Indifferentiable hashing to ordinary elliptic $\mathbb{F}_q$-curves of $j = 0$ with the cost of one exponentiation in $\mathbb{F}_q$

Dmitrii Koshelev [1]

Computer sciences and networks department, Télécom Paris

Abstract. Let $\mathbb{F}_q$ be a finite field and $E_b\colon y^2 = x^3 + b$ be an ordinary (i.e., non-supersingular) elliptic curve (of j-invariant 0) such that $\sqrt{b} \in \mathbb{F}_q$ and $q \not\equiv 1 \pmod{27}$. For example, these conditions are fulfilled for the group $\mathbb{G}_1$ of the curve BLS12-381 ($b = 4$). It is a de facto standard in the real world pairing-based cryptography at the moment. This article provides a new constant-time hash function $H\colon \{0,1\}^* \to E_b(\mathbb{F}_q)$ indifferentiable from a random oracle. Its main advantage is the fact that H computes only one exponentiation in $\mathbb{F}_q$. In comparison, the previous fastest constant-time indifferentiable hash functions to $E_b(\mathbb{F}_q)$ compute two exponentiations in $\mathbb{F}_q$. In particular, applying H to the widely used BLS multi-signature with m different messages, the verifier should perform only m exponentiations rather than $2m$ ones during the hashing phase.

Key words: cubic residue symbol and cubic roots, hashing to ordinary elliptic curves of j-invariant 0, indifferentiability from a random oracle, pairing-based cryptography.

Introduction

Since its invention in the early 2000s, *pairing-based cryptography* [1] has become more and more popular every year, for example in secure multi-party computations. One of the latest reviews of standards, commercial products and libraries for this type of cryptography is represented in [2, §4.1].

Let $\mathbb{F}_q$ be a finite field of $\mathrm{char}(\mathbb{F}_q) > 3$ and $E_b\colon y^2 = x^3 + b$ be an elliptic $\mathbb{F}_q$-curve whose the j-invariant is 0. The priority is given to the curves E_b, because the pairing computation on them is the most efficient (see [1, §4]). As is well known [1, Remark 2.22], only ordinary curves are safe to deal with the discrete logarithm problem. And according to [3, Example V.4.4] the ordinariness of E_b results in the restriction $q \equiv 1 \pmod 3$, i.e., $\omega := \sqrt[3]{1} \in \mathbb{F}_q$, where $\omega \neq 1$. Today, the most popular *pairing-friendly curve* in the industry is the Barreto–Lynn–Scott curve BLS12-381 [4, §2.1] for which $\lceil \log_2(q) \rceil = 381$.

Many pairing-based protocols (for example, the BLS multi-signature [5, §3], [6]) use a hash function of the form $H\colon \{0,1\}^* \to E_b(\mathbb{F}_q)$. There is the regularly updated draft [7] (see also [1, §8]) on the topic of hashing to elliptic curves. In order to be used in practice H must be *indifferentiable from a random oracle* [8, Definition 2] and *constant-time*, that is the computation time of its value is independent of an input argument.

Almost all such previously proposed hash functions are obtained as the composition $H :=$

[1] web page: https://www.researchgate.net/profile/Dimitri_Koshelev
email: dishport@yandex.ru

$e^{\otimes 2} \circ \mathfrak{h}$ of a hash function $\mathfrak{h}\colon \{0,1\}^* \to \mathbb{F}_q^2$ and the tensor square

$$e^{\otimes 2}\colon \mathbb{F}_q^2 \to E_b(\mathbb{F}_q) \qquad e^{\otimes 2}(t_1,t_2) := e(t_1) + e(t_2)$$

of some map $e\colon \mathbb{F}_q \to E_b(\mathbb{F}_q)$. Such a map is often called *encoding*. In this case the indifferentiability of H follows from [8, Theorem 1] if $\mathfrak{h}$ is indifferentiable and $e^{\otimes 2}$ is *admissible* in the sense of [8, Definition 4]. The fastest known encodings are Elligator 2 [9, §5] and the Wahby–Boneh "indirect" map [4]. Both (resp. H) can be implemented with the cost of one (resp. two) exponentiation(s) in $\mathbb{F}_q$.

This article essentially improves our ideas from [10]. There provided that $\sqrt{b} \in \mathbb{F}_q$ we construct one more encoding e whose the tensor square $e^{\otimes 2}$ is admissible. Moreover, e equally requires only one exponentiation in $\mathbb{F}_q$. However in this work (also for $\sqrt{b} \in \mathbb{F}_q$) we directly provide an admissible map $h\colon \mathbb{F}_q^2 \to E_b(\mathbb{F}_q)$ approximately with the same cost as e and such that $h(t,t) = \pm e(t)$. In other words, the tensor square is superfluous in this situation and hence we get rid of one exponentiation in $\mathbb{F}_q$. Let us also remark that h is given by quite simple formulas with small coefficients unlike the Wahby–Boneh encoding.

The same idea is applicable to the famous SWU (Shallue–van de Woestijne–Ulas) encoding [1, §8.3.4] with the cost of two exponentiations in $\mathbb{F}_q$. It is based on the seminal work [11, Lemma 3] of Skałba, where the author derives a map $\mathbb{F}_q^2 \to E(\mathbb{F}_q)$ for any elliptic $\mathbb{F}_q$-curve E of $j(E) \neq 0$. The research society refused this map, because it is determined by fairly cumbersome formulas in comparison with those of the SWU encoding. This article restores justice by implicitly showing that the result of Skałba is more valuable than its refinements of Shallue, van de Woestijne, and Ulas. Nevertheless, it still remains open the existence question of an indifferentiable hash function to the ordinary curve E with the cost of one exponentiation in the field $\mathbb{F}_q$.

1 Geometric results

As mentioned above, we are only interested in $q \equiv 1 \pmod 3$, i.e., $\omega := \sqrt[3]{1} \in \mathbb{F}_q^*$, where $\omega \neq 1$. Consider the two different cubic $\mathbb{F}_q$-twists $E_b^{(j)}$ (for $j \in \{1,2\}$) of the given curve $E_b = E_b^{(0)}$. There is on $E_b^{(i)} \subset \mathbb{A}^2_{(x_i,y_i)}$ (for $i \in \{0,1,2\}$) the $\mathbb{F}_q$-automorphism $[\omega](x_i,y_i) := (\omega x_i, y_i)$ of order 3. Take the quotient $T := (E_b \times E_b^{(1)} \times E_b^{(2)})/[\omega]^{\times 3}$ with respect to the diagonal action of $[\omega]$. This is a *Calabi–Yau threefold* according to [12, §1.3]. By the way, the SWU encoding (Skałba map) deals with another Calabi–Yau $\mathbb{F}_q$-threefold.

Without lost of generality suppose that $\sqrt[3]{b} \notin \mathbb{F}_q$. In the opposite case, one can start from $E_b^{(1)}$ or $E_b^{(2)}$. Under our assumption, the elliptic curves are determined by the equations $E_b^{(i)}\colon y_i^2 = b^i x_i^3 + b \simeq_{\mathbb{F}_q} E_{b^{2i+1}}$. Also, it is readily seen that T has the affine model

$$T\colon \begin{cases} y_1^2 - b = b(y_0^2 - b)t_1^3, \\ y_2^2 - b = b^2(y_0^2 - b)t_2^3 \end{cases} \quad \subset \quad \mathbb{A}^5_{(y_0,y_1,y_2,t_1,t_2)},$$

where $t_j := x_j/x_0$.

We can look at T as a curve in $\mathbb{A}^3_{(y_0,y_1,y_2)}$ given as the intersection of two quadratic surfaces over $\mathbb{F}_q(t_1,t_2)$, where the latter denotes the rational function field in two variables t_1, t_2 over

the constant field $\mathbb{F}_q$. Nevertheless, below it will be more convenient to work over the subfield $F := \mathbb{F}_q(s_1, s_2)$, where $s_j := t_j^3$.

Lemma 1 ([13])**.** *T/F is an elliptic curve having a short Weierstrass form $W\colon y^2 = x^3 + a_4x + a_6$ with the coefficients*

$$a_4 := -3(b^2s_1s_2 + \omega^2 s_1 + \omega b s_2)(b^2s_1s_2 + \omega s_1 + \omega^2 b s_2),$$
$$a_6 := -(b^2s_1s_2 - 2s_1 + bs_2)(2b^2s_1s_2 - s_1 - bs_2)(b^2s_1s_2 + s_1 - 2bs_2).$$

In particular, the discriminant and j-invariant of W equal

$$\Delta = \big(2^2 3^3 b s_1 s_2 (bs_1 - 1)(b^2 s_2 - 1)(s_1 - bs_2)\big)^2,$$
$$j = \big(2^4 3^2 (b^2 s_1 s_2 + \omega s_1 + \omega^2 b s_2)(b^2 s_1 s_2 + \omega^2 s_1 + \omega b s_2)\big)^3/\Delta.$$

Theorem 1 ([13])**.** *There is a point $\psi \in W(F)$ with the coordinates*

$$x = b(2bs_1 - 1)s_2 - (3bs_1 - 2)s_1, \qquad y = 3\sqrt{b}(2\omega + 1)s_1(bs_1 - 1)(bs_2 - s_1).$$

It corresponds to a point $\varphi \in T(F)$ whose the coordinates are the irreducible fractions $y_i(t_1, t_2) := num_i/den$, where

$$num_0 := \sqrt{b}\cdot\big(b^2s_1^2 - 2b^3s_1s_2 + 2bs_1 + b^4s_2^2 + 2b^2s_2 - 3\big),$$
$$num_1 := \sqrt{b}\cdot\big(-3b^2s_1^2 + 2b^3s_1s_2 + 2bs_1 + b^4s_2^2 - 2b^2s_2 + 1\big),$$
$$num_2 := \sqrt{b}\cdot\big(b^2s_1^2 + 2b^3s_1s_2 - 2bs_1 - 3b^4s_2^2 + 2b^2s_2 + 1\big),$$
$$den := b^2s_1^2 - 2b^3s_1s_2 - 2bs_1 + b^4s_2^2 - 2b^2s_2 + 1.$$

Moreover, $\sum_{i=0}^{2} y_i(t_1, t_2) + \sqrt{b} = 0$.

It is remarkable that the functions $y_i(t, t)$ are nothing but (up to the minus sign) those from [10, Theorem 1]. Besides, the important case $b = 4$ gives

$$num_0 = 2\cdot\big(2^4s_1^2 - 2^7s_1s_2 + 2^3s_1 + 2^8s_2^2 + 2^5s_2 - 3\big),$$
$$num_1 = 2\cdot\big(-2^4 3s_1^2 + 2^7s_1s_2 + 2^3s_1 + 2^8s_2^2 - 2^5s_2 + 1\big),$$
$$num_2 = 2\cdot\big(2^4s_1^2 + 2^7s_1s_2 - 2^3s_1 - 2^8 3s_2^2 + 2^5s_2 + 1\big),$$
$$den = 2^4s_1^2 - 2^7s_1s_2 - 2^3s_1 + 2^8s_2^2 - 2^5s_2 + 1.$$

In other words, $T/\mathbb{F}_q$ is an *elliptic threefold* whose the *elliptic fibration* is the projection to t_1, t_2. In these terms, $\varphi\colon \mathbb{A}^2_{(t_1,t_2)} \dashrightarrow T$ is an $\mathbb{F}_q$-section of the given fibration. In particular, $\mathrm{Im}(\varphi)$ is a rational $\mathbb{F}_q$-surface. In turn, W is a *global minimal* Weierstrass form for T. These and other notions of the theory of elliptic threefolds see, e.g., in [14]. For completeness, the much simpler theory of elliptic surfaces is well represented in [15].

If the point $\phi_0 := \big(\sqrt{b}, \sqrt{b}, \sqrt{b}\big)$ is chosen as the neutral element of the *Mordell–Weil group* $T(F)$, then as shown in [13] its 2-torsion subgroup $T(F)[2] = \{\phi_i\}_{i=0}^3$, where

$$\phi_1 := \big(\sqrt{b}, -\sqrt{b}, -\sqrt{b}\big), \qquad \phi_2 := \big(-\sqrt{b}, \sqrt{b}, -\sqrt{b}\big), \qquad \phi_3 := \big(-\sqrt{b}, -\sqrt{b}, \sqrt{b}\big).$$

The next theorem clarifies why ψ has the simplest coordinates among infinite order points from $W(F)$.

Theorem 2. *Consider F as the rational function field $k_1(s_2)$ (resp. $k_2(s_1)$) over the constant field $k_1 := \mathbb{F}_q(s_1)$ (resp. $k_2 := \mathbb{F}_q(s_2)$). Then, taking into account the lattice structure with respect to the height pairing,*

$$T(F) \simeq W(F) \simeq \mathrm{A}_1^* \oplus (\mathbb{Z}/2)^2, \qquad \textit{moreover}, \qquad W(F)/W(F)_{\mathrm{tor}} = \langle \psi \rangle.$$

Proof. Since T/k_j is obviously a rational surface, W/k_j is also so. With the help of [13] we get that the singular fibers of the Kodaira–Néron model of W/k_j have the types $\mathrm{I}_2, \mathrm{I}_2, \mathrm{I}_2, \mathrm{I}_0^*$ in Kodaira's notation. Consequently $W\big(\overline{k_1}(s_2)\big) \simeq W\big(\overline{k_2}(s_1)\big) \simeq \mathrm{A}_1^* \oplus (\mathbb{Z}/2)^2$ according to [15, Table 8.2]. Further, [13] allows to compute the canonical height of ψ, which turns out to equal $1/2$. This is also the minimal norm of the lattice A_1^*. Thus the theorem is proved. $\square$

We do not claim that $T(F)/T(F)_{\mathrm{tor}} = \langle \varphi \rangle$ with respect to ϕ_0 as the neutral element of $T(F)$, because this point does not correspond to that at infinity on W/F. We chose ϕ_0 just to describe $T(F)[2]$ in a more canonical way.

For the sake of compactness we put

$$\beta := -3\sqrt{b}, \qquad \infty := (1:0) \in \mathbb{P}^1, \qquad P_0 := (0, \sqrt{b}) \in E_b, \qquad \mathcal{O} := (0:1:0) \in E_b.$$

Denote by Num_i (resp. Den) the homogenization of num_i (resp. den) with respect to a new variable t_0. For $y \in \mathbb{F}_q$ consider on $\mathbb{P}^2_{(t_0:t_1:t_2)}$ the pencil of the $\mathbb{F}_q$-sextics

$$C_{i,y} \colon Num_i = Den \cdot y, \qquad C_{i,\infty} = C_\infty \colon Den = 0$$

and the $\mathbb{F}_q$-conics $D_{i,y} := \pi(C_{i,y})$, where

$$\pi \colon \mathbb{P}^2 \to \mathbb{P}^2 \qquad \pi(t_0 : t_1 : t_2) := (t_0^3 : t_1^3 : t_2^3).$$

Also, let $L_i \colon t_i = 0$,

$$R_0 := (1:0:0), \qquad R_1 := (0:1:0), \qquad R_2 := (0:0:1)$$

and $\mathbf{Q}_k := \pi^{-1}(Q_k)$, where

$$Q_0 := (0:b:1), \qquad Q_1 := (b^2:0:1), \qquad Q_2 := (b:1:0).$$

Below we formulate a few simple lemmas, which are readily checked. By the way, the indices $i \pm 1$ will always mean the operations $\pm$ modulo 3.

Lemma 2. *The order 3 projective $\mathbb{F}_q$-transformations*

$$\tau\colon \mathbb{P}^2 \xrightarrow{\sim} \mathbb{P}^2 \qquad \tau(t_0 : t_1 : t_2) := (bt_2 : t_0 : t_1) \qquad \text{and} \qquad \tau' := \pi \circ \tau \circ \pi^{-1}\colon \mathbb{P}^2 \xrightarrow{\sim} \mathbb{P}^2$$

give the isomorphisms

$$\tau\colon C_{i,y} \xrightarrow{\sim} C_{i+1,y}, \qquad \tau'\colon D_{i,y} \xrightarrow{\sim} D_{i+1,y}, \qquad \tau, \tau'\colon L_i \xrightarrow{\sim} L_{i+1}$$

as well as

$$\tau(R_i) = \tau'(R_i) = R_{i+1}, \qquad \tau'(Q_i) = Q_{i+1}.$$

It is worth noting that the curves $D_{i,\pm\sqrt{b}}$ (and hence $C_{i,\pm\sqrt{b}}$) are reducible over $\mathbb{F}_q$. Indeed,

$$D_{0,\sqrt{b}}\colon t_0(t_0 - bt_1 - b^2t_2) = 0, \qquad D_{0,-\sqrt{b}}\colon (t_0 - bt_1 + b^2t_2)(t_0 + bt_1 - b^2t_2) = 0. \tag{1}$$

Lemma 3. *There are the following equalities. First,*

$$D_{i,y} \cap D_\infty = D_{i,0} \cap D_\infty = \{Q_k\}_{k=0}^2.$$

Second,

$$D_{0,y} \cap D_{1,y} = \{Q_k\}_{k=0}^2 \cup \left\{\left(b^2(y - \sqrt{b}) : b(y - \sqrt{b}) : 4y\right)\right\}$$

for $y \neq \pm\sqrt{b}$. Third,

$$D_{i,y} \cap L_i = \{Q_i\}, \qquad D_{0,y} \cap L_1 = \left\{Q_1, \left(b^2(y - \sqrt{b}) : 0 : y - \beta\right)\right\},$$
$$D_\infty \cap L_k = \{Q_k\}, \qquad D_{0,y} \cap L_2 = \left\{Q_2, \left(b(y - \sqrt{b}) : y - \beta : 0\right)\right\}$$

also for $y \neq \pm\sqrt{b}$.

Lemma 4. *The set of singular points*

$$\mathrm{Sing}(C_{i,y}) = \begin{cases} \mathbf{Q}_i & \text{if} \quad y \notin \{\pm\sqrt{b}, \beta, \infty\}, \\ \mathbf{Q}_i \cup \{R_i\} & \text{if} \quad y = \beta, \\ \cup_{k=0}^2 \mathbf{Q}_k & \text{if} \quad y = \infty. \end{cases}$$

Moreover, $R_i \in C_{i,\beta}$ is an ordinary point of multiplicity 3 and all other singularities are cusps regardless of y.

Theorem 3. *For $y \neq \pm\sqrt{b}$ the curves $C_{i,y}$ are absolutely irreducible.*

Proof. The cases $y \in \{\beta, \infty\}$ are immediately processed by Magma [13]. In compliance with Lemma 4 for another y the curve $C_{i,y}$ has only 3 cusps, hence it has no more than 3 different absolutely irreducible components F_0, F_1, F_2. Consider the transformations

$$\chi_k\colon C_{i,y} \xrightarrow{\sim} C_{i,y} \qquad \chi_0 := (\omega t_0 : t_1 : t_2), \qquad \chi_1 := (t_0 : \omega t_1 : t_2), \qquad \chi_2 := (t_0 : t_1 : \omega t_2).$$

Since they are of order 3, for any $k, \ell, m \in \{0, 1, 2\}$, $\ell \neq m$ the case $\chi_k\colon F_\ell \xrightarrow{\sim} F_m$, $F_m \xrightarrow{\sim} F_\ell$ is not possible, otherwise $F_\ell = F_m$. Also, given ℓ note that $\chi_k\colon F_\ell \xrightarrow{\sim} F_\ell$ for all k if and only if F_ℓ is a Fermat cubic or the line L_m for some m. Consequently either F_0, F_1 are Fermat cubics or F_0, F_1, F_2 are conics conjugate by χ_k for some (or, equivalently, any) k.

It is checked in [13] that the second case does not occur. In the first one, we obtain the decomposition $D_{i,y} = \pi(F_0) \cup \pi(F_1)$ into lines. However it is easily shown that the discriminant of the conic $D_{i,y}$ equals $\pm 4b^6(y - \sqrt{b})(y + \sqrt{b})^2$, hence it is non-degenerate for $y \neq \pm\sqrt{b}$. $\square$

Hereafter we assume that $y \neq \pm\sqrt{b}$. Let $\sigma_{i,y}\colon C'_{i,y} \to C_{i,y}$ be the corresponding normalization morphisms. As is well known,

$$\#\sigma_{i,y}^{-1}(\mathbf{Q}_i) = \#\sigma_{i,\beta}^{-1}(R_i) = \#\sigma_{\infty}^{-1}(\mathbf{Q}_k) = 3, \qquad \sigma_{i,y}\colon C'_{i,y} \setminus \sigma_{i,y}^{-1}\big(\mathrm{Sing}(C_{i,y})\big) \xrightarrow{\sim} C_{i,y} \setminus \mathrm{Sing}(C_{i,y}).$$

Further, we have the coverings $\pi_{i,y} := \pi \circ \sigma_{i,y}\colon C'_{i,y} \to D_{i,y}$ whose the Galois group is clearly isomorphic to $(\mathbb{Z}/3)^2$.

Theorem 4. *For $y \notin \{\beta, \infty\}$ the geometric genus $g(C_{i,y}) = 7$. Also, $g(C_{i,\beta}) = 4$, $g(C_\infty) = 1$.*

Proof. Denote by r_y the number of ramified points $Q \in D_{i,y}$. Since $\pi_{i,y}$ is a Galois covering, the well defined ramification index $e_Q \in \{3, 9\}$ (see, e.g., [16, Corollary 3.7.2]). It is obvious that $Q \in L_k$ for some $k \in \{0, 1, 2\}$. Moreover, the case $e_Q = 9$ may occur only for $Q \in \{R_k\}_{k=0}^2$. From Lemmas 2, 3 it follows that

$$\#(D_{i,y} \cap L_i) = 1, \qquad \#(D_{i,y} \cap L_{i-1}) = \#(D_{i,y} \cap L_{i+1}) = \begin{cases} 1 & \text{if} \quad y = \infty, \\ 2 & \text{otherwise.} \end{cases}$$

Moreover, $R_{i-1}, R_{i+1} \notin D_{i,y}$, but $R_i \in D_{i,y}$ if and only if $y = \beta$. Therefore $r_y = 5$ for $y \notin \{\beta, \infty\}$, $r_\beta = 4$, and $r_\infty = 3$. Besides, according to Lemma 4 for all points $Q \in D_{i,y} \cap (\cup_{k=0}^2 L_k)$ we have $e_Q = 3$. Applying the Riemann–Hurwitz formula [3, Theorem II.5.9] to $\pi_{i,y}$, we eventually obtain $g(C_{i,y}) = 3r_y - 8$. □

2 New hash function

This paragraph clarifies how the $\mathbb{F}_q$-section $\varphi\colon \mathbb{A}^2_{(t_1,t_2)} \dashrightarrow T$ from Theorem 1 results in a constant-time map $h\colon \mathbb{F}_q^2 \to E_b(\mathbb{F}_q)$. First of all, for $a \in \mathbb{F}_q^*$ denote by $\left(\frac{a}{q}\right)_3 := a^{(q-1)/3}$ the *cubic residue symbol*, which is trivially a group homomorphism $\mathbb{F}_q^* \to \{\omega^i\}_{i=0}^2$.

Lemma 5 ([17, Remark 2.3])**.** *An element $a \in \mathbb{F}_q^*$ is a cubic residue if and only if $\left(\frac{a}{q}\right)_3 = 1$. Moreover, in this case*

$$\sqrt[3]{a} = \begin{cases} [18, \text{Proposition 1}] & \text{if} \quad q \equiv 1 \pmod 9 \text{ and } q \not\equiv 1 \pmod{27}, \\ a^{-(q-4)/9} = a^{(8q-5)/9} & \text{if} \quad q \equiv 4 \pmod 9, \\ a^{(q+2)/9} & \text{if} \quad q \equiv 7 \pmod 9. \end{cases}$$

To be definite, we put $\omega := \left(\frac{b}{q}\right)_3$ ($\neq 1$ by our assumption). Also, let us consider only $q \not\equiv 1 \pmod{27}$.

Letting $g_i := y_i^2 - b$ for $i \in \{0, 1, 2\}$, we get $T\colon \big\{g_j = b^j g_0 t_j^3$ for $j \in \{1, 2\}$. It is obvious that $\big\{\left(\frac{g_i}{q}\right)_3\big\}_{i=0}^2 = \{\omega^i\}_{i=0}^2$ whenever $g_i, t_j \in \mathbb{F}_q^*$. Besides, denote by $n \in \{0, 1, 2\}$ the position number of an element $t_1 \in \mathbb{F}_q^*$ in the set $\big\{\omega^i t_1\big\}_{i=0}^2$ ordered with respect to some order in $\mathbb{F}_q^*$. For example, if q is a prime, then this can be the usual numerical one.

One of crucial components of h is the auxiliary map

$$h'\colon T(\mathbb{F}_q) \to E_b(\mathbb{F}_q) \qquad h'(y_0, y_1, y_2, t_1, t_2) := \begin{cases} \left(\sqrt[3]{g_0},\ y_0\right) & \text{if} \quad g_0 = 0 \ \text{ or } \ \left(\frac{g_0}{q}\right)_3 = 1, \\ \left(\sqrt[3]{g_1},\ y_1\right) & \text{if} \quad \left(\frac{g_0}{q}\right)_3 = \omega^2, \\ \left(\sqrt[3]{g_2},\ y_2\right) & \text{if} \quad \left(\frac{g_0}{q}\right)_3 = \omega. \end{cases}$$

Unfortunately, in this form the value of h' is computed with the cost of two exponentiations in $\mathbb{F}_q$: the first for $\left(\frac{g_0}{q}\right)_3$ and the second for $\sqrt[3]{g_i}$. Instead, we give an equivalent definition of h' (up to the automorphisms $[\omega]^i$).

The case $q \equiv 4 \pmod 9$**.** Under this assumption

$$\left(\frac{\omega}{q}\right)_3 = \omega^{(q-1)/3} = \omega^{(q-4)/3} \cdot \omega = \omega^{3(q-4)/9} \cdot \omega = \omega.$$

Let $\theta := g_0^{(8q-5)/9}$ and $c_j := \sqrt[3]{(b/\omega)^j} \in \mathbb{F}_q^*$. We obtain

$$g_j = b^j g_0 t_j^3 = (c_j \theta t_j)^3 \qquad \text{if} \qquad \theta^3 = \omega^j g_0, \text{ i.e., } \left(\frac{g_0}{q}\right)_3 = \omega^{3-j}.$$

It is easily shown that

$$h'\colon T(\mathbb{F}_q) \to E_b(\mathbb{F}_q) \qquad h'(y_0, y_1, y_2, t_1, t_2) = \begin{cases} \left(\omega^n \theta,\ y_0\right) & \text{if} \quad \theta^3 = g_0, \\ \left(c_1 \theta t_1,\ y_1\right) & \text{if} \quad \theta^3 = \omega g_0, \\ \left(c_2 \theta t_2,\ y_2\right) & \text{if} \quad \theta^3 = \omega^2 g_0. \end{cases}$$

Since

$$\theta^3 = g_0^{-(q-4)/3} = g_0^{q-1-(q-4)/3} = g_0^{(2q+1)/3} = g_0^{2(q-1)/3} \cdot g_0,$$

this map is well defined everywhere on $T(\mathbb{F}_q)$. It is worth noting that θ can be computed with the cost of one exponentiation in $\mathbb{F}_q$ even if g_0 is given as a fraction u/v for $u \in \mathbb{F}_q$, $v \in \mathbb{F}_q^*$. Indeed,

$$\theta = (u/v)^{(8q-5)/9} = u^{(8q-5)/9} \cdot v^{(q-4)/9} = u^3 (u^8 v)^{(q-4)/9}. \tag{2}$$

The case $q \equiv 10 \pmod{27}$ **(relevant for BLS12-381).** Take any $\zeta := \sqrt[9]{1} \in \mathbb{F}_q^*$ such that $\zeta^3 = \omega$. In this case

$$\left(\frac{\zeta}{q}\right)_3 = \zeta^{(q-1)/3} = \omega^{(q-1)/9} = \omega^{(q-10)/9} \cdot \omega = \omega^{3(q-10)/27} \cdot \omega = \omega.$$

Let $\theta := g_0^{(2q+7)/27}$ and $c_j := \sqrt[3]{(b/\zeta)^j} \in \mathbb{F}_q^*$. Given $i \in \{0, 1, 2\}$ we obtain

$$g_j = b^j g_0 t_j^3 = (c_j \theta t_j)^3 / \omega^i \qquad \text{if} \qquad \theta^3 = \omega^i \zeta^j g_0, \text{ i.e., } \left(\frac{g_0}{q}\right)_3 = \omega^{3-j}.$$

It is easily shown that

$$h'\colon T(\mathbb{F}_q) \to E_b(\mathbb{F}_q) \qquad h'(y_0, y_1, y_2, t_1, t_2) = \begin{cases} \big(\omega^n\theta/\zeta^i,\ y_0\big) & \text{if} \quad \exists i\colon \theta^3 = \omega^i g_0, \\ \big(c_1\theta t_1/\zeta^i,\ y_1\big) & \text{if} \quad \exists i\colon \theta^3 = \omega^i \zeta g_0, \\ \big(c_2\theta t_2/\zeta^i,\ y_2\big) & \text{if} \quad \exists i\colon \theta^3 = \omega^i \zeta^2 g_0. \end{cases}$$

Since

$$\theta^3 = g_0^{(2q+7)/9} = g_0^{2(q-1)/9} \cdot g_0,$$

this map is well defined everywhere on $T(\mathbb{F}_q)$. It is worth noting that θ can be computed with the cost of one exponentiation in $\mathbb{F}_q$ even if g_0 is given as a fraction u/v for $u \in \mathbb{F}_q$, $v \in \mathbb{F}_q^*$. Indeed,

$$\begin{aligned} \theta = (u/v)^{(2q+7)/27} = u^{(2q+7)/27} \cdot v^{q-1-(2q+7)/27} = u^{(2q+7)/27} \cdot v^{(25q-34)/27} = \\ = u \cdot u^{2(q-10)/27} \cdot v^3 v^{5(5q-23)/27} = uv^8 (u^2 v^{25})^{(q-10)/27}. \end{aligned} \tag{3}$$

The cases $q \equiv 7 \pmod 9$ and $q \equiv 19 \pmod{27}$ are processed in a similar way. To be definite, throughout the rest of the article we will deal with the modified version of h'. Finally, we come to the map desired

$$h\colon \mathbb{F}_q^2 \to E_b(\mathbb{F}_q) \qquad h(t_1, t_2) := \begin{cases} P_0 & \text{if} \quad t_1 t_2 = 0, \\ \mathcal{O} & \text{if} \quad den(t_1, t_2) = 0, \\ (h' \circ \varphi)(t_1, t_2) & \text{otherwise.} \end{cases}$$

We emphasize that in the definition of h' (a fortiori, in φ) the cubic residue symbol does not appear. Further, by returning the value of h in (weighted) projective coordinates, we entirely avoid inversions in the field. Besides, the constants ω, c_j (and ζ, $\zeta^{-1} = \zeta^8$ if $q \equiv 10 \pmod{27}$) are found once at the precomputation stage. By the way, in the formulas (2), (3) we take $u := num_0^2 - b \cdot den^2$ and $v := den^2$. Calculating the value θ every time no matter whether $t_0 t_1 uv = 0$ or not, we eventually obtain

Remark 1. *The map h is computed in constant time, namely in that of one exponentiation in $\mathbb{F}_q$.*

3 Indifferentiability from a random oracle

Theorem 5. *For any point $P \in E_b(\mathbb{F}_q) \setminus \{\pm P_0, \mathcal{O}\}$ we have*

$$|\#h^{-1}(P) - (q+1)| \leqslant 7\lfloor 2\sqrt{q} \rfloor + 6, \qquad |\#h^{-1}(P_0) - 3q| \leqslant \lfloor 2\sqrt{q} \rfloor,$$

$$|\#h^{-1}(-P_0) - 2(q+1)| \leqslant 2\lfloor 2\sqrt{q} \rfloor, \qquad |\#h^{-1}(\mathcal{O}) - (q+1)| \leqslant \lfloor 2\sqrt{q} \rfloor.$$

Proof. All the inequalities follow from the Hasse–Weil–Serre bound [16, Theorem 5.3.1] for the number of $\mathbb{F}_q$-points on a projective non-singular absolutely irreducible $\mathbb{F}_q$-curve.

First, suppose that $h(t_1, t_2) = \pm P_0$. Then $t_1 t_2 = 0$ or $\theta = g_0 = 0$. In the first case, $h(0, t_2) = h(t_1, 0) = P_0$. In the second one, $(1 : t_1 : t_2) \in C_{0,\pm\sqrt{b}}$. These curves decompose as $C_{0,\sqrt{b}} = L_0 \cup F_0$ and $C_{0,-\sqrt{b}} = F_1 \cup F_2$, where F_k are Fermat cubics (cf. the equations (1)). The latter are obviously elliptic curves (of j-invariant 0). In accordance with Lemma 3 we have $(C_{0,\pm\sqrt{b}} \cap C_\infty)(\mathbb{F}_q) = \emptyset$. Note also that $(F_1 \cap F_2)(\mathbb{F}_q) = (L_i \cap F_k)(\mathbb{F}_q) = \emptyset$ for all $i, k \in \{0, 1, 2\}$.

In turn, $(C_\infty \cap L_k)(\mathbb{F}_q) = \emptyset$ according to Lemma 3, hence $h^{-1}(\mathcal{O}) = C_\infty(\mathbb{F}_q)$. Besides, $\mathrm{Sing}(C_\infty)(\mathbb{F}_q) = \emptyset$ (see Lemma 4). As a result, we obtain the bijection $\sigma_\infty \colon C'_\infty(\mathbb{F}_q) \xrightarrow{\sim} C_\infty(\mathbb{F}_q)$. Finally, the geometric genus $g(C_\infty) = 1$ by virtue of Theorem 4.

Now take $P = (x, y) \in E_b(\mathbb{F}_q) \setminus \{\pm P_0, \mathcal{O}\}$. The case $y = \beta$ does not occur, because $\beta^2 - b = 8b$ is not a cubic residue in $\mathbb{F}_q$. In compliance with Lemmas 2, 3 we see that

$$(C_{i,y} \cap C_\infty)(\mathbb{F}_q) = (C_{i,y} \cap C_{i+1,y})(\mathbb{F}_q) = (C_{i,y} \cap L_i)(\mathbb{F}_q) = \emptyset, \qquad \#(C_{i,y} \cap L_k)(\mathbb{F}_q) \leqslant 3$$

for all $i, k \in \{0, 1, 2\}$. Besides, the x-coordinates of $h(t_1, t_2)$ and $h(\omega t_1, t_2)$ (resp. $h(t_1, \omega t_2)$) are always different if $i \in \{0, 1\}$ (resp. $i = 2$), because $\theta(t_1, t_2) = \theta(\omega t_1, t_2) = \theta(t_1, \omega t_2)$. Therefore

$$h^{-1}\big(\{P, [\omega](P), [\omega]^2(P)\}\big) \;=\; \bigsqcup_{i=0}^{2} h^{-1}\big([\omega]^i(P)\big) \;=\; \bigsqcup_{i=0}^{2} C_{i,y}(\mathbb{F}_q) \setminus (L_{i-1} \cup L_{i+1}).$$

Since $\#h^{-1}\big([\omega]^i(P)\big) = \#h^{-1}\big([\omega]^{i+1}(P)\big)$, we obtain

$$3 \cdot \#h^{-1}(P) = \sum_{i=0}^{2} \#C_{i,y}(\mathbb{F}_q) \setminus (L_{i-1} \cup L_{i+1}).$$

Consequently,

$$\sum_{i=0}^{2} (\#C_{i,y}(\mathbb{F}_q) - 6) \leqslant 3 \cdot \#h^{-1}(P) \leqslant \sum_{i=0}^{2} \#C_{i,y}(\mathbb{F}_q).$$

Further, $\#C_{i,y}(\mathbb{F}_q) = \#C_{i+1,y}(\mathbb{F}_q)$ according to Lemma 2. Thus

$$3(\#C_{i,y}(\mathbb{F}_q) - 6) \leqslant 3 \cdot \#h^{-1}(P) \leqslant 3 \cdot \#C_{i,y}(\mathbb{F}_q)$$

and hence

$$|\#h^{-1}(P) - \#C_{i,y}(\mathbb{F}_q)| \leqslant 6.$$

At the same time, Theorem 4 says that $g(C_{i,y}) = 7$. Besides, $\mathrm{Sing}(C_{i,y})(\mathbb{F}_q) = \emptyset$ (see Lemma 4). As a result, $\sigma_{i,y} \colon C'_{i,y}(\mathbb{F}_q) \xrightarrow{\sim} C_{i,y}(\mathbb{F}_q)$. We eventually obtain

$$|\#h^{-1}(P) - (q+1)| \leqslant |\#h^{-1}(P) - \#C_{i,y}(\mathbb{F}_q)| + |\#C_{i,y}(\mathbb{F}_q) - (q+1)| \leqslant 6 + 7\lfloor 2\sqrt{q} \rfloor.$$

The theorem is proved. □

Corollary 1. *The map $h \colon \mathbb{F}_q^2 \to E_b(\mathbb{F}_q)$ is surjective at least for $q \geqslant 211$.*

Corollary 2. *The distribution on $E_b(\mathbb{F}_q)$ defined by h is ϵ-statistically indistinguishable from the uniform one* [8, Definition 3]*, where $\epsilon := 16q^{-1/2} + O(q^{-1})$.*

Proof. For any point $P \in E_b(\mathbb{F}_q)$ put

$$\delta(P) := \left|\frac{\#h^{-1}(P)}{q^2} - \frac{1}{\#E_b(\mathbb{F}_q)}\right| \leqslant \left|\frac{\#h^{-1}(P)}{q^2} - \frac{1}{q}\right| + \left|\frac{1}{q} - \frac{1}{\#E_b(\mathbb{F}_q)}\right| =$$
$$= \frac{|\#h^{-1}(P) - q|}{q^2} + \frac{|\#E_b(\mathbb{F}_q) - q|}{q \cdot \#E_b(\mathbb{F}_q)} \leqslant \frac{|\#h^{-1}(P) - q|}{q^2} + \frac{\lfloor 2\sqrt{q}\rfloor + 1}{q(q + 1 - \lfloor 2\sqrt{q}\rfloor)} =$$
$$= \frac{|\#h^{-1}(P) - q|}{q^2} + \frac{2}{q^{3/2}} + O\Big(\frac{1}{q^2}\Big).$$

If $P \notin \{\pm P_0, \mathcal{O}\}$ from Theorem 5 we obtain

$$\delta(P) = \frac{16}{q^{3/2}} + O\Big(\frac{1}{q^2}\Big).$$

Similarly,

$$\delta(P_0) = \frac{2}{q} + O\Big(\frac{1}{q^{3/2}}\Big), \qquad \delta(-P_0) = \frac{1}{q} + O\Big(\frac{1}{q^{3/2}}\Big), \qquad \delta(\mathcal{O}) = \frac{4}{q^{3/2}} + O\Big(\frac{1}{q^2}\Big).$$

Thus

$$\sum_{P \in E_b(\mathbb{F}_q)} \delta(P) \leqslant (q + \lfloor 2\sqrt{q}\rfloor - 2)\Big(\frac{16}{q^{3/2}} + O\Big(\frac{1}{q^2}\Big)\Big) + \frac{3}{q} + O\Big(\frac{1}{q^{3/2}}\Big) = \frac{16}{q^{1/2}} + O\Big(\frac{1}{q}\Big).$$

The corollary is proved. □

For $t_2 \in \mathbb{F}_q$ consider the encoding $h_{t_2} \colon \mathbb{F}_q \to E_b(\mathbb{F}_q)$ of the form $h_{t_2}(t_1) := h(t_1, t_2)$. By definition, $h_0(t_1) = P_0$ for any $t_1 \in \mathbb{F}_q$. Nevertheless, by analogy with [10, Theorem 2] we can prove the next lemma. Its main difference is that $h_{t_2}(t_1) = h_{t_2}(\omega t_1)$ whenever $\sqrt[3]{g_2} \in \mathbb{F}_q$, hence 10 appears instead of 6.

Lemma 6. *For $t_2 \in \mathbb{F}_q^*$ and $P \in E_b(\mathbb{F}_q)$ we have $\#h_{t_2}^{-1}(P) \leqslant 10$ and hence $q/10 \leqslant \#\mathrm{Im}(h_{t_2})$.*

By this lemma [8, Algorithm 1] still works well in the case of h. Indeed, for $P \in E_b(\mathbb{F}_q)$ pick uniformly at random $t_2 \in \mathbb{F}_q$ and then find uniformly at random $t_1 \in h_{t_2}^{-1}(P)$. This gives

Remark 2. *The map h is samplable* [8, Definition 4].

Remarks 1, 2 and Corollary 2 imply that h is *admissible* in the sense of [8, Definition 4]. Finally, using [8, Theorem 1], we establish

Corollary 3. *Consider the composition $H := h \circ \mathfrak{h} \colon \{0,1\}^* \to E_b(\mathbb{F}_q)$ of a hash function $\mathfrak{h} \colon \{0,1\}^* \to \mathbb{F}_q^2$ and h. The hash function H is indifferentiable from a random oracle if $\mathfrak{h}$ is so.*

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] Y. Sakemi et al., *Pairing-friendly curves*, https://datatracker.ietf.org/doc/draft-irtf-cfrg-pairing-friendly-curves, 2020.

[3] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, **106**, Springer, New York, 2009.

[4] 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.

[5] D. Boneh et al., "Aggregate and verifiably encrypted signatures from bilinear maps", Advances in Cryptology — EUROCRYPT 2003, LNCS, **2656**, ed. E. Biham, Springer, Berlin, 2003, 416–432.

[6] D. Boneh et al., *BLS signatures*, https://datatracker.ietf.org/doc/draft-irtf-cfrg-bls-signature, 2020.

[7] A. Faz-Hernandez et al., *Hashing to elliptic curves*, https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve, 2020.

[8] 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.

[9] D. Bernstein et al., "Elligator: Elliptic-curve points indistinguishable from uniform random strings", ACM SIGSAC Conference on Computer & Communications Security, 2013, 967–980.

[10] D. Koshelev, *Efficient indifferentiable hashing to elliptic curves $y^2 = x^3 + b$ provided that b is a quadratic residue*, ePrint IACR 2020/1070.

[11] M. Skałba, "Points on elliptic curves over finite fields", *Acta Arithmetica*, **117**:3 (2005), 293–301.

[12] K. Oguiso, T. Truong, "Explicit examples of rational and Calabi–Yau threefolds with primitive automorphisms of positive entropy", *Journal of Mathematical Sciences, the University of Tokyo*, **22** (2015), 361–385.

[13] D. Koshelev, *Magma code*, https://github.com/dishport/Indifferentiable-hashing-to-ordinary-elliptic-curves-of-j-0-with-the-cost-of-one-exponentiation, 2021.

[14] K. Hulek, R. Kloosterman, "Calculating the Mordell-Weil rank of elliptic threefolds and the cohomology of singular hypersurfaces", *Annales de l'Institut Fourier*, **61**:3 (2011), 1133–1179.

[15] M. Schütt, T. Shioda, *Mordell–Weil lattices*, A Series of Modern Surveys in Mathematics, **70**, Springer-Verlag, Singapore, 2019.

[16] H. Stichtenoth, *Algebraic function fields and codes*, Graduate Texts in Mathematics, **254**, Springer, Berlin, 2009.

[17] A. Dudeanu, G.-R. Oancea, S. Iftene, "An x-coordinate point compression method for elliptic curves over $\mathbb{F}_p$", International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, 2010, 65–71.

[18] G. Cho et al., "New cube root algorithm based on the third order linear recurrence relations in finite fields", *Designs, Codes and Cryptography*, **75**:3 (2015), 483–495.