But from the curve equation we know that $\dfrac{\alpha x-\beta y}{\alpha y-\beta x} = xy$; so $\overline{\varepsilon} = \chi(x^2) = 1$.

Then $\overline{t} = \overline{v} = \dfrac{x}{y} = t$, $\overline{x} = -\sqrt{\dfrac{\overline{t}(\alpha\overline{t}-\beta)}{\alpha-\beta\overline{t}}} = -\sqrt{\dfrac{t(\alpha t-\beta)}{\alpha-\beta t}} = -\sqrt{z} = x$ and $\overline{y} = \dfrac{\overline{x}}{\overline{t}} = \dfrac{x}{t} = y$. Hence we conclude that $\phi'(\overline{r}) = (\overline{x}, \overline{y}) = (x, y)$.

- Second case: $x = \sqrt{z} \in \sqrt{\mathbb{F}_q^2}$ and $\overline{r} = \alpha\sqrt{\dfrac{\alpha x}{u\beta(y(\alpha^2+\beta^2)-\alpha\beta x)}}$. Since $\overline{r} \in R \setminus \{0\}$, we can define $\overline{v}, \overline{\varepsilon}, \overline{t}, \overline{x}$ and $\overline{y}$ from $\overline{r}$ as in theorem 3. We have:

$$\overline{v} = \frac{\beta(\alpha^2+u\beta^2\overline{r}^2)}{\alpha(\alpha^2+\beta^2)} = \frac{\beta}{\alpha(\alpha^2+\beta^2)}\left(\alpha^2 + \frac{\alpha^3\beta x}{y(\alpha^2+\beta^2)-\alpha\beta x}\right) = \frac{\alpha\beta y}{y(\alpha^2+\beta^2)-\alpha\beta x}.$$

$$\begin{aligned}
\overline{\varepsilon} &= \chi\left(\frac{\overline{v}(\alpha\overline{v}-\beta)}{\alpha-\beta\overline{v}}\right) = \chi\left(\frac{\frac{\alpha\beta y}{y(\alpha^2+\beta^2)-\alpha\beta x}\left(\frac{\alpha^2\beta y}{y(\alpha^2+\beta^2)-\alpha\beta x}-\beta\right)}{\alpha-\frac{\alpha\beta^2 y}{y(\alpha^2+\beta^2)-\alpha\beta x}}\right) \\
&= \chi\left(\frac{\beta^3 y(\alpha x-\beta y)}{\alpha(\alpha y-\beta x)\left(y(\alpha^2+\beta^2)-\alpha\beta x\right)}\right) = \chi\left(\frac{\beta^3 x y^2}{\alpha\left(y(\alpha^2+\beta^2)-\alpha\beta x\right)}\right) \\
&= \chi\left(\alpha\beta x\left(y(\alpha^2+\beta^2)-\alpha\beta x\right)\right) = -1 \text{ since } \chi\left(u\alpha\beta x y(\alpha^2+\beta^2-\alpha\beta\frac{y}{x})\right) = 1.
\end{aligned}$$

$\overline{\varepsilon} = -1$ implies that $\overline{t} = \dfrac{\overline{v}(\alpha^2+\beta^2)-\alpha\beta}{\alpha\beta\overline{v}} = \dfrac{\frac{\alpha\beta y(\alpha^2+\beta^2)}{y(\alpha^2+\beta^2)-\alpha\beta x}-\alpha\beta}{\frac{\alpha^2\beta^2 y}{y(\alpha^2+\beta^2)-\alpha\beta x}} = \dfrac{x}{y} = t$. So $\overline{x} = \sqrt{\dfrac{\overline{t}(\alpha\overline{t}-\beta)}{\alpha-\beta\overline{t}}} = \sqrt{\dfrac{t(\alpha t-\beta)}{\alpha-\beta t}} = \sqrt{z} = x$ and $\overline{y} = \dfrac{\overline{x}}{\overline{t}} = \dfrac{x}{t} = y$.

Hence we conclude that $(x, y) \in \mathrm{Im}(\phi_{\alpha,\beta})$.

Efficiency of $\phi_{\alpha,\beta}$ and $\phi^{-1}_{\alpha,\beta}$: For any $r \in R$, computing $\phi_{\alpha,\beta}(r)$ takes 2 inversions, 1 square-root computation, one computation of the quadratic character χ and some multiplications. One can use Euclid's algorithm to compute the inverses; note that the computation of χ can be replaced by an exponentiation (with exponent $(q-1)/2$); and if $q \equiv 3 \mod 4$, the square-root computation is also replaced by an exponentiation. Inverting $\phi_{\alpha,\beta}$ takes one essential exponentiation, the square-root computation to obtain $\overline{r}$, and one inversion.

Extending $\phi_{\alpha,\beta}$: We can extend the definition of $\phi_{\alpha,\beta}$ on $\mathbb{F}_q$ as follows:

(i) if $q \equiv 1 \mod 4$: we have $R = \mathbb{F}_q^*$. Define the function $\overline{\phi_{\alpha,\beta}}$ by $\overline{\phi_{\alpha,\beta}}(r) = \phi_{\alpha,\beta}(r)$ if $r \in R$, and $\overline{\phi_{\alpha,\beta}}(0) = (0, 0)$.

(ii) if $q \equiv 3 \mod 4$: We choose $u = -1$; then we have $R = \mathbb{F}_q^* \setminus \left\{\pm\dfrac{\alpha}{\beta}\right\}$. If in addition $\alpha^2 + \beta^2$ is not a square, define the function $\overline{\phi_{\alpha,\beta}}$ by:

- $\overline{\phi_{\alpha,\beta}}(r) = \phi_{\alpha,\beta}(r)$ if $r \in R$;
- $\overline{\phi_{\alpha,\beta}}(r) = \left(\dfrac{\beta\sqrt{-(\alpha^2+\beta^2)}}{\alpha^2}, \dfrac{\beta^2\sqrt{-(\alpha^2+\beta^2)}}{\alpha(\alpha^2+\beta^2)}\right)$ if $r = \pm\dfrac{\alpha}{\beta}$;
- $\overline{\phi_{\alpha,\beta}}(0) = (0, 0)$.

We call $\overline{\phi_{\alpha,\beta}}$ the **AIEE-For-Huff**.

3.3. An AIIE for the classical Edwards model $x^2 + y^2 = 1 + dx^2y^2$

With Elligator-2's method [4], to encode on Edwards curves, it is necessary to use a birational equivalence. In this section, we propose an algorithm which encodes directly an element of $\mathbb{F}_q$ to a point of an Edwards curves $E_d : x^2 + y^2 = 1 + dx^2y^2$, where d is not a square, and without any birational equivalence.

Theorem 4. *Let q be an odd prime power, and $d \in \mathbb{F}_q^*$ such that $d \neq \pm 1, -2$ and d is not a square. Let u be a nonzero non-square and let R be a subset of $\mathbb{F}_q$ defined by $R = \{r \in \mathbb{F}_q^* : ur^2 + 1 \neq 0,\ ur^2(1-d) - (1+3d) \neq 0,\ ur^2(1+3d) - (1-d) \neq 0\}$.*
For any non-zero $r \in R$, the following elements are well-defined:

$$v = \frac{(d-1)ur^2 - 3 - d}{ur^2(d-1) + 1 + 3d}; \qquad \varepsilon = \chi[(1-v^2)(1-dv^2)];$$
$$x = \frac{\varepsilon(v+1)(dv+1) + dv^2 - 1}{2d(v+1) + (1-d)}; \qquad y = -\varepsilon\sqrt{\frac{1-x^2}{1-dx^2}}.$$

Furthermore, $\varepsilon \neq 0$ and $x^2 + y^2 = 1 + dx^2y^2$.

Proof.

(i) v is well-defined by the definition of the set R.

(ii) Since d is not a square, then ε is well-defined. Now let us show that $\varepsilon \neq 0$. Suppose that $1-v=0$; this implies that $ur^2(d-1)+3d+1-(d-1)ur^2+3+d=0 \Rightarrow d=-1$; impossible by our hypothesis on d. Suppose that $1+v=0$; thus $ur^2(d-1)+d-1=0$ and $ur^2+1=0$. This is impossible by the definition of the set R. Finally ε is well-defined and is non-zero.

(iii) x is well-defined when $2d(v+1)+1-d \neq 0$. Suppose that $2d(v+1)+1-d=0$; this implies that $2d(d-1)ur^2-2d(3+d)+2dur^2(d-1)+2d(1+3d)+ur^2(1-d)(d-1)+(1-d)(1+3d)=0 \Rightarrow 4dur^2(d-1)-ur^2(d-1)^2-4d(1-d)+(1-d)(1+3d)=0 \Rightarrow (d-1)\left(4dur^2-ur^2(d-1)+4d-1-3d\right)=0$. This leads to $ur^2(1+3d)+(d-1)=0$, which contradicts the definition of R.

(iv) y is well-defined when $1-dx^2 \neq 0$ and $\chi\left(\frac{1-x^2}{1-dx^2}\right)=1$. At first, recall that d is not a square by hypothesis; so $1-dx^2 \neq 0$. Now let us show that $\dfrac{1-x^2}{1-dx^2}$ is a non-zero square. For this, we must consider two cases:

- If $\varepsilon=1$, then $x=v$ and $\chi\left(\frac{1-x^2}{1-dx^2}\right)=\chi\left(\frac{1-v^2}{1-dv^2}\right)=\varepsilon=1$.
- If $\varepsilon=-1$, then $x=\frac{-(v+1)(d+1)+(d-1)}{2d(v+1)+(1-d)}$. Let $H(x)=\frac{1-x^2}{1-dx^2}=\frac{(1-x)(1+x)}{1-dx^2}$. Our objective now is to write $\chi(H(x))$ in function of $\chi(H(v))$, and then use the fact that $\chi(H(v))=\varepsilon=-1$. First we compute $1-x, 1+x, 1-dx^2$ and find:
  $[2d(v+1)+(1-d)](1+x)=(v+1)(d-1)$;
  $[2d(v+1)+(1-d)](1-x)=(v+1)(3d+1)+2(1-d)$;
  and $[2d(v+1)+(1-d)]^2(1-dx^2)=(d-1)^2(1-dv^2)$.
  Then $H(x)=\dfrac{(1-x)(1+x)}{1-dx^2}=\dfrac{((v+1)(3d+1)+2(1-d))\cdot[(v+1)(d-1)]}{(d-1)^2(1-dv^2)}$
  $=\dfrac{(v+1)[(v+1)(3d+1)+2(1-d)]}{(d-1)(1-dv^2)}=\dfrac{H(v)}{1-v}\left(\dfrac{(v+1)(3d+1)+2(1-d)}{d-1}\right)$,
  where $H(v)=(1-v)(1+v)/(1-dv^2)$. Replace v by its value to see that:
  $(v+1)(1+3d)+2(1-d)=\dfrac{2(d-1)[(1+ur^2)(1+3d)-ur^2(d-1)-(1+3d)]}{ur^2(d-1)+(1+3d)}$
  and $(1-v)(d-1)=\dfrac{4(d+1)(d-1)}{ur^2(d-1)+(1+3d)}$; so $\frac{(v+1)(3d+1)+2(1-d)}{(1-v)(d-1)}=ur^2$.
  Since $r\neq 0$ in R, then $\chi(H(x))=\chi(H(v))\cdot\chi(ur^2)=1$ as desired.

Hence $(1-x^2)/(1-dx^2)$ is a non-zero square and y is well-defined. Moreover (x,y) verifies $x^2+y^2=1+dx^2y^2$.

Definition 2. *In the situation of theorem 4, the encoding function for the Edwards curve* $E_d:\ x^2+y^2=1+dx^2y^2$ *is the function* $\phi_d:\ R\to E_d : r\mapsto \phi_d(r)=(x,y)$.

The following proposition characterizes the image set of the function ϕ_d.

Proposition 7. *(i) For $r \in R$, the set of preimages of $\phi_d(r)$ is $\{-r, r\}$.*

(ii) $\mathrm{Im}(\phi_d)$ *is the set of* $(x, y) \in E_d$ *such that* $1 - x^2 \neq 0$, $x \neq \dfrac{-(d+1)}{2d}$ *and* $\chi[u(d-1)(1-x)(x(3d+1)+d+3)] = 1$.

(iii) Let $(x, y) \in \mathrm{Im}(\phi_d)$ *and define* $\overline{r}$ *as follows:*

$\overline{r} = \sqrt{\dfrac{x(3d+1)+d+3}{u(d-1)(1-x)}}$, *if* $y \notin \sqrt{\mathbb{F}_q^2}$, *and* $\overline{r} = \sqrt{\dfrac{(d-1)(1-x)}{u[x(3d+1)+d+3)]}}$, *if* $y \in \sqrt{\mathbb{F}_q^2}$. *Then* $\overline{r} \in R$ *and* $\phi_d(\overline{r}) = (x, y)$.

Proof.

(i) It is obvious that $\phi_d(-r) = \phi_d(r)$ since the definition of ϕ_d only uses r^2. Now let $r' \in R$ such that $\phi_d(r') = \phi_d(r)$. We want to show that $r' = r$ or $r' = -r$.
From r' we define the elements $v', \varepsilon', t', x', y'$ as in theorem 4. So $\phi_d(r') = \phi_d(r) \Rightarrow x' = x$ and $y' = y$. Thus we have $-\varepsilon'\sqrt{\frac{(1-x^2)}{1-dx^2}} = -\varepsilon\sqrt{\frac{(1-x^2)}{1-dx^2}}$. So $\varepsilon' = \varepsilon$; and we have $v' = v$ by replacing ε' by ε in $x' = x$. Finally $v = v'$ implies that $r'^2 = r^2$, that is $r' = \pm r$.

(ii) Forward part: Let $(x, y) \in \mathrm{Im}(\phi_4)$, we need to show $1 - x^2 \neq 0$, $x \neq -\frac{d+1}{2d}$ and $\chi[u(d-1)(1-x)(x(3d+1)+d+3)] = 1$. Since $(x, y) \in \mathrm{Im}(\phi_4)$, then there exists $r \in R$ such that $\phi_4(r) = (x, y)$. From r, define v and ε as in theorem 4.

If $\varepsilon = 1$, then $x = v = \dfrac{(d-1)ur^2 - 3 - d}{ur^2(d-1) + 1 + 3d}$. We have $1 + x = \dfrac{2(d-1)(ur^2+1)}{ur^2(d-1)+1+3d}$, $1 - x = \dfrac{4(d+1)}{ur^2(d-1)+1+3d}$ and $x + \frac{d+1}{2d} = \dfrac{(d-1)[(3d+1)ur^2 + d - 1]}{2d[(d-1)ur^2 + 1 + 3d]}$, thus $1 + x \neq 0$, $1 - x \neq 0$ and $x \neq -\frac{d+1}{2d}$, by definition of R. Moreover, we have $x(3d+1) + d + 3 = \dfrac{4ur^2(d-1)(d+1)}{ur^2(d-1)+1+3d}$; hence $u(d-1)(1-x)(x(3d+1)+d+3) = \dfrac{16u^2r^2(d-1)^2(d+1)^2}{(ur^2(d-1)+1+3d)^2}$ which is a nonzero square by definition of R, as desired.

If $\varepsilon = -1$, then $x = \dfrac{-(v+1)(d+1)+(d-1)}{2d(v+1)+(1-d)} = \dfrac{d-1-ur^2(d+3)}{ur^2(3d+1)+d-1}$. We have $1 - x = \dfrac{4ur^2(d+1)}{ur^2(3d+1)+d-1}$, $1+x = \dfrac{2(d-1)(ur^2+1)}{ur^2(1+3d)+d-1}$ and $x+\frac{d+1}{2d} = \dfrac{(d-1)[ur^2(d-1)+1+3d]}{2d[ur^2(1+3d)+d-1]}$, thus $1 + x \neq 0$, $1 - x \neq 0$ and $x \neq -\frac{d+1}{2d}$, by definition of R. Moreover, we have $x(3d+1) + d + 3 = \dfrac{4(d-1)(d+1)}{ur^2(3d+1)+d-1}$; hence $u(d-1)(1-x)(x(3d+1)+d+3) = \dfrac{16u^2r^2(d-1)^2(d+1)^2}{(ur^2(d-1)+1+3d)^2}$, which is a nonzero square by definition of R, as desired.

Reverse part: Let $(x,y) \in E_d$ such that $1-x^2 \neq 0$, $x \neq -\frac{d+1}{2d}$ and $\chi[u(d-1)(1-x)(x(3d+1)+d+3)] = 1$. We want to show that $(x,y) \in \mathrm{Im}(\phi_d)$. For this, we consider the cases where $y = -\sqrt{(1-x^2)/(1-dx^2)}$ and where $y = \sqrt{(1-x^2)/(1-dx^2)}$.

- If $y = -\sqrt{(1-x^2)/(1-dx^2)}$, put $\overline{r} = \sqrt{\frac{x(3d+1)+d+3}{u(d-1)(1-x)}}$ then $\overline{r}$ is well defined.
  First we need to show that $\overline{r} \in R$. We have:
  - $\overline{r} \neq 0$, since $\chi[u(d-1)(1-x)(x(3d+1)+d+3)] = 1$,
  - $u\overline{r}^2 + 1 = 0 \Rightarrow 1+x = 0$ which is impossible,
  - $u\overline{r}^2(1-d) - (1+3d) = 0 \Rightarrow 4(d-1)(d+1) = 0$ which is impossible,
  - $u\overline{r}^2(1+3d) - (1-d) = 0 \Rightarrow x = -\frac{d+1}{2d}$ which is impossible.

  Now, from $\overline{r}$, define $\overline{v}, \overline{\varepsilon}, \overline{x}$ and $\overline{y}$ as in theorem 4. Our objective is to show that $\overline{x} = x$ and $\overline{y} = y$.
  From $(d-1)u\overline{r}^2 - (3+d) = 4x(d+1)/(1-x)$ and $u\overline{r}^2(d-1) + (1+3d) = 4(d+1)/(1-x)$, we deduce $\overline{v} = x$. So $\overline{\varepsilon} = \chi\left(\frac{1-x^2}{1-dx^2}\right) = 1$ and $\overline{x} = \overline{v} = x$. Finally we have $\overline{y} = -\overline{\varepsilon}\sqrt{\frac{1-x^2}{1-dx^2}} = y$.

- If $y = \sqrt{(1-x^2)/(1-dx^2)}$, put $\overline{r} = \sqrt{\frac{(d-1)(1-x)}{u[x(3d+1)+d+3)]}}$, then $\overline{r}$ is well defined.
  As for previous case, first, we need to prove that $\overline{r} \in R$. We have:
  - $\overline{r} \neq 0$, since $\chi[u(d-1)(1-x)(x(3d+1)+d+3)] = 1$,
  - $u\overline{r}^2 + 1 = 0 \Rightarrow 1+x = 0$ which is impossible,
  - $u\overline{r}^2(1-d) - (1+3d) = 0 \Rightarrow x = -\frac{d+1}{2d} = 0$ which is impossible,
  - $u\overline{r}^2(1+3d) - (1-d) = 0 \Rightarrow 4(d-1)(d+1) = 0$ which is impossible.

  Now let us define $\overline{v}, \overline{\varepsilon}, \overline{x}$ and $\overline{y}$ from $\overline{r}$. Replacing $\overline{r}$ by its value in $\overline{v}$, we find $\overline{v} = \dfrac{-2-x(d+1)}{d+1+2dx}$ and $\dfrac{1-\overline{v}^2}{1-d\overline{v}^2} = \dfrac{(d-1)(1+x)(x(1+3d)+d+3)}{(d-1)^2(1-dx^2)} = \left(\dfrac{(1+x)(1-x)}{1-dx^2}\right)\left(\dfrac{(x(1+3d)+d+3)}{(d-1)(1-x)}\right)$.
  Recall that (x,y) is in E_d and that $\chi\left(\dfrac{(x(1+3d)+d+3)}{(d-1)(1-x)}\right) = -1$ by hypothesis, thus $\overline{\varepsilon} = -1$.
  From $\overline{v} = \dfrac{-2-x(d+1)}{d+1+2dx}$, we have $\overline{x} = \dfrac{-(\overline{v}+1)(d+1)+(d-1)}{2d(\overline{v}+1)+(1-d)} = x$. We deduce that $\overline{y} = -\overline{\varepsilon}\sqrt{\dfrac{1-\overline{x}^2}{1-d\overline{x}^2}} = \sqrt{\dfrac{1-x^2}{1-dx^2}} = y$. Thus $\phi_d(\overline{r}) = (x,y)$ as desired.

(iii) Follows from the previous part of the proof.

Efficiency of ϕ_d and ϕ_d^{-1}:

For any $r \in R$, computing $\phi_d(r)$ takes 3 inversions, one computation of χ, one square-root computation and some multiplications. Elligator-2 method [4] applied to Edwards

curves by using a birational equivalence, takes 5 inversions, one computation of χ, one square-root computation and some multiplications. One can use Euclid's algorithm to compute the inverses, or use an exponentiation; note that the computation of χ can be replaced by an exponentiation (with exponent $(q-1)/2$); and if $q \equiv 3 \mod 4$, the square-root computation is also replaced by an exponentiation. And as in [4], the computation of χ can be combined into the square-root computation as follows. First compute a power of $\frac{1-v^2}{1-dv^2}$ as above, obtaining a square root of $\dfrac{1-v^2}{1-dv^2}$ if $\dfrac{1-v^2}{1-dv^2}$ is a square. If the square of this power turns out to match $\dfrac{1-v^2}{1-dv^2}$ then $\varepsilon = 1$ and $x = v$. Otherwise $\varepsilon = -1$ and $\dfrac{1-x^2}{1-dx^2} = ur^2\left(\dfrac{1-v^2}{1-dv^2}\right)$ (by definition of ur^2, see proof of theorem 4); multiply the previous power by r and by a precomputed power of u to obtain a square root of $\dfrac{1-x^2}{1-dx^2}$.

Similar comments apply to computing ϕ_d^{-1}; there is one square-root computation, one inversion and few multiplications. Also note that q is not required to be congruent to 3 modulo 4 to encode all points of $\mathbb{F}_q$, as said in the next remark.

Extension of ϕ_d:

Our objective now is to extend the encoding function $\phi_d : R \to E(\mathbb{F}_q)$ to $\overline{\phi_d} : \mathbb{F}_q \to E(\mathbb{F}_q)$. For this,we put $\phi_d(r) = \overline{\phi_d}(r)\ \forall r \in R$ and we must send all points r in $\mathbb{F}_q \setminus R$ to points P in $E(\mathbb{F}_q)\setminus \mathrm{Im}(\phi_d)$ via $\overline{\phi_d}$. For constructing such a point P in $E(\mathbb{F}_q)\setminus \mathrm{Im}(\phi_d)$, we use the characterization of the encoding ϕ_d (see proposition 7). Furthermore, if $r, r' \in \mathbb{F}_q \setminus R$, with $r \neq r'$, we need to have $\overline{\phi_d}(r) \neq \overline{\phi_d}(r')$ in order to preserve the *almost*-injectivity of ϕ_d. We can extend the definition of ϕ_d on $\mathbb{F}_q$ as follows.

(i) If $\chi((1-d)(1+3d)) = 1$ then $R = \mathbb{F}_q^*$ when $q \equiv 1 \mod 4$ and $R = \mathbb{F}_q^* \setminus \{\pm\sqrt{\frac{-1}{u}}\}$ when $q \equiv 3 \mod 4$, thus we need 1 and 2 points in $E(\mathbb{F}_q) \setminus \mathrm{Im}(\phi_d)$ respectively in order to extend ϕ_4. Since $(1,0)$ and $(-1,0)$ are in $E(\mathbb{F}_q) \setminus \mathrm{Im}(\phi_d)$ by the above characterization of $\mathrm{Im}(\phi_d)$, then we propose the following:

  (a) If $q \equiv 1 \mod 4$: put $\overline{\phi_d}(0) = (1,0)$.

  (b) If $q \equiv 3 \mod 4$: put $\overline{\phi_d}(0) = (1,0)$ and $\overline{\phi}_4(\pm\sqrt{\frac{-1}{u}}) = (-1,0)$.

(ii) If $\chi((1-d)(1+3d)) = -1$ then $R = \mathbb{F}_q^* \setminus \left\{\pm\sqrt{\frac{1-d}{u(1+3d)}}, \pm\sqrt{\frac{1+3d}{u(1-d)}}\right\}$ when $q \equiv 1 \mod 4$ and $R = \mathbb{F}_q^* \setminus \left\{\pm\sqrt{\frac{-1}{u}}, \pm\sqrt{\frac{1-d}{u(1+3d)}}, \pm\sqrt{\frac{1+3d}{u(1-d)}}\right\}$ when $q \equiv 3 \mod 4$, thus we need 3 and 4 points in $E(\mathbb{F}_q) \setminus \mathrm{Im}(\phi_d)$ respectively in order to extend ϕ_4. Since $(1,0)$ and $(-1,0)$ are in $E(\mathbb{F}_q) \setminus \mathrm{Im}(\phi_d)$ by the above characterization of $\mathrm{Im}(\phi_d)$, then we need two other points in $E(\mathbb{F}_q) \setminus \mathrm{Im}(\phi_d)$. There exist different methods for doing this. We propose in the following at least two examples.

  (a) Example 1: If $\chi((d-1)(d+3)) = 1$, then $(0,1), (0,-1) \in E(\mathbb{F}_q) \setminus \mathrm{Im}(\phi_d)$, therefore, we choose:

i. $\overline{\phi_d}(0) = (1,0)$, $\overline{\phi}_4\left(\pm\sqrt{\frac{1-d}{u(1+3d)}}\right) = (0,-1)$ and $\overline{\phi}_4\left(\pm\sqrt{\frac{1+3d}{u(1-d)}}\right) = (0,1)$, when $q \equiv 1 \mod 4$.

ii. $\overline{\phi_d}(0) = (1,0)$, $\overline{\phi}_4(\pm\sqrt{-1/u}) = (-1,0)$, $\overline{\phi}_4\left(\pm\sqrt{\frac{1-d}{u(1+3d)}}\right) = (0,-1)$ and $\overline{\phi}_4\left(\pm\sqrt{\frac{1+3d}{u(1-d)}}\right) = (0,1)$ when $q \equiv 3 \mod 4$.

(b) Example 2: If $\chi(-2(1+d)) = 1$, then $\left(-\frac{d+3}{1+3d}, 2\sqrt{-2(d+1)}/(d-1)\right)$, $\left(-\frac{d+3}{1+3d}, -2\sqrt{-2(d+1)}/(d-1)\right) \in E(\mathbb{F}_q) \setminus \mathrm{Im}(\phi_d)$, therefore, we choose:

i. $\overline{\phi_d}(0) = (1,0)$, $\overline{\phi}_4\left(\pm\sqrt{\frac{1-d}{u(1+3d)}}\right) = \left(-\frac{d+3}{1+3d}, 2\sqrt{-2(d+1)}/(d-1)\right)$ and $\overline{\phi}_4\left(\pm\sqrt{\frac{1+3d}{u(1-d)}}\right) = \left(-\frac{d+3}{1+3d}, -2\sqrt{-2(d+1)}/(d-1)\right)$, when $q \equiv 1 \mod 4$.

ii. $\overline{\phi_d}(0) = (1,0)$, $\overline{\phi}_4(\pm\sqrt{-1/u}) = (-1,0)$, $\overline{\phi}_4\left(\pm\sqrt{\frac{1-d}{u(1+3d)}}\right) = \left(-\frac{d+3}{1+3d}, 2\sqrt{-2(d+1)}/(d-1)\right)$ and $\overline{\phi}_4\left(\pm\sqrt{\frac{1+3d}{u(1-d)}}\right) = \left(-\frac{d+3}{1+3d}, -2\sqrt{-2(d+1)}/(d-1)\right)$ when $q \equiv 3 \mod 4$.

We call $\overline{\phi_d}$ the **AIEE-For-Edwards**.

3.4. An AIIE for the Weierstrass model $y^2 = x^3 + ax^2 + c$

In this section, we propose an injective encoding for the the Weierstrass model $y^2 = x^3 + ax^2 + c$ with $\mathrm{char}(\mathbb{F}_q) = 3$. The encoding comes from the following algorithm.

Algorithm 2.
Input: *$a, c \in \mathbb{F}_q$ (with $\mathrm{char}(\mathbb{F}_q) = 3$) such that $\chi(-ac) = 1$, u a non-square in $\mathbb{F}_q$, $r \in \mathbb{F}_q^*$;*
Output: *A point (x, y) on $E_{a,c} : y^2 = x^3 + ax^2 + c$;*

1. $s^2 = -\dfrac{c}{a}$;

2. $v = \dfrac{ur^2 - s^2}{s}$;

3. $\varepsilon = \chi(v^3 + av^2 + c)$;

4. $x = \dfrac{v}{2}\left(1 + \dfrac{s + \varepsilon v}{s + v}\right)$;

5. $y = -\varepsilon\sqrt{x^3 + ax^2 + c}$;

6. ***Return*** (x, y);

Theorem 5. *Let $a, c \in \mathbb{F}_q$ (with $\mathrm{char}(\mathbb{F}_q) = 3$) such that $\chi(-ac) = 1$, u a non-square in $\mathbb{F}_q$ and $r \in \mathbb{F}_q^*$. Let $E_{a,c}$ be the elliptic curve defined over $\mathbb{F}_q$ by $y^2 = x^3 + ax^2 + c$. Then algorithm 2 defines a deterministic encoding $\phi_{a,c} : \mathbb{F}_q^* \to E_{a,c}$, $r \mapsto \phi_{a,c}(r) = (x, y)$.*

Proof.

(i) By hypothesis $c \neq 0$ and $a \neq 0$; so v is defined. $v = 0 \Leftrightarrow u = (r/s)^2$; contradiction since u is not a square.

(ii) $v^3 + av^2 + c \neq 0$ since $c \neq 0$. This implies that $\varepsilon \neq 0$.

(iii) Suppose that $v + s = 0$; so $ur^2 = 0$ which is impossible by our hypothesis on u and r. Thus x is defined and $x \neq 0$, since $v \neq 0$.

(iv) We show that $x^3 + bx^2 + c$ is a square. The first case is when $\varepsilon = 1$; so $x = v$ and $\chi(x^3 + ax^2 + c) = \chi(v^3 + av^2 + c) = \varepsilon = 1$. For the second case we have $\varepsilon = -1$; so $x = \dfrac{sv}{v+s}$. Recall that $as^2 = -c$, $(s+v)^3 = s^3 + v^3$ and $sv + s^2 = ur^2$. So $(v+s)^3(x^3 + ax^2 + c) = s^3v^3 + as^2v^2(v+s) + cv^3 + cs^3 = s^3(v^3 + av^2 + c)$ and then $\chi(x^3 + ax^2 + c) = \chi(s(v+s))\chi(v^3 + av^2 + c) = -\chi(sv + s^2) = -\chi(ur^2) = 1$.
Hence $x^3 + ax^2 + c$ is a non-zero square in both cases. Furthermore $y^2 = x^3 + ax^2 + c$.

Proposition 8. *In the situation of theorem 5, the following results hold:*

(i) For $r \in \mathbb{F}_q^*$, the set of preimages of $\phi_{a,c}(r)$ under $\phi_{a,c}$ is $\{-r, r\}$.

(ii) $\mathrm{Im}(\phi_{a,c})$ is the set of $(x,y) \in E_{a,c}$ such that $\chi(us(s+x)) = 1$ if $y \notin \sqrt{\mathbb{F}_q^2}$, and $\chi(us(s-x)) = 1$ if $y \in \sqrt{\mathbb{F}_q^2}$.

(iii) For $(x,y) \in \mathrm{Im}(\phi_{a,c})$, let $\overline{r}$ defined as follows:
$\overline{r} = \sqrt{(s(s+x))/u}$ if $y \notin \sqrt{\mathbb{F}_q^2}$ $\quad$ $\overline{r} = s\sqrt{s/(u(s-x))}$ if $y \in \sqrt{\mathbb{F}_q^2}$.

Then $\phi_{a,c}(\overline{r}) = (x,y)$.

Proof.

(i) Same proof as proof of proposition 5.

(ii) **Forward part**: we show that any $(x,y) \in \mathrm{Im}(\phi_{a,c})$ verifies $\chi(us(s+x)) = \chi(us(s-x)) = 1$. In fact, let $r \in \mathbb{F}_q^*$ such that $\phi_{a,c}(r) = (x,y)$; and define v, ε from r. If $\varepsilon = 1$, then $x = v$; so $us(s+x) = us(s+v) = us\left(s + \dfrac{ur^2 - s^2}{s}\right) = u^2r^2$. Thus $\chi(us(s+x)) = 1$. If $\varepsilon = -1$, then $x = \dfrac{sv}{s+v}$; so $us(s-x) = us\left(s - \dfrac{sv}{s+v}\right) = \dfrac{us^3}{s+v} = us^3\left(\dfrac{1}{s + \frac{ur^2 - s^2}{s}}\right) = \dfrac{s^4}{r^2}$. Thus $\chi(us(s-x)) = 1$.
Reverse part: let $(x,y) \in E_{a,c}$ such that $\chi(us(s-x))$(if $y = \sqrt{x^3 + ax^2 + c}$) or $\chi(us(s+x)) = 1$(if $y = -\sqrt{x^3 + ax^2 + c}$). We show that $(x,y) \in \mathrm{Im}(\phi_{a,c})$.
We consider the following two cases:

- if $y = -\sqrt{x^3 + ax^2 + c}$, let $\overline{r} = \sqrt{s(s+x)/u} \neq 0$; then define $\overline{v}, \overline{\varepsilon}, \overline{x}, \overline{y}$ from $\overline{r}$ as in theorem 6. So $\overline{v} = \dfrac{u\overline{r}^2 - s^2}{s} = \dfrac{s(s+x) - s^2}{s} = x$ and $\overline{\varepsilon} = \chi(\overline{v}^3 + a\overline{v}^2 + c) = \chi(x^3 + ax^2 + c) = 1$. This implies that $\overline{x} = \overline{v} = x$ and $\overline{y} = -\overline{\varepsilon}\sqrt{\overline{x}^3 + a\overline{x}^2 + c} = -\sqrt{x^3 + ax^2 + c} = y$. Hence $(\phi_{a,c})(\overline{r}) = (x, y)$ and $(x, y) \in \mathrm{Im}(\phi_{a,c})$.
- if $y = \sqrt{x^3 + ax^2 + c}$, let $\overline{r} = s\sqrt{s/(u(s-x))} \neq 0$ since $us(s-x)$ is a non-zero square. So define $\overline{v}, \overline{\varepsilon}, \overline{x}, \overline{y}$ from $\overline{r}$ as in theorem 6. We then have $\overline{v} = \dfrac{u\overline{r}^2 - s^2}{s} = \dfrac{\frac{s^3}{s-x} - s^2}{s} = \dfrac{sx}{s-x}$. Recall that $as^2 = -c$ and $(s-v)^3 = s^3 - v^3$; so $(s-x)^3(\overline{v}^3 + a\overline{v}^2 + c) = s^3x^3 + as^2x^2(s-x) + c(s^3 - x^3) = s^3(x^3 + ax^2 + c) \Rightarrow \overline{\varepsilon} = \chi(\overline{v}^3 + a\overline{v}^2 + c) = \chi(s(s-x)) = -1$ since $\chi(us(s-x)) = 1$ by hypothesis, and $\chi(u) = -1$. Now replacing $\overline{\varepsilon}$ by -1 and $\overline{v}$ by $\dfrac{sx}{s-x}$ in $\overline{x}$ shows that $\overline{x} = x$. Furthermore we have $\overline{y} = -\overline{\varepsilon}\sqrt{\overline{x}^3 + a\overline{x}^2 + c} = \sqrt{x^3 + ax^2 + c} = y$ and we conclude that $(x, y) \in \mathrm{Im}(\phi_{a,c})$.

(iii) Follows from the proof of the second statement.

Extending $\phi_{a,c}$: As above, if f has a root, then we can use Elligator-2 method [4]. For this case also, suppose that $f(x) = x^3 + ax^2 + c \neq 0,\ \forall x \in \mathbb{F}_q$. Then $R = \mathbb{F}_q^*$. We propose here to extend $\phi_{a,c}$ to $\mathbb{F}_q$. Let $\overline{\phi_{a,c}} : \mathbb{F}_q \to E(\mathbb{F}_q)$ defined as follows:

- $\overline{\phi_{a,c}}(r) = \phi_{a,c}(r) = (x, y)$ if $r \in R = \mathbb{F}_q^*$;
- for $r = 0$, let $d \in \mathbb{F}_q$ and put $c = \dfrac{-(d^2 - a^3 + a)^2}{a^5}$. Then $-ac$ is a square and $f(s) = \dfrac{s^2d^2}{a^2}$ is also a square. We use this result to extend $\phi_{a,c}$ as follows: $\overline{\phi_{a,c}}(0) = \left(s, \sqrt{f(s)}\right)$.

We call $\overline{\phi_{a,c}}$ the **AIEE-For-WeierstrassChar3**.

4. Hashing into elliptic curves

Brier *et al.* [6] showed that the construction $H(m) = f(h_1(m)) + f(h_2(m))$ is indifferentiable from a random oracle, where f is the Icart's encoding [9] and the h_1, h_2 are modeled as random oracles. To show the indifferentiability, they bounded the statistical distance between the distribution defined by their construction and the uniform distribution. Farashahi *et al.* [14] generalized the result of Brier *et al.* to all known deterministic encodings to elliptic (and hyperelliptic curves). In fact, they showed that given a deterministic encoding f, the construction $H(m) = f(h_1(m)) + \ldots f(h_s(m))$ is indifferentiable from a random oracle, if the h_i are modeled as random oracles and s is strictly greater than the genus of the target curve. Our objective here is to apply these results to one of our encodings, namely the encoding ϕ_d for the Edwards curve $x^2 + y^2 = 1 + dx^2y^2$.

4.1. Admissible and well-distributed encodings

We recall the following definitions and theorems from [14] and [17].

Definition 3. *Let S, R be two finite sets and F a function from S to R. Then F is an ε-admissible encoding if it satisfies the following properties:*

(i) computable, that is F is computable in deterministic polynomial time;

(ii) regular: for s uniformly distributed in S, the distribution of $F(s)$ is ε-statistically indistinguishable from the uniform distribution in R;

(iii) samplable: there is an efficient randomized algorithm I such that for any $r \in R$, $I(r)$ induces a distribution that is ε-statistically indistinguishable from the uniform distribution in $F^{-1}(r)$.

F is an admissible encoding if ε is a negligible function of the security parameter.

Definition 4. *Let E be an elliptic curve over $\mathbb{F}_q$ and a function $\phi : \mathbb{F}_q \to E(\mathbb{F}_q)$.*

*(i) ϕ is a B-**well-distributed encoding** for a certain constant $B > 0$, if for any nontrivial character ξ of $E(\mathbb{F}_q)$, the following holds: $\left|\sum_{r\in\mathbb{F}_q} \xi(\phi(r))\right| \leq B\sqrt{q}$. If B doesn't depend on the security parameter (that allows to chose q) then ϕ is said to be **well-distributed**.*

(ii) ϕ is a (d, B)-well-bounded encoding, for positive constants d, B, if ϕ is B-well-distributed and each point in $E(\mathbb{F}_q)$ have at most d preimages under ϕ.

Theorem 6.
Let $h : \mathcal{T} = \mathcal{T}(\mathbb{F}_q) \to E = E(\mathbb{F}_q)$ be a non constant morphism of curves, and ξ be any nontrivial character of $E(\mathbb{F}_q)$. Assume that h does not factor through a nontrivial unramified morphism $\mathcal{Z} \to E$, then

$$\left|\sum_{P\in\mathcal{T}} \xi(h(P))\right| \leq (2\widehat{g} - 2)\sqrt{q}$$

, where $\widehat{g}$ is the genus of $\mathcal{T}$. Furthermore, if q is odd and λ is a non constant rational function on $\mathcal{T}$, we have

$$\left|\sum_{P\in\mathcal{T}} \xi(h(P))\chi(\lambda(P))\right| \leq (2\widehat{g} - 2 + 2\deg\lambda)\sqrt{q}$$

4.2. Indifferentiable Hashing

Let E be a curve with a $\mathbb{F}_q$-rational point and J be its jacobian.

Theorem 7. *[14]*
If $f : \mathbb{F}_q \to E(\mathbb{F}_q)$ is a B-well-distributed encoding into E, then the statistical distance between the distribution defined by the construction $(u_1, \ldots, u_s) \mapsto f(u_1) \ldots f(u_s)$ on $J(\mathbb{F}_q)$ and the uniform distribution is bounded as follows:

$$\sum_{D \in J(\mathbb{F}_q)} \left| \frac{N_s(D)}{q^s} - \frac{1}{\#J(\mathbb{F}_q)} \right| \leq \frac{B^s}{q^{s/2}} \sqrt{\#J(\mathbb{F}_q)}$$

where $N_s(D) = \#\{(u_1, \ldots u_s \in (\mathbb{F}_q)^s : \ f(u_1) + \ldots f(u_s) = D\}$ for $D \in J(\mathbb{F}_q)$.

As said in [14], this theorem shows that f is a well-distributed encoding and if s is greater than the genus of the curve, the distribution of the new construction is statistically indistinguishable from the uniform distribution. Moreover, it is admissible if f is also computable and samplable, and the hash function $m \mapsto f(h_1(m)) + \ldots + f(h_s(m))$ is indifferentiable from a random oracle if the $h_1, \ldots, h_s$ are modeled as random oracles into $\mathbb{F}_q$.

4.3. Application to the encoding ϕ_d

In this section, we apply the results and proofs of Farashahi *et al.* [14] (for the Shallue-Woestijne-Ulas encoding) to one of our previous encodings. We will show that the encoding ϕ_d over the Edwards curve $x^2 + y^2 = 1 + dx^2y^2$ when $q \equiv 3 \mod 4$ is well-distributed, and thus give rise to a indifferentiable hash function construction.

Recall that ϕ_d is an efficient *almost*-injective and invertible encoding from the subset $R = \{r \in \mathbb{F}_q^* : ur^2 + 1 \neq 0, \ ur^2(1-d) - (1+3d) \neq 0, \ ur^2(1+3d) - (1-d) \neq 0\}$ to the elliptic curve $E_d : \ x^2 + y^2 = 1 + dx^2y^2$, and let $\Omega = \mathbb{F}_q \setminus R$. By the invertibility of ϕ_d, we know that for $(x, y) \in \mathrm{Im}(\phi_d)$, there exists two preimages $r, -r$ such that $\phi_d(\pm r) = (x, y)$. When $q = 3 \mod 4$, we have:

$y = \sqrt{\dfrac{1-x^2}{1-dx^2}} \Rightarrow \chi_q(y) = 1$ and $y = -\sqrt{\dfrac{1-x^2}{1-dx^2}} \Rightarrow \chi_q(y) = -1$. Thus:

- $\chi_q(y) = -1 \Leftrightarrow r^2 = \dfrac{(d-1)(1-x)}{u[x(3d+1)+d+3)]}$ $\qquad$ Eq $-$ (0)

- $\chi_q(y) = 1 \Leftrightarrow r^2 = \dfrac{x(3d+1)+d+3}{u(d-1)(1-x)}$ $\qquad$ Eq $-$ (1).

From now, the proof is similar to the one of of Farashahi *et al* (in [14] subsection 5.3).

By equation Eq $-$ (1), we define the coverings $h_i : \mathcal{C}_i \to E$, $i = 0, 1$, by the smooth projective curve whose function fields (denoted $\mathbb{F}_q(x, y, r)$) is the extension of $\mathbb{F}_q(x, y)$ given by Eq $-$ (i).

Since r is a rational function on C_i, we have a morphism $f_i : C_i \to \mathbb{P}^1$, such that any point in $\mathbb{A}^1(\mathbb{F}_q) \setminus \Omega$ has exactly two preimages in $\mathcal{C}_i$ for one of $i = 0, 1$, and none in

the other. Since $q = 3 \mod 4$, then these two preimages are conjugate under $y \to -y$. Therefore, exactly one of them satisfies $\chi_q(y) = (-1)^i$. Let $P \in C_i$ be that preimage; so $\phi_d(u) = h_i(P)$.

Theorem 8. *For any nontrivial character ξ of $E_d(\mathbb{F}_q)$, the following holds when $q \equiv 3 \mod 4$:*

$$\left| \sum_{r \in \mathbb{F}_q} \xi(\phi_d(r)) \right| \leq 12\sqrt{q} + 31.$$

Proof. Let $r \in R$, $\Omega = \mathbb{F}_q \setminus R$ and $h_i : C_i \to E_d$ $(i = 0, 1)$ defined as previously; also define $\Omega_i = \{P \in C_i : \ f_i(P) \in \Omega\}$. So we can write:

$$\sum_{r \in R} \xi(\phi_d(r)) = \sum_{P \in C_0(\mathbb{F}_q) \setminus \Omega_0, \ \chi(y) = +1} \xi(h_0(P)) + \sum_{P \in C_1(\mathbb{F}_q) \setminus \Omega_1, \ \chi(y) = -1} \xi(h_1(P)) \quad (*).$$

Also observe that:

$$\frac{1}{2} \sum_{P \in C_i(\mathbb{F}_q), \ \chi(y) = 0} \xi(h_i(P)) + \sum_{P \in C_i(\mathbb{F}_q), \ \chi(y) = (-1)^i} \xi(h_i(P)) = \sum_{P \in C_i(\mathbb{F}_q)} \xi(h_i(P)) \cdot \left(\frac{1 + (-1)^i \chi(y)}{2} \right). \quad (**)$$

One can see that the first term of the left-hand side of this equality contains at most $2 \cdot 2 = 4$ terms, when expressing y^2 in terms of x and by $\mathrm{Eq} - (0)$ and $\mathrm{Eq} - (1)$.
To estimate the right-hand side of the equality, one can use theorem 6. In fact, by Eiseinstein criterion, h_0 and h_1 are totally ramified over points such that $x = \dfrac{-d-3}{3d+1}$; so they cannot factor through any unramified covering of E_d. Hence, applying theorem 6, we have:

$$\sum_{P \in C_i(\mathbb{F}_q)} \xi(h_i(P)) \cdot \left(\frac{1 + (-1)^i \chi(y)}{2} \right) \leq (2g_i - 2 + \deg(y))\sqrt{q}$$

where g_i is the genus of C_i and $\deg(y)$ is the degree of y seen as a rational function on C_i. Denote by e_P the ramification index at P and by d_i the degree of h_i; since the h_i are ramified only at $x = \dfrac{-d-3}{3d+1}$, then by the Riemann-Hurwitz formula and using the fact that any point has two conjugate preimages, we have $2g_i - 2 = d_i(2g_{E_d} - 2) + \sum_{P \in C_i}(e_P - 1) = d_i(2 \cdot 1 - 2) + 2(2 - 1) + \sum_{P \in C_i, x \neq -t} (e_P - 1) = 0 + 2 + 0 = 2$. Hence C_i is a curve of genus $g_i = 2$.

On the other side, we have $\deg(y) = [\mathbb{F}_q(x, y, r) : \mathbb{F}_q(x, y)] \cdot [\mathbb{F}_q(x, y) : \mathbb{F}_q(y)] = 2 \cdot 2 = 4$. Finally, we have:

$$\sum_{P \in C_i(\mathbb{F}_q)} \xi(h_i(P)) \cdot \left(\frac{1 + (-1)^i \chi(y)}{2} \right) \leq (2 \cdot 2 - 2 + 4)\sqrt{q} = 6\sqrt{q}.$$

Now it follows from **(*)** and **(**)** that:
$\left|\sum_{r\in R}\xi(\phi_d(r))\right| = 2\cdot\left[\sum_{P\in C_i(\mathbb{F}_q)}\xi(h_i(P))\cdot\left(\frac{1+(-1)^i\chi(y)}{2}\right) - \frac{1}{2}\sum_{P\in C_i(\mathbb{F}_q),\ \chi(y)=0}\xi(h_i(P))\right] + \#\Omega_0 + \#\Omega_1 \leq$
$2(6\sqrt{q}-2) + \#\Omega_0 + \#\Omega_1 = 12\sqrt{q} - 4 + \#\Omega_0 + \#\Omega_1$.
This leads to $\left|\sum_{r\in\mathbb{F}_q}\xi(\phi_d(r))\right| \leq 12\sqrt{q} - 4 + \#\Omega_0 + \#\Omega_1 + \#\Omega$. But from the definition of the set R, Ω has at most $1+6=7$ elements. Hence using the facts that $\Omega_i = \{P \in C_i : f_i(P) \in \Omega\}$ and f_i is of degree 2 (since any point in $\mathbb{A}^1(\mathbb{F}_q)\setminus\Omega$ has exactly two preimages in $\mathcal{C}_i$), so $\#\Omega_i \leq 2\#\Omega = 14$. Finally, we have $\left|\sum_{r\in\mathbb{F}_q}\xi(\phi_d(r))\right| \leq 12\sqrt{q} + 31$.

Corollary 1. *Let $h_1, h_2 : \{0,1\}^* \to \mathbb{F}_q$ be two hash functions modeled as random oracles. Then the construction $H : m \mapsto \phi_d(h_1(m)) + \phi_d(h_2(m))$ is indifferentiable from a random oracle.*

Proof. By the previous theorem, we know that the encoding ϕ_d is $(12+31q^{-1/2})$-well-distributed. From theorem 1 and theorem 2 in [14], we deduce that is H regular. It is admissible since it is clearly computable and samplable (see [6], [14]). Hence we conclude that $m \mapsto f(h_1(m)) + f(h_2(m))$ is indifferentiable from a random oracle when h_1, h_2 are modeled as random oracles.

5. Conclusion

We have proposed new encoding functions for various forms of elliptic curves. Our encodings are almost injective and easily invertible. This is useful for constructing indifferentiable hash functions following the idea of *Farashahi et al.*

References

[1] Tatsuaki Okamoto Alfred Menezes and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5):1639–1646, 1993.

[2] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. *In CRYPTO (2001), LNCS, Springer*, 2139(3):213–229, 2001.

[3] B. Lynn D. Boneh and H. Shacham. Short signatures from the weil pairing. *In ASIACRYPT, LNCS, Springer*, 2248:514–532, 2001.

[4] Anna Krasnova Daniel J. Bernstein, Mike Hamburg and Tanja Lange. Elligator: Elliptic-curve points indistinguishable from uniform random strings. *ACM CCS*, 2013.

[5] Chen Qian ET AL. Diego F. Aranha, Pierre-Alain Fouque. Binary elligator squared. *Available at http://www.researchgate.net/publication/268333288*, November 2004.

[6] Jean-Sébastien Coron Thomas Icart ET AL. Eric Brier. Efficient Indifferentiable Hashing into Ordinary Elliptic Curves. *In CRYPTO (2010), LNCS, Springer*, 6223:237–254, 2010.

[7] Reza Rezaeian Farashahi. Efficient indifferentiable hashing into ordinary elliptic curves. *In AFRICACRYPT (2011), LNCS, Springer*, 6737:278–289, 2011.

[8] Pierre-Alain Fouque and Mehdi Tibouchi. Estimating the size of the image of deterministic hash functions to elliptic curves. *In LATINCRYPT (2010), LNCS, Springer*, 6212:81–91, 2010.

[9] Thomas Icart. How to hash into elliptic curves. *In CRYPTO (2009), LNCS, Springer*, 5677:303–316, 2009.

[10] The Tor Project Inc. Tor. *Available at www.torproject.org*, September 2015.

[11] Bodo Möller. A public-key encryption scheme with pseudo-random ciphertexts. *ESORICS, LNCS, Springer*, 3193:335–351, 2004.

[12] A. Joux P.-A. Fouque and M. Tibouchi. Injective encodings to elliptic curves. *In Information Security and Privacy - 18th Australasian Conference, LNCS, Springer*, 7959:16, July 2013.

[13] Antoine Joux Pierre-Alain Fouque and Mehdi Tibouchi. Injective encodings to elliptic curves. *In ACISP (2013), LNCS, Springer*, 7959:203–218, 2013.

[14] Igor E. Shparlinski ET AL. Reza R. Farashahi, Pierre-Alain Fouque. Indifferentiable deterministic hashing to elliptic and hyperelliptic curves. *Mathematics of Computation*, 82(281):491–512, January 2013.

[15] Andrew Shallue and Christiaan Van de Woestijne. Construction of rational points on elliptic curves over finite fields. *In ANTS (2006), LNCS, Springer*, 4076:510–524, 2006.

[16] Mariusz Skalba. Points on elliptic curves over finite fields. *Acta Arith.*, 117:293–301, 2005.

[17] Mehdi Tibouchi. Elligator squared: Uniform points on elliptic curves of prime order as uniform random strings. *To appear in Financial Cryptography, LNCS, Springer*, 2014.

[18] Philip D. MacKenzie Victor Boyko and Sarvar Patel. Provably secure password-authenticated key exchange using diffie-hellman. *In EUROCRYPT (2000), LNCS, Springer*, 1807:156171, 2001.