

# Faster indifferentiable hashing to elliptic $\mathbb{F}_{q^2}$ -curves

Dmitrii Koshelev<sup>1</sup>

Computer sciences and networks department, Télécom Paris  
Center for research and advanced development, Infotecs

**Abstract.** Let  $\mathbb{F}_q$  be a finite field and  $E: y^2 = x^3 + ax + b$  be an elliptic  $\mathbb{F}_{q^2}$ -curve of  $j(E) \notin \mathbb{F}_q$ . This article provides a new constant-time hash function  $\mathcal{H}: \{0, 1\}^* \rightarrow E(\mathbb{F}_{q^2})$  indifferentiable from a random oracle. Furthermore,  $\mathcal{H}$  can be computed with the cost of 3 exponentiations in  $\mathbb{F}_q$ . In comparison, the actively used (indifferentiable constant-time) simplified SWU hash function to  $E(\mathbb{F}_{q^2})$  computes 2 exponentiations in  $\mathbb{F}_{q^2}$ , i.e., it costs 4 ones in  $\mathbb{F}_q$ . In pairing-based cryptography one often uses the hashing to elliptic  $\mathbb{F}_{q^2}$ -curves  $E_b: y^2 = x^3 + b$  (of  $j$ -invariant 0) having an  $\mathbb{F}_{q^2}$ -isogeny  $\tau: E \rightarrow E_b$  of small degree. Therefore the composition  $\tau \circ \mathcal{H}: \{0, 1\}^* \rightarrow \tau(E(\mathbb{F}_{q^2}))$  is also an indifferentiable constant-time hash function.

**Key words:** constant-time implementation, hashing to elliptic and hyperelliptic curves, indifferentiability from a random oracle, isogenies, pairing-based cryptography, Weil restriction.

## Introduction

Suppose there is the subgroup  $G \subset E_b(\mathbb{F}_{q^2})$  of a large prime order  $\ell \mid N := \#E_b(\mathbb{F}_{q^2})$ . As is well known, only groups of such order are used in discrete logarithm cryptography. Many protocols of *pairing-based cryptography* [1] use a hash function  $\mathcal{H}: \{0, 1\}^* \rightarrow G$  *indifferentiable from a random oracle* [2, Definition 2]. In particular,  $\mathcal{H}$  should be *constant-time*, i.e., the computation time of its value is independent of an input argument. The latter is necessary to be protected against *timing attacks* [1, §8.2.2, §12.1.1]. A survey of this kind of hashing is well represented in [1, §8], [3].

It is sufficient to find a hash function  $\mathcal{H}: \{0, 1\}^* \rightarrow E_b(\mathbb{F}_{q^2})$ . Indeed, one of quick methods [1, §8.5] can be applied for computing the cofactor multiplication  $[N/\ell]: E_b(\mathbb{F}_{q^2}) \rightarrow G$ . This process obviously preserves the indifferentiability property. By the way, in practice  $q$  is almost always a prime such that  $q \equiv 3 \pmod{4}$ , i.e.,  $i := \sqrt{-1} \notin \mathbb{F}_q$  in order to accelerate the arithmetic of the field  $\mathbb{F}_{q^2}$  (see, e.g., [1, §5.2.1]).

Many hash functions  $\mathcal{H}$  are induced from some map  $h: \mathbb{F}_{q^2} \rightarrow E_b(\mathbb{F}_{q^2})$ , called *encoding*, such that  $\#\text{Im}(h) = \Theta(q^2)$ . In turn,  $q^2 \approx \#E_b(\mathbb{F}_{q^2})$  according to the Hasse inequality [4, Theorem V.1.1]. In other words,  $h$  should cover most  $\mathbb{F}_{q^2}$ -points of  $E_b$ . However there are no surjective encodings  $h$  for *ordinary* (i.e., *non-supersingular*) curves  $E_b$  (cf. [1, §8.3.2]). As is well known [1, §4], only such curves are interesting in pairing-based cryptography at the moment. Thus the trivial composition  $h \circ \eta$  with a hash function  $\eta: \{0, 1\}^* \rightarrow \mathbb{F}_{q^2}$  is not indifferentiable.

---

<sup>1</sup>web page: [https://www.researchgate.net/profile/Dimitri\\_Koshelev](https://www.researchgate.net/profile/Dimitri_Koshelev)  
email: dimitri.koshelev@gmail.com

Instead, it is often considered the composition  $\mathcal{H} := h^{\otimes 2} \circ \eta^2$  of the map

$$h^{\otimes 2}: \mathbb{F}_{q^2}^2 \rightarrow E_b(\mathbb{F}_{q^2}) \quad (t_0, t_1) \mapsto h(t_0) + h(t_1)$$

(also called encoding) and the hash function

$$\eta^2: \{0, 1\}^* \rightarrow \mathbb{F}_{q^2}^2 \quad m \mapsto (\eta(m|0), \eta(m|1)),$$

where  $|$  is the concatenation operation. In this case, the indifferentiability of  $\mathcal{H}$  follows from [2, Theorem 1] if  $\eta$  is so and  $h^{\otimes 2}$  is *admissible* in the sense of [2, Definition 4].

There is the so-called *SWU encoding* [1, §8.3.4], which is applicable to any elliptic  $\mathbb{F}_{q^2}$ -curve (not necessarily of  $j$ -invariant 0). Nevertheless, it generally requires the computation of 2 Legendre symbols (i.e., quadratic residuosity tests) in  $\mathbb{F}_q$ . Unfortunately, this operation (as well as the inversion one in  $\mathbb{F}_q$ ) is vulnerable to timing attacks if it is not implemented as an exponentiation in  $\mathbb{F}_q$  (see, e.g., [1, §2.2.9, §5.1.6]). But the latter is known to be a fairly laborious operation.

There is also the *simplified SWU encoding* [2, §7], which, on the contrary, can be implemented without Legendre symbols at all by virtue of [5, §2]. This encoding exists for all elliptic curves  $E$  whose  $j(E) \neq 0$ . The most difficult case  $j(E) = 1728$  is processed in [6]. In turn, the quite popular *Elligator 2 encoding* [7, §5] (very similar in nature) is appropriate for  $E_b$  only in the case  $\sqrt[3]{b} \in \mathbb{F}_{q^2}$ , that is  $2 \mid N$ .

Sometimes it is possible to use an  $\mathbb{F}_{q^2}$ -isogeny  $\tau: E \rightarrow E_b$  of small degree (the Wahby–Boneh approach [8]). For example, the curve BLS12-381 [8, §2.1] (whose  $b = 4(1 + i)$  and  $\lceil \log_2(q) \rceil = 381$ ) has such an isogeny of degree 3 for which  $j(E) = -2^{15}3 \cdot 5^3$ . Today, this curve is a de facto standard in the real-world pairing-based cryptography [9, §4.1.3]. More precisely, the encoding to  $E_b(\mathbb{F}_{q^2})$  can be constructed simply as the composition  $\tau \circ h$ , where  $h: \mathbb{F}_{q^2} \rightarrow E(\mathbb{F}_{q^2})$  is any one. It is clear that  $(\tau \circ h)^{\otimes 2} = \tau \circ h^{\otimes 2}$  is admissible as an encoding to the subgroup  $\tau(E(\mathbb{F}_{q^2})) \subset E_b(\mathbb{F}_{q^2})$ . Since  $\ell$  is large, actually  $G \subset \tau(E(\mathbb{F}_{q^2}))$ .

We show in §1 that under the conditions  $2 \nmid \#E(\mathbb{F}_{q^2})$  and  $j(E) \notin \mathbb{F}_q$  there is a *2-sheeted cover*  $\varphi_0: H \rightarrow E$  from a *real (split) hyperelliptic  $\mathbb{F}_q$ -curve*  $H$  (see, e.g., [10, §10.1.1]) of geometric genus 2. Then in §2 we construct a very simple encoding  $h: \mathbb{F}_q \rightarrow H(\mathbb{F}_q)$  (2) such that the map

$$h^{\otimes 3}: \mathbb{F}_q^3 \rightarrow J(\mathbb{F}_q) \quad (x_0, x_1, x_2) \mapsto h(x_0) + h(x_1) + h(x_2)$$

is admissible, where  $J$  is the *Jacobian* of  $H$ . Encodings to similar hyperelliptic curves are discussed in [11], [12].

Thus we automatically get the encoding  $\varphi_0 \circ h: \mathbb{F}_q \rightarrow E(\mathbb{F}_{q^2})$ . Moreover, by virtue of Theorem 1 its cubic power  $(\varphi_0 \circ h)^{\otimes 3}: \mathbb{F}_q^3 \rightarrow E(\mathbb{F}_{q^2})$  is also admissible. As above, its composition with the indifferentiable hash function

$$\eta^3: \{0, 1\}^* \rightarrow \mathbb{F}_q^3 \quad m \mapsto (\eta(m|00), \eta(m|01), \eta(m|10)),$$

where  $\eta: \{0, 1\}^* \rightarrow \mathbb{F}_q$ , gives such one to  $E(\mathbb{F}_{q^2})$ .

In other terms, we construct an  $\mathbb{F}_q$ -isogeny  $\phi := \theta^{-1} \circ \varphi: J \rightarrow R$  (with the kernel  $(\mathbb{Z}/2)^2$ ) to the *Weil restriction*  $R$  (see, e.g., [10, §5.7]) of  $E$  with respect to the extension  $\mathbb{F}_{q^2}/\mathbb{F}_q$ , where  $\varphi$  (resp.  $\theta^{-1}$ ) is defined in §1 (resp. [6, §1]). Formulas of such an isogeny are found in [13] based on the classical result [14]. Of course, one can apply these formulas for the hashing

instead of ours (1), which are derived differently. By the way, it is preferable to use  $(\varphi_0 \circ h)^{\otimes 3}$  rather than  $\phi \circ h^{\otimes 3}$ , because the addition in  $E(\mathbb{F}_{q^2}) = R(\mathbb{F}_q)$  seems to be much more efficient than in  $J(\mathbb{F}_q)$  (see [10, §10.4.2]).

The simplified SWU encoding  $h$  computes 1 square root in  $\mathbb{F}_{q^2}$ , hence the corresponding hash function  $\mathcal{H}$  (as well as  $h^{\otimes 2}$ ) computes 2 ones. The fact is that evaluating  $\eta$  is incomparably faster [3, §5]. In turn, 1 square root in  $\mathbb{F}_{q^2}$  costs 2 ones in  $\mathbb{F}_q$  according to [1, Algorithm 5.18]. The inversion operation and quadratic test in this algorithm are not taken into account by the same reason as in [5, §2]. As is well known, a square root in  $\mathbb{F}_q$  can be represented as an exponentiation in  $\mathbb{F}_q$  if  $q \equiv 3 \pmod{4}$ . In total,  $\mathcal{H}$  is implementable with the cost of 4 exponentiations in  $\mathbb{F}_q$ , although this is not remarked in [8, §4.2]. In comparison, the new hash function performs 3 square roots (i.e., exponentiations) in  $\mathbb{F}_q$ .

In particular, applying the latter to the widely used *BLS multi-signature (aggregate signature)* [15] with  $n$  different messages, the verifier should compute only  $3n$  exponentiations in  $\mathbb{F}_q$  rather than  $4n$  ones during the hashing phase. The author was recently informed that  $n \approx 16000$  in the famous blockchain Ethereum, which, like many others, uses the curve BLS12-381.

We suppose that  $N = \#E(\mathbb{F}_{q^2})$  is odd just to be definite, that is this condition can be omitted if desired. We restrict ourselves to this case, because it is the most difficult and BLS12-381 satisfies it. The more essential requirement consists in the fact that  $j(E) \notin \mathbb{F}_q$  (cf. Lemma 1). Fortunately, as shown in the computer algebra system Magma [16] the mentioned curve is  $\mathbb{F}_{q^2}$ -isogenous (with the help of an isogeny of degree 7) to the curve  $E$  with

$$j(E) = -3802283679744000\sqrt{21} - 17424252776448000,$$

where  $\sqrt{21} \notin \mathbb{F}_q$ . Our code [16] also generates the coefficients of  $H$ ,  $\varphi_0$  and  $E$ ,  $\tau$  in the generic case.

## 1 Two-sheeted cover $\varphi_0: H \rightarrow E$

Consider a finite field  $\mathbb{F}_q$  of characteristic  $> 3$  and elliptic  $\mathbb{F}_{q^2}$ -curves

$$E = E^{(0)}: y^2 = f_0(x) := x^3 + ax + b, \quad E^{(1)}: y^2 = f_1(x) := x^3 + a^q x + b^q.$$

They are obviously  $\mathbb{F}_{q^2}$ -isogenous by means of the Frobenius morphism  $\text{Fr}$ . If  $j(E) \in \mathbb{F}_q$  (that is  $j(E) = j(E^{(1)})$ ), then, in addition, there is an  $\overline{\mathbb{F}_q}$ -isomorphism

$$\sigma: E \xrightarrow{\sim} E^{(1)} \quad (x, y) \mapsto (\lambda^2 x, \lambda^3 y),$$

where

$$\lambda := \begin{cases} a^{(q-1)/4} = b^{(q-1)/6} & \text{if } j(E) \notin \{0, 1728\}, \text{ i.e., } ab \neq 0, \\ a^{(q-1)/4} & \text{if } j(E) = 1728, \text{ i.e., } b = 0, \\ b^{(q-1)/6} & \text{if } j(E) = 0, \text{ i.e., } a = 0. \end{cases}$$

Moreover,  $\lambda \in \mathbb{F}_{q^2}$  whenever  $ab \neq 0$ , because  $\lambda = \lambda^3 / \lambda^2 = (b/a)^{(q-1)/2}$ . The same is true if  $b = 0$  and  $q \equiv 1 \pmod{4}$  (resp.  $a = 0$  and  $q \equiv 1 \pmod{3}$ ).

Further, put  $A := E \times E^{(1)}$  with the projections  $pr_k: A \rightarrow E^{(k)}$  for  $k \in \mathbb{Z}/2$ . As it will become clear later, we need to work with  $\pi$ -invariant objects, where

$$\pi: A \xrightarrow{\sim} A \quad (P_0, P_1) \mapsto (\text{Fr}(P_1), \text{Fr}(P_0))$$

is the “twisted” Frobenius endomorphism.

Consider the decompositions

$$f_0(x) = (x - r_0)(x - r_1)(x - r_2), \quad f_1(x) = (x - r_0^q)(x - r_1^q)(x - r_2^q),$$

where

$$0 = r_0 + r_1 + r_2, \quad a = r_0r_1 + r_0r_2 + r_1r_2, \quad b = -r_0r_1r_2.$$

We will study the most difficult situation when  $r_j \notin \mathbb{F}_{q^2}$  for  $j \in \mathbb{Z}/3$  or, without loss of generality,  $r_j^{q^2} = r_{j+1}$ . For instance, the case  $b = 0$  is excluded from our consideration.

We are interested in the isomorphism  $\chi: E[2] \xrightarrow{\sim} E^{(1)}[2]$  defined by the bijection  $r_j \mapsto r_{j+1}^q$ . Its graph  $\Gamma \simeq (\mathbb{Z}/2)^2$  is clearly  $\pi$ -invariant, hence the corresponding isogeny  $\widehat{\varphi}': A \rightarrow A/\Gamma$  is also  $\pi$ -invariant. Here  $A/\Gamma$  is a principally polarized abelian surface (details see, e.g., in [17, §1]). The isomorphism  $\chi$  is said to be *reducible* if  $A/\Gamma$  is  $\overline{\mathbb{F}_q}$ -isomorphic (as PPAS) to the direct product of 2 elliptic curves.

**Lemma 1.** *The following statements are equivalent:*

1.  $\chi$  is reducible;
2.  $\chi$  is the restriction to  $E[2]$  of an  $\overline{\mathbb{F}_q}$ -isomorphism  $E \xrightarrow{\sim} E^{(1)}$ ;
3.  $j(E) \in \mathbb{F}_q$  and moreover  $q \equiv 1 \pmod{3}$  if  $j(E) = 0$ .

*Proof.* Concerning the equivalence of the first two statements see [18, Proposition 3]. Let’s prove that of the last two. We start from the implication **3**  $\Rightarrow$  **2**. The existence of the isomorphism  $\sigma$  implies that  $f_1(\lambda^2 r_j) = 0$ . In the case  $\lambda^2 r_0 = r_1^q$  we get  $\lambda^2 r_j = r_{j+1}^q$ , because  $\lambda \in \mathbb{F}_{q^2}$ .

If  $\lambda^2 r_0 = r_0^q$ , then similarly  $\lambda^2 r_j = r_j^q$ . Therefore  $\lambda^{2q} r_j^q = r_{j+1}$  and hence  $\lambda^{2(q+1)} r_j = r_{j+1}$ . As a result,  $\lambda^{2(q+1)} = \omega \in \mathbb{F}_q$ , where  $\omega^2 + \omega + 1 = 0$ . In other words,  $a = 0$  and  $r_j = -\omega^j \sqrt[3]{b}$ . Since  $r_j = \omega r_{j+2}$ , we have  $\omega \lambda^2 r_{j+2} = r_j^q$ , that is  $\omega \lambda^2 r_j = r_{j+1}^q$ . The case  $\lambda^2 r_0 = r_2^q$  is processed in the same way.

The inverse implication (**2**  $\Rightarrow$  **3**) is not trivial only for  $j(E) = 0$ . Suppose the opposite:  $q \equiv 2 \pmod{3}$  or, equivalently,  $\omega^q = \omega^2$ . We see that

$$\frac{r_{j+1}^q}{\lambda^2 r_j} = \frac{\omega^{j+2} (\sqrt[3]{b})^q}{\lambda^2 \sqrt[3]{b}} = \frac{\omega^{j+2} b^{(q-1)/3}}{\lambda^2} = \omega^{j+2+\ell}$$

for some fixed  $\ell \in \mathbb{Z}/3$ . Since this cubic root depends on  $j$ , we come to a contradiction.  $\square$

In accordance with [4, Example V.4.4] the condition  $q \equiv 1 \pmod{3}$  is fulfilled if  $E$  is an ordinary curve of  $j(E) = 0$ .

Hereafter we assume that  $\chi$  is irreducible, i.e.,  $J' := A/\Gamma$  is the Jacobian of some hyperelliptic curve  $H'$  of geometric genus 2. Applying [18, Proposition 4] to  $\chi$ , we obtain, modulo notation, the following explicit formulas (verified in [16]):

$$R_0 := \frac{(r_0 - r_2)^2}{(r_1 - r_0)^q} + \frac{(r_1 - r_0)^2}{(r_2 - r_1)^q} + \frac{(r_2 - r_1)^2}{(r_0 - r_2)^q}, \quad R_1 := r_0(r_0 - r_2)^q + r_1(r_1 - r_0)^q + r_2(r_2 - r_1)^q;$$

$A := \Delta^q R_0 / R_1$ , where  $\Delta = -(4a^3 + 27b^2)$  is the discriminant of  $E$ ;

$$A_0 := A(r_0 - r_1)(r_1 - r_2), \quad A_1 := A(r_1 - r_2)(r_2 - r_0), \quad A_2 := A(r_2 - r_0)(r_0 - r_1);$$

Note that  $A_j^{q^2} = A_{j+1}$ . Finally, the hyperelliptic curve is given by the equation

$$H': y^2 = f'(x) := -(A_0 x^2 + A_1^q)(A_1 x^2 + A_2^q)(A_2 x^2 + A_0^q).$$

Besides, there are 2-sheeted covers

$$\varphi'_0: H' \rightarrow E \quad (x, y) \mapsto (c/x^2 + d, ey/x^3), \quad \varphi'_1: H' \rightarrow E^{(1)} \quad (x, y) \mapsto (c^q x^2 + d^q, e^q y),$$

where

$$c := -A^{q-1} \frac{R_1}{R_0}, \quad d := \left( r_0 \frac{(r_2 - r_1)^2}{(r_0 - r_2)^q} + r_1 \frac{(r_0 - r_2)^2}{(r_1 - r_0)^q} + r_2 \frac{(r_1 - r_0)^2}{(r_2 - r_1)^q} \right) / R_0, \quad e := \frac{\Delta^q}{A^3}.$$

It is easy to prove that the isogeny  $\varphi': J' \rightarrow A$ , dual to  $\widehat{\varphi}'$ , is the natural extension of the morphism

$$(\varphi'_0, \varphi'_1): H' \rightarrow A \quad P \mapsto (\varphi'_0(P), \varphi'_1(P)).$$

It is an example of degenerate *Richelot isogeny* [19, §8.3].

The covers  $\varphi'_k$  are nothing but the natural maps  $\varphi'_0: H' \rightarrow H'/-\alpha \simeq E$  and  $\varphi'_1: H' \rightarrow H'/\alpha \simeq E^{(1)}$  under the involutions

$$\pm\alpha: H' \simeq H' \quad (x, y) \mapsto (-x, \pm y).$$

And through  $(\varphi'_0, \varphi'_1)$  the latter trivially correspond to

$$\pm\alpha: A \simeq A \quad (P_0, P_1) \mapsto (\mp P_0, \pm P_1).$$

As usual,  $H'$  has the smooth model  $Y^2 = F'(X, Z) := Z^6 f'(X/Z)$  in the weighted projective space  $\mathbb{P}(1, 3, 1)$  with the coordinates  $(X : Y : Z)$ , where  $x = X/Z$ ,  $y = Y/Z^3$ . The correct analogue of the “twisted” Frobenius endomorphism on  $H'$  is the map

$$\pi: H' \rightarrow H' \quad (X : Y : Z) \mapsto (Z^q : Y^q : X^q),$$

because under this definition the morphism  $(\varphi'_0, \varphi'_1)$  (and hence  $\varphi'$ ) is  $\pi$ -invariant.

For the sake of simplicity throughout the rest of the article  $q \equiv 3 \pmod{4}$ , that is  $i := \sqrt{-1} \notin \mathbb{F}_q$ . Although further formulas can be easily modified in the opposite case, choosing any quadratic non-residue in  $\mathbb{F}_q$  instead of  $-1$ . It is readily checked that  $H: Y^2 =$

$F'(X + iZ, X - iZ)$  is an  $\mathbb{F}_q$ -curve. In other terms,  $\psi^{-1} \circ \pi \circ \psi$  is the “ordinary” Frobenius endomorphism on  $H$ , where

$$\begin{aligned}\psi: H &\simeq H' & (X : Y : Z) &\mapsto (X + iZ : Y : X - iZ), \\ \psi^{-1}: H' &\simeq H & (X : Y : Z) &\mapsto \left( \frac{X + Z}{2} : Y : \frac{X - Z}{2i} \right).\end{aligned}$$

Denote by  $J$  the Jacobian of  $H$ . Let us keep the notation for the natural extensions  $\psi: J \simeq J'$  and  $\psi^{-1}: J' \simeq J$ . Of course, they are still mutually inverse. Also, put  $\varphi := \varphi' \circ \psi: J \rightarrow A$ .

Introduce new constants  $c_k, d_k, e_k \in \mathbb{F}_q$  such that

$$c = c_0 + c_1i, \quad d = d_0 + d_1i, \quad e = e_0 + e_1i.$$

Using Magma [16], we check that the compositions  $\varphi_k := \varphi'_k \circ \psi = pr_k \circ \varphi|_H$  are equal to

$$\varphi_k: H \rightarrow E^{(k)} \quad (x, y) \mapsto (x_0 + (-1)^k x_1i, y_0 + (-1)^k y_1i),$$

where

$$\begin{aligned}x_k &:= \frac{c_k(x^4 - 6x^2 + 1) + (-1)^k 4c_{k+1}x(x^2 - 1)}{(x^2 + 1)^2} + d_k, \\ y_k &:= \frac{e_k x(x^2 - 3) + (-1)^k e_{k+1}(3x^2 - 1)}{(x^2 + 1)^3} y.\end{aligned} \tag{1}$$

It is worth stressing that  $x_k, y_k \in \mathbb{F}_q(H)$ .

Let  $(J')^\pi$  (resp.  $A^\pi$ ) be the subgroup of all  $\pi$ -invariant points on  $J'$  (resp.  $A$ ). Obviously,  $\psi: J(\mathbb{F}_q) \simeq (J')^\pi$ . Besides,  $\tilde{\varphi}': A^\pi \simeq (J')^\pi$  (or, equivalently,  $\varphi': (J')^\pi \simeq A^\pi$ ), because  $\varphi' \circ \tilde{\varphi}' = [2]$  and  $A[2] \cap A^\pi$  is the trivial group. Finally,  $pr_k: A^\pi \simeq E^{(k)}(\mathbb{F}_{q^2})$  with the inverse maps

$$pr_k^{-1}: E^{(k)}(\mathbb{F}_{q^2}) \simeq A^\pi \quad pr_0^{-1}: P \mapsto (P, \text{Fr}(P)), \quad pr_1^{-1}: P \mapsto (\text{Fr}(P), P).$$

Let's summarize the main result of this paragraph.

**Theorem 1.** *We have the sequence of morphisms*

$$H \subset J \xrightarrow{\varphi} A \xrightarrow{pr_k} E^{(k)} \quad \text{such that} \quad H(\mathbb{F}_q) \subset J(\mathbb{F}_q) \xrightarrow{\varphi} A^\pi \xrightarrow{pr_k} E^{(k)}(\mathbb{F}_{q^2}).$$

## 2 Encoding $h: \mathbb{F}_q \rightarrow H(\mathbb{F}_q)$

It is shown in [16] that the  $\mathbb{F}_q$ -curve  $H$  from the previous paragraph has the affine form

$$H: y^2 = f(x) := f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 - f_4x^2 + f_5x - f_6$$

with the infinite points  $\mathcal{O}_\pm := (1 : \pm\sqrt{f_6} : 0)$ . By virtue of Theorem 1 and the fact that  $2 \nmid \#E(\mathbb{F}_{q^2})$  the polynomial  $f$  has no  $\mathbb{F}_q$ -roots. Indeed, if  $f(x) = 0$  for  $x \in \mathbb{F}_q^*$  (resp.  $x = 0$ ), then  $f(-x^{-1}) = 0$  (resp.  $f_6 = 0$ , i.e.,  $\mathcal{O}_+ = \mathcal{O}_-$ ), because  $f(-x^{-1}) = -f(x)/x^6$ . The equality

$x = -x^{-1}$  holds only for  $x = \pm i \notin \mathbb{F}_q$ . Therefore  $H$  can not possess the unique Weierstrass  $\mathbb{F}_q$ -point. However, as is well known [19, Lemma 8.1.3], two distinct such points give a point from  $J[2] \cap J(\mathbb{F}_q)$ .

The involutions  $\pm\alpha: H' \simeq H'$  are transformed to ones

$$\pm\alpha: H \simeq H \quad (X : Y : Z) \mapsto (-Z : \pm iY : X).$$

In particular,  $P_{\pm} := (0, \pm\sqrt{-f_6}) \xleftarrow{\alpha} \mathcal{O}_{\pm}$ . Thus we have the encoding

$$h: \mathbb{F}_q \rightarrow H(\mathbb{F}_q) \quad x \mapsto \begin{cases} (x, y) & \text{if } y := \sqrt{f(x)} \in \mathbb{F}_q, \\ \alpha(x, y) & \text{if } y \notin \mathbb{F}_q, \text{ i.e., } iy = \sqrt{-f(x)} \in \mathbb{F}_q. \end{cases}$$

For  $n := (q+1)/4 \in \mathbb{N}$  put  $g(x) := f(x)^n$ . Abusing the notation, we will often just write  $f, g$ . Note that  $g^2 = f^{(q+1)/2} = \left(\frac{f}{q}\right)f$ , where  $\left(\frac{f}{q}\right) = f^{(q-1)/2}$  is the Legendre symbol. It will be convenient to use the notation

$$X_{\pm} := \{x \in \mathbb{F}_q^* \mid \sqrt{\pm f} \in \mathbb{F}_q, \text{ i.e., } g^2 = \pm f\}, \quad S := pr_x^{-1}(X_+),$$

where  $pr_x$  is the projection  $H \rightarrow \mathbb{A}_x^1$ . Then  $x \mapsto -x^{-1}$  is a bijection between  $X_+$  and  $X_-$ .

Unfortunately, in addition to finding the square root the previous definition of  $h$  requires to compute the Legendre symbol. However (up to a sign of  $y$ ) the encoding can be rewritten in the following way:

$$h: \mathbb{F}_q \rightarrow H(\mathbb{F}_q) \quad x \mapsto \begin{cases} \mathcal{O}_+ & \text{if } x = 0 \text{ and } \sqrt{f_6} \in \mathbb{F}_q, \\ (x, g) & \text{if } g^2 = f, \\ (-x^{-1}, gx^{-3}) & \text{if } g^2 = -f. \end{cases} \quad (2)$$

In practice,  $h$  can be restricted to  $\mathbb{F}_q^*$  in order to avoid hitting the point  $\mathcal{O}_+$ . Representing the coordinates of  $h(x)$  by their numerators and common denominator (i.e., by 3 elements of  $\mathbb{F}_q$ ), we get

**Remark 1.** *The encoding  $h$  is computed in constant time of an exponentiation in  $\mathbb{F}_q$ .*

The same is true for  $\varphi_0 \circ h: \mathbb{F}_q \rightarrow E(\mathbb{F}_{q^2})$ . Indeed, by definition,  $\varphi_0 \circ -\alpha = \varphi_0$ , that is  $\varphi_0(-x^{-1}, gx^{-3}) = \varphi_0(x, ig)$ . Hence we do not have to find  $x^{-1}$  before evaluating the covering map  $\varphi_0$ .

Obviously,  $\#h^{-1}(P_{\pm}), \#h^{-1}(\mathcal{O}_{\pm}) \leq 1$ . In turn, for any  $x_0, x_1 \in X_+$  (or  $X_-$ ) such that  $h(x_0) = h(x_1)$  we have  $x_0 = x_1$ . However for some  $x \in \mathbb{F}_q^*$  maybe  $h(x) = h(-x^{-1})$ . Therefore we obtain

**Lemma 2.** *For any point  $P \in H(\mathbb{F}_q)$  we have  $\#h^{-1}(P) \leq 2$  and hence  $q/2 \leq \#\text{Im}(h)$ .*

The last definition of  $h$  can be made injective if to set the sign of the  $y$ -coordinate more accurately (e.g., as in [8, §2]), but in this case we do not know how to correctly modify the proof of the next theorem. As is easily seen, actually  $\#H(\mathbb{F}_q) = q + 1$ .

**Theorem 2.** *The encoding  $h: \mathbb{F}_q \rightarrow H(\mathbb{F}_q)$  is  $B$ -well-distributed in the sense of [20, Definition 1], where  $B := 18 + O(q^{-1/2})$ .*

*Proof.* Consider the functions  $f_+ := y$ ,  $f_- := (-1)^n xy$  on the curve  $H$ . Notice that  $\left(\frac{f_\pm}{q}\right) = 1$  whenever  $x \in X_\pm$  and  $y = y(h(x))$ . Indeed,  $\left(\frac{y}{q}\right) = \left(\frac{f}{q}\right)^n = 1$  if  $x \in X_+$  (resp.  $(-1)^n$  if  $x \in X_-$ ). And for  $x \in X_-$  we have  $\left(\frac{y}{q}\right) = (-1)^n \left(\frac{x}{q}\right)$ . Given a non-trivial character  $\chi: J(\mathbb{F}_q) \rightarrow \mathbb{C}^*$  we see that

$$\sum_{x \in X_\pm} \chi(h(x)) = \sum_{P \in pr_x^{-1}(X_+)} \frac{1 + \left(\frac{f_\pm(P)}{q}\right)}{2} \cdot \chi(P).$$

As a consequence,

$$\left| \sum_{x \in X_\pm} \chi(h(x)) \right| \leq \frac{1}{2} \sum_{k \in \{0,1\}} \left| \sum_{P \in H(\mathbb{F}_q)} \left(\frac{f_\pm^k(P)}{q}\right) \cdot \chi(P) \right| + O(1).$$

Here notation  $O(1)$  is used to avoid handling the set  $pr_x^{-1}(\{0, \infty\}) = \{P_\pm, \mathcal{O}_\pm\}$ . According to [20, Theorem 7] and the fact that

$$\deg(f_+) = \deg(pr_y) = 6, \quad \deg(f_-) = \deg(pr_x) + \deg(pr_y) = 8$$

(where  $pr_y$  is the projection  $H \rightarrow \mathbb{A}_y^1$ ) we obtain

$$\left| \sum_{P \in H(\mathbb{F}_q)} \left(\frac{f_\pm^k(P)}{q}\right) \cdot \chi(P) \right| \leq 2(g(H) - 1 + k \deg(f_\pm)) \sqrt{q} \leq \begin{cases} 2(1 + 6k)\sqrt{q} & \text{for } +, \\ 2(1 + 8k)\sqrt{q} & \text{for } -. \end{cases}$$

Thus

$$\left| \sum_{x \in X_\pm} \chi(h(x)) \right| \leq O(1) + \begin{cases} 8\sqrt{q} & \text{for } +, \\ 10\sqrt{q} & \text{for } - \end{cases}$$

and hence

$$\left| \sum_{x \in \mathbb{F}_q} \chi(h(x)) \right| \leq \left| \sum_{x \in X_+} \chi(h(x)) \right| + \left| \sum_{x \in X_-} \chi(h(x)) \right| + O(1) \leq 18\sqrt{q} + O(1).$$

The theorem is proved. □

Further, from [10, Exercise 10.7.9], [20, Corollary 4] it immediately follows that

**Corollary 1.** *The distribution on  $J(\mathbb{F}_q)$  defined by  $h^{\otimes 3}: \mathbb{F}_q^3 \rightarrow J(\mathbb{F}_q)$  is  $\epsilon$ -statistically indistinguishable [2, Definition 3] from the uniform one, where  $\epsilon := 18^3 q^{-1/2} + O(q^{-3/4})$ .*

According to Remark 1 the encoding  $h^{\otimes 3}$  is computable in constant time of 3 exponentiations in  $\mathbb{F}_q$ . Finally, it is easily shown that  $h^{\otimes 3}$  is also *samplable* [2, Definition 4]. Therefore we establish

**Corollary 2.** *The encoding  $h^{\otimes 3}$  is admissible.*

## References

- [1] N. El Mrabet, M. Joye, *Guide to Pairing-Based Cryptography*, Cryptography and Network Security Series, Chapman and Hall/CRC, New York, 2017.
- [2] E. Brier et al., “Efficient indifferentiable hashing into ordinary elliptic curves”, *Advances in Cryptology — CRYPTO 2010*, LNCS, **6223**, ed. T. Rabin, Springer, Berlin, 2010, 237–254.
- [3] A. Faz-Hernandez et al., *Hashing to elliptic curves*, <https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve>, 2021.
- [4] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, **106**, Springer, New York, 2009.
- [5] D. Koshelev, *Hashing to elliptic curves of  $j = 0$  and quadratic imaginary orders of class number 2*, ePrint IACR 2020/969, 2021.
- [6] D. Koshelev, *Hashing to elliptic curves of  $j$ -invariant 1728*, ePrint IACR 2019/1294, accepted in *Cryptography and Communications*, 2020.
- [7] D. Bernstein et al., “Elligator: Elliptic-curve points indistinguishable from uniform random strings”, *ACM SIGSAC Conference on Computer & Communications Security*, 2013, 967–980.
- [8] R. Wahby, D. Boneh, “Fast and simple constant-time hashing to the BLS12-381 elliptic curve”, *IACR Transactions on Cryptographic Hardware and Embedded Systems*, **2019**:4, 154–179.
- [9] Y. Sakemi et al., *Pairing-friendly curves*, <https://datatracker.ietf.org/doc/draft-irtf-cfrg-pairing-friendly-curves>, 2020.
- [10] S. Galbraith, *Mathematics of public key cryptography*, Cambridge University Press, New York, 2012.
- [11] P.-A. Fouque, M. Tibouchi, “Deterministic encoding and hashing to odd hyperelliptic curves”, *Pairing-Based Cryptography — Pairing 2010*, LNCS, **6487**, eds. M. Joye, A. Miyaji, A. Otsuka, Springer, Berlin, 2010, 265–277.
- [12] P.-A. Fouque, A. Joux, M. Tibouchi, “Injective encodings to elliptic curves”, *Australasian Conference on Information Security and Privacy*, LNCS, **7959**, eds. C. Boyd, L. Simpson, Springer, Berlin, 2013, 203–218.
- [13] D. Bernstein, T. Lange, “Hyper-and-elliptic-curve cryptography”, *LMS Journal of Computation and Mathematics*, **17**:A (2014), 181–202.
- [14] J. Scholten, *Weil restriction of an elliptic curve over a quadratic extension*, [https://www.researchgate.net/publication/228946053\\_Weil\\_restriction\\_of\\_an\\_elliptic\\_curve\\_over\\_a\\_quadratic\\_extension](https://www.researchgate.net/publication/228946053_Weil_restriction_of_an_elliptic_curve_over_a_quadratic_extension), 2003.
- [15] D. Boneh et al., *BLS signatures*, <https://datatracker.ietf.org/doc/draft-irtf-cfrg-bls-signature>, 2020.
- [16] D. Koshelev, *Magma code*, <https://github.com/dishport/Faster-indifferentiable-hashing-to-elliptic-Fq2-curves>, 2021.
- [17] E. Kani, “The number of curves of genus two with elliptic differentials”, *Journal für die Reine und Angewandte Mathematik*, **485** (1997), 93–122.
- [18] E. Howe, F. Leprévost, B. Poonen, “Large torsion subgroups of split Jacobians of curves of genus two or three”, *Forum Mathematicum*, **12**:3 (2000), 315–364.
- [19] B. Smith, *Explicit endomorphisms and correspondences*, <https://ses.library.usyd.edu.au/handle/2123/1066>, 2005.
- [20] R. Farashahi et al., “Indifferentiable deterministic hashing to elliptic and hyperelliptic curves”, *Mathematics of Computation*, **82**:281 (2013), 491–512.