

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

Dmitrii Koshelev¹

Computer sciences and networks department, Télécom Paris

Abstract. Let \mathbb{F}_q be a finite field and $E_b: y^2 = x^3 + b$ 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 curves BLS12-381 ($b = 4$) and BLS12-377 ($b = 1$) and for the group \mathbb{G}_2 of the curve BW6-761 ($b = 4$). The curves mentioned are a de facto standard in the real world pairing-based cryptography at the moment. This article provides a new constant-time hash function $H: \{0, 1\}^* \rightarrow E_b(\mathbb{F}_q)$ 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 given in [2, §4.1].

Let \mathbb{F}_q be a finite field of $\text{char}(\mathbb{F}_q) > 3$ and $E_b: y^2 = x^3 + b$ 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 ordinarity 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 curves* in the industry are the Barreto–Lynn–Scott curves BLS12-381 [4, §2.1], BLS12-377 [5] and the Brezing–Weng curve BW6-761 [6, §3], where the numbers after - equal $\lceil \log_2(q) \rceil$.

Many pairing-based protocols (for example, the BLS multi-signature [7, §3], [8]) use a hash function of the form $H: \{0, 1\}^* \rightarrow E_b(\mathbb{F}_q)$. There is the regularly updated draft [9] (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* [10, Definition 2] and *constant-time*, that is the computation time of its value is independent of an input argument.

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

Almost all such previously proposed hash functions are obtained as the composition $H := e^{\otimes 2} \circ \mathfrak{h}$ of a hash function $\mathfrak{h}: \{0, 1\}^* \rightarrow \mathbb{F}_q^2$ and the tensor square

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

of some map $e: \mathbb{F}_q \rightarrow E_b(\mathbb{F}_q)$. Such a map is often called *encoding*. In this case the indifferenciability of H follows from [10, Theorem 1] if \mathfrak{h} is indifferenciability and $e^{\otimes 2}$ is *admissible* in the sense of [10, Definition 4]. The fastest known encodings are Elligator 2 [11, §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 [12]. More precisely, 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 $h: \mathbb{F}_q^2 \rightarrow E_b(\mathbb{F}_q)$ 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 the given 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.

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 $\omega \neq 1$. Further, for the sake of being definite, suppose that $\sqrt[3]{b} \notin \mathbb{F}_q$. The opposite case is much simpler, hence results of the article can be extended to it without problems. For $i \in \{0, 1, 2\}$ consider the elliptic curves $E_b^{(i)}: y_i^2 = b^i x_i^3 + b \simeq_{\mathbb{F}_q} E_{b^{2i+1}}$. Note that $E_b^{(1)}, E_b^{(2)}$ are two different cubic \mathbb{F}_q -twists of $E_b = E_b^{(0)}$.

There is on $E_b^{(i)}$ 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 [13, §1.3]. It is readily seen that it has the affine \mathbb{F}_q -model

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

where $t_j := x_j/x_0$. By the way, the famous SWU (Shallue–van de Woestijne–Ulas) encoding [1, §8.3.4] deals with another Calabi–Yau \mathbb{F}_q -threefold.

We can look at T as an $\mathbb{F}_q(t_1, t_2)$ -curve given as the intersection of two quadratic $\mathbb{F}_q(t_1, t_2)$ -surfaces, where $\mathbb{F}_q(t_1, t_2)$ denotes the rational function field in two variables t_1, t_2 over the constant field \mathbb{F}_q . Below it will be convenient to use the auxiliary variables $s_j := t_j^3$.

Theorem 1 ([14]). *T over $\mathbb{F}_q(t_1, t_2)$ is an elliptic curve having a Weierstrass form $W: y^2 = x^3 + a_4x + a_6$ with the coefficients*

$$\begin{aligned} a_4 &:= -3(b^2 s_1 s_2 + \omega^2 s_1 + \omega b s_2)(b^2 s_1 s_2 + \omega s_1 + \omega^2 b s_2), \\ a_6 &:= -(b^2 s_1 s_2 - 2s_1 + b s_2)(2b^2 s_1 s_2 - s_1 - b s_2)(b^2 s_1 s_2 + s_1 - 2b s_2). \end{aligned}$$

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

$$\begin{aligned}\Delta &= (3^3 b s_1 s_2 (b s_1 - 1) (b^2 s_2 - 1) (s_1 - b s_2))^2, \\ j &= 2^8 3^6 (b^2 s_1 s_2 + \omega s_1 + \omega^2 b s_2)^3 (b^2 s_1 s_2 + \omega^2 s_1 + \omega b s_2)^3 / \Delta.\end{aligned}$$

Theorem 2 ([14]). *There is on W the $\mathbb{F}_q(t_1, t_2)$ -point*

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

It corresponds to an $\mathbb{F}_q(t_1, t_2)$ -point φ on T whose the coordinates are the irreducible fractions $y_i(t_1, t_2) := \text{num}_i / \text{den}$, where

$$\begin{aligned}\text{num}_0 &:= \sqrt{b} \cdot (b^2 s_1^2 - 2b^3 s_1 s_2 + 2b s_1 + b^4 s_2^2 + 2b^2 s_2 - 3), \\ \text{num}_1 &:= \sqrt{b} \cdot (-3b^2 s_1^2 + 2b^3 s_1 s_2 + 2b s_1 + b^4 s_2^2 - 2b^2 s_2 + 1), \\ \text{num}_2 &:= \sqrt{b} \cdot (b^2 s_1^2 + 2b^3 s_1 s_2 - 2b s_1 - 3b^4 s_2^2 + 2b^2 s_2 + 1), \\ \text{den} &:= b^2 s_1^2 - 2b^3 s_1 s_2 - 2b s_1 + b^4 s_2^2 - 2b^2 s_2 + 1.\end{aligned}$$

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 [12, Theorem 1]. The frequent case $b = 4$ gives

$$\begin{aligned}\text{num}_0 &= 2 \cdot (2^4 s_1^2 - 2^7 s_1 s_2 + 2^3 s_1 + 2^8 s_2^2 + 2^5 s_2 - 3), \\ \text{num}_1 &= 2 \cdot (-2^4 3 s_1^2 + 2^7 s_1 s_2 + 2^3 s_1 + 2^8 s_2^2 - 2^5 s_2 + 1), \\ \text{num}_2 &= 2 \cdot (2^4 s_1^2 + 2^7 s_1 s_2 - 2^3 s_1 - 2^8 3 s_2^2 + 2^5 s_2 + 1), \\ \text{den} &= 2^4 s_1^2 - 2^7 s_1 s_2 - 2^3 s_1 + 2^8 s_2^2 - 2^5 s_2 + 1.\end{aligned}$$

In other words, T is an *elliptic threefold* (see, e.g., [15]) whose the elliptic fibration is the projection to t_1, t_2 . In these terms, $\varphi: \mathbb{A}_{(t_1, t_2)}^2 \dashrightarrow T$ is an \mathbb{F}_q -section of the given fibration. In particular, $\text{Im}(\varphi)$ is a *rational \mathbb{F}_q -surface*.

For the sake of compactness we put

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

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 $\mathbb{P}_{(t_0, t_1, t_2)}^2$ the pencil of the \mathbb{F}_q -sextics

$$C_{i, y}: \text{Num}_i = \text{Den} \cdot y, \quad C_{i, \infty} = C_\infty: \text{Den} = 0$$

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

$$\pi: \mathbb{P}^2 \rightarrow \mathbb{P}^2 \quad \pi(t_0 : t_1 : t_2) := (t_0^3 : t_1^3 : t_2^3).$$

Also, let $L_i: t_i = 0$,

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

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

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

Below we formulate a few simple lemmas, which are readily checked.

Lemma 1. *The order 3 projective \mathbb{F}_q -transformations*

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

give the isomorphisms

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

as well as

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

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

$$C_{0,\sqrt{b}}: t_0^3(t_0^3 - bt_1^3 - b^2t_2^3) = 0, \quad C_{0,-\sqrt{b}}: (t_0^3 - bt_1^3 + b^2t_2^3)(t_0^3 + bt_1^3 - b^2t_2^3) = 0. \quad (1)$$

Lemma 2. *There are the following equalities. First,*

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

Second,

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

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

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

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

Lemma 3. *The set of singular points*

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

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

Lemma 4. 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 [14]. In compliance with Lemma 3 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

$$\varphi_k: C_{i,y} \simeq C_{i,y} \quad \varphi_0 := (\omega t_0 : t_1 : t_2), \quad \varphi_1 := (t_0 : \omega t_1 : t_2), \quad \varphi_2 := (t_0 : t_1 : \omega t_2).$$

Since they are of order 3, for any $k, \ell, m \in \{0, 1, 2\}$, $\ell \neq m$ the case $\varphi_k: F_\ell \simeq F_m, F_m \simeq F_\ell$ is not possible, otherwise $F_\ell = F_m$. Also, given ℓ note that $\varphi_k: F_\ell \simeq F_\ell$ 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 φ_k for some k . Note that we can take $k = 0$ without loss of generality.

It is checked in [14] 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 $\sigma_{i,y}: C'_{i,y} \rightarrow C_{i,y}$ be the corresponding normalization morphisms. As is well known,

$$\#\sigma_{i,y}^{-1}(\mathbf{Q}_i) = \#\sigma_{i,\beta}^{-1}(R_i) = \#\sigma_\infty^{-1}(\mathbf{Q}_k) = 3, \quad \sigma_{i,y}: C'_{i,y} \setminus \sigma_{i,y}^{-1}(\text{Sing}(C_{i,y})) \simeq C_{i,y} \setminus \text{Sing}(C_{i,y}).$$

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

Theorem 3. For $y \notin \{\beta, \infty\}$ the geometric genus $g(C_{i,y}) = 7$. In turn, $g(C_{i,\beta}) = 4$ and $g(C_\infty) = 1$.

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 1, 2 it follows that

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

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 3 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 $g(C_{i,y}) = 3r_y - 8$. \square

2 New hash function

This paragraph clarifies how the \mathbb{F}_q -section $\varphi: \mathbb{A}_{(t_1, t_2)}^2 \dashrightarrow T$ from Theorem 2 results in a constant-time map $h: \mathbb{F}_q^2 \rightarrow E_b(\mathbb{F}_q)$. 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 $\mathbb{F}_q^* \rightarrow \{\omega^i\}_{i=0}^2$.

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*

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

Without loss of generality we will assume that $\left(\frac{b}{q}\right)_3 = \omega$ rather than ω^2 . 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 $T: \{g_j = b^j g_0 t_j^3 \text{ for } j \in \{1, 2\}\}$. It is obvious that $\left\{\left(\frac{g_i}{q}\right)_3\right\}_{i=0}^2 = \{\omega^i\}_{i=0}^2$ 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 $\{\omega^i t_1\}_{i=0}^2$ 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

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

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 $q \equiv 4 \pmod{9}$ (relevant for BW6-761). 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

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

It is easily shown that

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

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,

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

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

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

It is easily shown that

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

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 $q \equiv 7 \pmod{9}$ (relevant for BLS12-377) 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, for any $t_1, t_2 \in \mathbb{F}_q$ we put

$$h(t_1, t_2) := \begin{cases} P_0 & \text{if } t_1 t_2 = 0, \\ \mathcal{O} & \text{if } \text{den}(t_1, t_2) = 0, \\ (h' \circ \varphi)(t_1, t_2) & \text{otherwise.} \end{cases}$$

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 $u := \text{num}_0^2 - b \cdot \text{den}^2$ and $v := \text{den}^2$. Calculating the value θ every time no matter whether $t_0 t_1 uv = 0$ or not, we eventually obtain

Remark 1. *The map $h: \mathbb{F}_q^2 \rightarrow E_b(\mathbb{F}_q)$ is computed in constant time, namely in that of one exponentiation in \mathbb{F}_q .*

3 Indifferentiability from a random oracle

Theorem 4. *For any point $P \in E_b(\mathbb{F}_q) \setminus \{\pm P_0, \mathcal{O}\}$ we have*

$$\begin{aligned} |\#h^{-1}(P) - (q+1)| &\leq 7\lfloor 2\sqrt{q} \rfloor + 6, & |\#h^{-1}(P_0) - 3q| &\leq \lfloor 2\sqrt{q} \rfloor, \\ |\#h^{-1}(-P_0) - 2(q+1)| &\leq 2\lfloor 2\sqrt{q} \rfloor, & |\#h^{-1}(\mathcal{O}) - (q+1)| &\leq \lfloor 2\sqrt{q} \rfloor. \end{aligned}$$

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, $(1 : t_1 : t_2) \in C_{0, \pm\sqrt{b}}$. More precisely, these curves (given by Equations (1)) 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. The latter are obviously elliptic curves (of j -invariant 0). In accordance with Lemma 2 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 2, hence $h^{-1}(\mathcal{O}) = C_\infty(\mathbb{F}_q)$. Besides, $\text{Sing}(C_\infty)(\mathbb{F}_q) = \emptyset$ (see Lemma 3). As a result, we obtain the bijection $\sigma_\infty : C'_\infty(\mathbb{F}_q) \xrightarrow{\sim} C_\infty(\mathbb{F}_q)$. Finally, the geometric genus $g(C_\infty) = 1$ by virtue of Theorem 3.

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 1, 2 we see that

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

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

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

where $[\omega]^*(P) := \{P, [\omega](P), [\omega]^2(P)\}$. Since $\#h^{-1}([\omega]^i(P)) = \#h^{-1}([\omega]^{i+1}(P))$, 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,

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

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

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

and hence

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

At the same time, Theorem 3 says that $g(C_{i,y}) = 7$. Besides, $\text{Sing}(C_{i,y})(\mathbb{F}_q) = \emptyset$ (see Lemma 3). As a result, $\sigma_{i,y}: C'_{i,y}(\mathbb{F}_q) \simeq C_{i,y}(\mathbb{F}_q)$. We eventually obtain

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

The theorem is proved. \square

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

Corollary 2. *The distribution on $E_b(\mathbb{F}_q)$ defined by h is ϵ -statistically indistinguishable from the uniform one [10, Definition 3], where $\epsilon := 16q^{-1/2} + O(q^{-1})$.*

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

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

If $P \notin \{\pm P_0, \mathcal{O}\}$ from Theorem 4 we obtain

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

Similarly,

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

Thus

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

The corollary is proved. \square

Further, [10, Algorithm 1] still works well in our case. Indeed, for $P \in E_b(\mathbb{F}_q)$ pick uniformly at random $t_1 \in \mathbb{F}_q$ and then find uniformly at random $t_2 \in \mathbb{F}_q$ such that $(t_1, t_2) \in h^{-1}(P)$. This gives

Remark 2. *The map $h: \mathbb{F}_q^2 \rightarrow E_b(\mathbb{F}_q)$ is samplable [10, Definition 4].*

Remarks 1, 2 and Corollary 2 imply that h is *admissible* in the sense of [10, Definition 4]. Finally, using [10, Theorem 1], we establish

Corollary 3. *Consider the composition $H := h \circ \mathfrak{h}: \{0, 1\}^* \rightarrow E_b(\mathbb{F}_q)$ of a hash function $\mathfrak{h}: \{0, 1\}^* \rightarrow \mathbb{F}_q^2$ 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] A. Vlasov, *EIP-2539: BLS12-377 curve operations*, <https://eips.ethereum.org/EIPS/eip-2539>, 2020.
- [6] Y. El Housni, A. Guillevic, “Optimized and secure pairing-friendly elliptic curves suitable for one layer proof composition”, *CANS 2020: Cryptology and Network Security*, LNCS, **12579**, ed. S. Krenn, H. Shulman, S. Vaudenay, Springer, Cham, 2020, 259–279.
- [7] 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.
- [8] D. Boneh et al., *BLS signatures*, <https://datatracker.ietf.org/doc/draft-irtf-cfrg-bl-signature>, 2020.
- [9] A. Faz-Hernandez et al., *Hashing to elliptic curves*, <https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve>, 2020.
- [10] 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.
- [11] D. Bernstein et al., “Elligator: Elliptic-curve points indistinguishable from uniform random strings”, *ACM SIGSAC Conference on Computer & Communications Security*, 2013, 967–980.
- [12] D. Koshelev, *Efficient indifferentiable hashing to elliptic curves $y^2 = x^3 + b$ provided that b is a quadratic residue*, ePrint IACR 2020/1070.
- [13] 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.
- [14] D. Koshelev, *Magma code*, <https://github.com/dishport/Indifferentiable-hashing-to-ordinary-elliptic-curves-of-j-0-with-the-cost-of-one-exponentiation>, 2021.
- [15] 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.
- [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.