Efficient indifferentiable hashing to elliptic curves $y^2 = x^3 + b$ provided that b is a quadratic residue

Dmitrii Koshelev [1]

Versailles Laboratory of Mathematics, Versailles Saint-Quentin-en-Yvelines University
Center for Research and Advanced Development, Infotecs

Abstract. Let $\mathbb{F}_q$ be a finite field and $E_b\colon y^2 = x^3 + b$ be an ordinary elliptic $\mathbb{F}_q$-curve of j-invariant 0 such that $\sqrt{b} \in \mathbb{F}_q$. In particular, this condition is fulfilled for the curve BLS12-381 and for one of sextic twists of the curve BW6-761 (in both cases $b = 4$). These curves are very popular in pairing-based cryptography. The article provides an efficient constant-time encoding $h\colon \mathbb{F}_q \to E_b(\mathbb{F}_q)$ of an absolutely new type for which $q/6 \leqslant \#\mathrm{Im}(h)$. We prove that at least for $q \equiv 4 \pmod 9$ the hash function $H\colon \{0,1\}^* \to E_b(\mathbb{F}_q)$ induced by h is indifferentiable from a random oracle. The main idea of our encoding consists in extracting in $\mathbb{F}_q$ (for $q \equiv 1 \pmod 3$) a cubic root instead of a square root as in the well known (universal) SWU encoding and in its simplified analogue. Besides, the new hashing can be implemented without quadratic and cubic residuosity tests (as well as without inversions) in $\mathbb{F}_q$. Thus in addition to the protection against timing attacks, H is much more efficient than the SWU hash function, which generally requires to perform 4 quadratic residuosity tests in $\mathbb{F}_q$. For instance, in the case of BW6-761 this allows to avoid approximately $4 \cdot 761 \approx 3000$ field multiplications.

Key words: cubic residue symbol and cubic roots, elliptic surfaces, hashing to elliptic curves, indifferentiability from a random oracle, pairing-based cryptography.

Introduction

Many protocols of *pairing-based cryptography* [1] use a hash function $H\colon \{0,1\}^* \to E_b(\mathbb{F}_q)$ *indifferentiable from a random oracle* [2, Definition 2]. In particular, H should be *constant-time*, i.e., the computation time of its value is independent of an input argument. The latter is necessary in order 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].

In practice, almost all hash functions H are induced from some mapping $h\colon \mathbb{F}_q \to E_b(\mathbb{F}_q)$, called *encoding*, such that $\#\mathrm{Im}(h) = \Theta(q)$. Here $q \approx \#E_b(\mathbb{F}_q)$ according to the Hasse inequality [4, Theorem V.1.1]. In other words, h should cover most $\mathbb{F}_q$-points of E_b. However there are no surjective encodings h for ordinary (i.e., non-supersingular) curves E_b. As is well known, only such curves are applied in pairing-based cryptography. Thus the trivial composition $h \circ \mathfrak{h}$ with a hash function $\mathfrak{h}\colon \{0,1\}^* \to \mathbb{F}_q$ is not appropriate.

Instead, it is often considered the composition $H := h^{\otimes 2} \circ \mathfrak{h}$ of a hash function $\mathfrak{h}\colon \{0,1\}^* \to \mathbb{F}_q^2$ and the tensor square

$$h^{\otimes 2}\colon \mathbb{F}_q^2 \to E_b(\mathbb{F}_q), \qquad h^{\otimes 2}(t,t') := h(t) + h(t').$$

[1] web page: https://www.researchgate.net/profile/Dimitri_Koshelev
email: dishport@yandex.ru
This work was supported by a public grant as part of the FMJH project

In this case the indifferentiability of H follows from [2, Theorem 1] if $\mathfrak{h}$ 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 $\mathbb{F}_q$-curve (not necessarily of $j = 0$). Nevertheless, it generally requires the computation of two 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 the exponentiation in $\mathbb{F}_q$. 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 with $j(E) \neq 0$. The most difficult case $j(E) = 1728$ is processed in [6]. Besides, it exists for E_b in the case $\sqrt[3]{b} \in \mathbb{F}_q$, that is $2 \mid \#E_b(\mathbb{F}_q)$ (see [7, Remark in §2]). Therefore throughout the article we will assume the converse. However at the moment the encoding is still not applicable to some curves E_b, including the sextic twist (with $b = 4$) of the curve BW6-761 from [8].

The simplified SWU encoding is sometimes constructed by means of a vertical $\mathbb{F}_q$-isogeny (the Wahby–Boneh approach [9]) or $\mathbb{F}_{q^2}$-isogeny (the Koshelev approach [5]) $\psi\colon E \to E_b$ of small degree d. For example, the curve BLS12-381 (also with $b = 4$) [9, §2.1] benefits from a vertical $\mathbb{F}_q$-isogeny of degree $d = 11$. More precisely, for ψ defined over $\mathbb{F}_q$ (unlike that over $\mathbb{F}_{q^2}$) the encoding can be realized simply as the composition $h := \psi \circ h'\colon \mathbb{F}_q \to E_b(\mathbb{F}_q)$, where $h'\colon \mathbb{F}_q \to E(\mathbb{F}_q)$.

The disadvantage of using such isogenies is increasing the computational time of h as $d \to \infty$, even though this correlation is linear. Indeed, since $2 \nmid \#E_b(\mathbb{F}_q)$, it is sufficient to assume that $2 \nmid d$. According to Vélu's formulas [10, §12.3] we have

$$\psi(x, y) = \left(\frac{\psi_0(x)}{\psi_1(x)},\ y\frac{\psi_2(x)}{\psi_3(x)}\right),$$

where ψ_i are polynomials of degrees

$$\deg(\psi_0) = d, \qquad \deg(\psi_1) = d - 1, \qquad \deg(\psi_2) = \deg(\psi_3) = 3(d-1)/2.$$

Thus the computing ψ requires $\approx 5d$ field multiplications if Horner's method is applied to evaluate ψ_i.

As a consequence, new constructions of efficient constant-time encodings $h\colon \mathbb{F}_q \to E_b(\mathbb{F}_q)$ are desirable in order to be independent of the existence of isogenies. The given work discovers one such encoding provided that $\sqrt{b} \in \mathbb{F}_q$. We also prove that $h^{\otimes 2}$ is admissible (at least for $q \equiv 4 \pmod 9$) and hence the corresponding hash function $H\colon \{0,1\}^* \to E_b(\mathbb{F}_q)$ is indifferentiable from a random oracle.

1 Geometric results

We everywhere assume that $\mathrm{char}(\mathbb{F}_q) > 3$ and $q \equiv 1 \pmod 3$, i.e., $\omega := \sqrt[3]{1} \in \mathbb{F}_q^*$, where $\omega \neq 1$. By virtue of [4, Example V.4.4] this is true if E_b is an ordinary elliptic curve. Further, for $i \in \{0, 1, 2\}$ consider the elliptic curves $E_b^{(i)}\colon y_i^2 = b^i x_i^3 + b$. 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 $[\omega]\colon (x_i, y_i) \mapsto (\omega x_i, y_i)$ of order 3.

Take the quotient $T := (E_b \times E_b^{(1)} \times E_b^{(2)})/[\omega]^{\times 3}$, which is a *Calabi–Yau threefold* according to [11, §1.3]. It is readily seen that it has the affine model

$$T\colon \begin{cases} y_1^2 - b = bt_1^3(y_0^2 - b), \\ y_2^2 - b = b^2 t_2^3 (y_0^2 - b) \end{cases} \quad \subset \quad \mathbb{A}^5_{(y_0,y_1,y_2,t_1,t_2)},$$

where $t_j := x_j/x_0$. By the way, the SWU encoding deals with another Calabi–Yau $\mathbb{F}_q$-threefold.

Putting $t := t_1 = t_2$, we obtain the $\mathbb{F}_q(t)$-curve given as the intersection of two quadratic $\mathbb{F}_q(t)$-surfaces

$$\mathcal{E}\colon \begin{cases} y_1^2 - b = bt^3(y_0^2 - b), \\ y_2^2 - b = b^2 t^3 (y_0^2 - b) \end{cases} \quad \subset \quad \mathbb{A}^3_{(y_0,y_1,y_2)},$$

where $\mathbb{F}_q(t)$ denotes the rational function field in one variable t over the constant field $\mathbb{F}_q$.

Lemma 1 ([12]). *$\mathcal{E}$ is an elliptic $\mathbb{F}_q(t)$-curve of j-invariant*

$$256 \cdot \frac{\big(b^4t^6 - b^2(b+1)t^3 + b^2 - b + 1\big)^3}{\big(b(b-1)(b^2t^3-1)(bt^3-1)\big)^2}.$$

In other words, $\mathcal{E} \subset \mathbb{A}^4_{(y_0,y_1,y_2,t)}$ is an *elliptic $\mathbb{F}_q$-surface* (see, e.g., [13, Chapter III]), whose the elliptic fibration is the projection to t. In [10, §2.5.4] it is described how to transform $\mathcal{E}$ into Weierstrass form.

Using the theory of the *Mordell–Weil lattices* of elliptic $\mathbb{F}_q$-surfaces, we establish the following result, which can be readily checked. At the same time, in order not to complicate the text we do not explain how exactly the formulas are derived.

Theorem 1 ([12]). *$\mathcal{E}$ has the $\mathbb{F}_q(t)$-point (i.e., $\mathbb{F}_q$-section) φ, whose the coordinates are the irreducible fractions $y_i(t) := num_i(t)/den(t)$, where*

$$\begin{aligned} num_0(t) &:= \sqrt{b} \cdot \big(-b^2(b-1)^2 \cdot t^6 - 2b(b+1) \cdot t^3 + 3\big), \\ num_1(t) &:= \sqrt{b} \cdot \big(b^2(b+3)(b-1) \cdot t^6 - 2b(b-1) \cdot t^3 + 1\big), \\ num_2(t) &:= \sqrt{b} \cdot \big(b^2(3b+1)(b-1) \cdot t^6 - 2b(b-1) \cdot t^3 - 1\big), \\ den(t) &:= b^2(b-1)^2 \cdot t^6 - 2b(b+1) \cdot t^3 + 1. \end{aligned}$$

Moreover, $y_0(t) - y_1(t) + y_2(t) = \sqrt{b}$.

For the frequent case $b = 4$ we obtain

$$\begin{aligned} num_0(t) &= 2 \cdot \big(-2^4 3^2 \cdot t^6 - 2^3 5 \cdot t^3 + 3\big), \qquad & num_1(t) &= 2 \cdot \big(2^4 3 \cdot 7 \cdot t^6 - 2^3 3 \cdot t^3 + 1\big), \\ num_2(t) &= 2 \cdot \big(2^4 3 \cdot 13 \cdot t^6 - 2^3 3 \cdot t^3 - 1\big), \qquad & den(t) &= 2^4 3^2 \cdot t^6 - 2^3 5 \cdot t^3 + 1. \end{aligned}$$

Consider the $\mathbb{F}_q$-curves

$$C_i\colon \begin{cases} y^2 = x^3 + b, \\ den(t)y = num_i(t) \end{cases} \quad \subset \quad \mathbb{A}^3_{(t,x,y)}.$$

We will identify C_i with their projective closures in $\mathbb{P}^1\times E_b\subset\mathbb{P}^1\times\mathbb{P}^2$. Also, let

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

and

$$Q_0:=(\infty,-P_0),\qquad Q_1:=(0,P_0),\qquad Q_2:=(0,-P_0).$$

Lemma 2 ([12])**.** *The curves C_i are absolutely irreducible and Q_i is the unique singular point on $C_i\subset\mathbb{P}^1\times\mathbb{P}^2$. Moreover, Q_i is an ordinary one of multiplicity 3.*

Let $\sigma_i\colon C_i'\to C_i$ be the corresponding normalizations. As is known,

$$\#\sigma_i^{-1}(Q_i)=3,\qquad \sigma_i\colon C_i'\setminus\sigma_i^{-1}(Q_i)\xrightarrow{\sim} C_i\setminus\{Q_i\}.$$

We have the projections $pr_{\mathbb{P}^1}\colon C_i\to\mathbb{P}^1$ and $pr_{E_b}\colon C_i\to E_b$ as well as the coverings

$$\pi_i:=pr_{\mathbb{P}^1}\circ\sigma_i\colon C_i'\to\mathbb{P}^1,\qquad \rho_i:=pr_{E_b}\circ\sigma_i\colon C_i'\to E_b$$

of degrees 3 and 6 respectively. Moreover, π_i are cyclic (i.e., Kummer) coverings.

Lemma 3. *The geometric genus $g(C_i')=13$.*

Proof. Applying the Riemann–Hurwitz formula [4, Theorem II.5.9] to π_i, we see that $g(C_i')=r-2$, where r is the number of ramified elements $t\in\mathbb{P}^1$. It is easily checked that t is ramified if and only if $\big(y_i(t)=\pm\sqrt{b}$ and $pr_{\mathbb{P}^1}^{-1}(t)\neq Q_i\big)$ or $den(t)=0$. In turn,

$$y_0(t)=\sqrt{b}\ \Leftrightarrow\ t^3=\frac{\pm1}{b(b-1)},\qquad y_0(t)=-\sqrt{b}\ \Leftrightarrow\ t=\infty\text{ or }t^3=\frac{1}{b(b+1)},$$

$$y_1(t)=\sqrt{b}\ \Leftrightarrow\ t=0\text{ or }t^3=\frac{-1}{b(b-1)},\qquad y_1(t)=-\sqrt{b}\ \Leftrightarrow\ t^3=\frac{1}{b(b\pm1)},$$

$$y_2(t)=\sqrt{b}\ \Leftrightarrow\ t^3=\frac{1}{b(1\pm b)},\qquad y_2(t)=-\sqrt{b}\ \Leftrightarrow\ t=0\text{ or }t^3=\frac{1}{b(b-1)}$$

and

$$den(t)=0\ \Leftrightarrow\ t^3=\frac{1}{b(\sqrt{b}\pm1)^2}.$$

Thus for every curve $r=15$ and the lemma is proved. □

Lemma 4. *Coverings $\rho_i\colon C_i'\to E_b$ don't factor through a non-trivial unramified one $E\to E_b$.*

Proof. Assume the converse. Also, there is obviously the decomposition $\rho_i=\psi_i\circ\varphi_i$ into $\varphi_i\colon C_i'\to D_i'$ and $\psi_i\colon D_i'\to E_b$ such that

$$\mathbb{F}_q(C_i')\simeq\mathbb{F}_q(D_i')[t]/(t^3-s),\qquad \mathbb{F}_q(D_i')\simeq\mathbb{F}_q(E_b)[s]/p_i(s),$$

where $p_i(s):=den(\sqrt[3]{s})y-num_i(\sqrt[3]{s})$. In particular, $\deg(p_i)=\deg(\psi_i)=2$ and hence ψ_i is ramified. Thus $\mathbb{F}_q(C_i')$ is the compositum of $\mathbb{F}_q(E)$ and $\mathbb{F}_q(D_i')$. By virtue of Abhyankar's Lemma [14, Theorem 3.9.1] for any $P\in C_i'$ we obtain that the ramification index

$$e\big(P\mid\rho_i(P)\big)=e\big(\varphi_i(P)\mid\rho_i(P)\big)\leqslant 2.$$

At the same time, there is $P\in C_i'$ such that

$$e\big(P\mid\rho_i(P)\big)\geqslant e\big(P\mid\varphi_i(P)\big)=3.$$

This contradiction proves the lemma. □

2 New encoding

For $a \in \mathbb{F}_q^*$ denote by $\left(\frac{a}{q}\right)_3 := a^{(q-1)/3}$ the *cubic residue symbol*, which is a group homomorphism $\mathbb{F}_q^* \to \{\omega^i\}_{i=0}^2$.

Lemma 5 ([15, 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*

$$\sqrt[3]{a} = \begin{cases} \text{[16, Proposition 1]} & \text{if} \quad q \equiv 1 \pmod 9 \text{ and } q \not\equiv 1 \pmod{27}, \\ a^{-(q-4)/9} = a^{(8q-5)/9} & \text{if} \quad q \equiv 4 \pmod 9, \\ a^{(q+2)/9} & \text{if} \quad q \equiv 7 \pmod 9. \end{cases}$$

Without loss of generality we will assume that $\left(\frac{b}{q}\right)_3 = \omega$.

This paragraph clarifies how the section $\varphi\colon \mathbb{A}^1_t \dashrightarrow \mathcal{E} \subset \mathbb{A}^4_{(y_0,y_1,y_2,t)}$ from Theorem 1 gives a constant-time encoding $h\colon \mathbb{F}_q \to E_b(\mathbb{F}_q)$. It will be considered the cases $q \equiv 4 \pmod 9$ (occurs for BW6-761) and $q \equiv 10 \pmod{27}$ (does for BLS12-381). The cases $q \equiv 7 \pmod 9$ and $q \equiv 19 \pmod{27}$ are processed in a similar way.

Letting $g_i := y_i^2 - b$ for $i \in \{0,1,2\}$, we get $\mathcal{E}\colon \{g_j = b^j t^3 g_0 \text{ for } j \in \{1,2\}$. It is obvious that $\left\{\left(\frac{g_i}{q}\right)_3\right\}_{i=0}^2 = \{\omega^i\}_{i=0}^2$ whenever $g_i, t \in \mathbb{F}_q^*$. Besides, denote by $n \in \{0,1,2\}$ the position number of an element $t \in \mathbb{F}_q^*$ in the set $\left\{\omega^i t\right\}_{i=0}^2$ 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.

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

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

Consider the auxiliary map

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

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 $\mathcal{E}(\mathbb{F}_q)$.

It is worth noting that the element 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 any $u \in \mathbb{F}_q$, $v \in \mathbb{F}_q^*$. Indeed,

$$\theta = (u/v)^{(8q-5)/9} = u^{(8q-5)/9} \cdot v^{(q-4)/9} = u^3 (u^8 v)^{(q-4)/9}. \tag{1}$$

The case $q \equiv 10 \pmod{27}$**.** 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

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

Consider the auxiliary map

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

Since

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

this map is well defined everywhere on $\mathcal{E}(\mathbb{F}_q)$.

It is worth noting that the element 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 any $u \in \mathbb{F}_q$, $v \in \mathbb{F}_q^*$. Indeed,

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

In both cases, for any $t \in \mathbb{F}_q$ we put

$$h(t) := \begin{cases} (h' \circ \varphi)(t) & \text{if} \quad den(t) \neq 0, \\ \mathcal{O} & \text{if} \quad den(t) = 0. \end{cases}$$

We emphasize that in the definition of h' (a fortiori, φ) the cubic residue symbol (in other words, cubic residuosity test) does not appear. In turn, 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. Finally, by virtue of the formulas (1), (2) the value $\theta(t) = 0$ if $den(t) = 0$, because $g_0 = u/v$ for $u := num_0^2 - b \cdot den^2$ and $v := den^2$. In other words, $h(t) = \mathcal{O}$ if and only if $\theta(t) = 0$, but $u(t) \neq 0$. Calculating the value $\theta(t)$ every time regardless of whether $uv(t) = 0$ or not, we eventually obtain

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

Sometimes it will be convenient to use the notation $S := h^{-1}\big(\{\pm P_0, \mathcal{O}\}\big)$.

Theorem 2. *For any point $P \in E_b(\mathbb{F}_q)$ we have $\#h^{-1}(P) \leqslant 6$ and hence $q/6 \leqslant \#\mathrm{Im}(h)$.*

Proof. First, suppose that $h(t) = \pm P_0$. Then $\theta(t) = g_0(t) = 0$ or $t = 0$. In the first case, $y_0(t) = \pm\sqrt{b}$. In the second one, $y_0(0) = 3\sqrt{b}$, $g_0(0) = 8b$, and hence $\left(\frac{g_0(0)}{q}\right)_3 = \omega$. Since $y_2(0) = -\sqrt{b}$, we have $h(0) = -P_0$. As a result, $\#h^{-1}(P_0) \leqslant 6$ and $\#h^{-1}(-P_0) \leqslant 4$. In turn, since $\deg(den) = 6$, we get $\#h^{-1}(\mathcal{O}) \leqslant 6$.

Now take $t \in \mathbb{F}_q \setminus S$. Let the value $g_i(t)$ is a cubic residue in $\mathbb{F}_q$. Then for $t' \in \mathbb{F}_q$ from the collision $h(t) = h(t')$ it follows that exists $k \in \{0, 1, 2\}$ such that $y_i(t) = y_k(t')$. Every given equation has at most 6 solutions in $\mathbb{F}_q$ with respect to t'. However the x-coordinates of $h(t')$ and $h(\omega t')$ are different, because $\theta(t') = \theta(\omega t')$. Hence we can take into account only 2 solutions (with the different cubic powers). The theorem is proved. □

3 Indifferentiability from a random oracle

For $i \in \{0, 1, 2\}$ let $T_i := \left\{t \in \mathbb{F}_q \mid \sqrt[3]{g_i(t)} \in \mathbb{F}_q^*\right\}$. Therefore $\mathbb{F}_q = T_0 \sqcup T_1 \sqcup T_2 \sqcup S$. Besides, we will need the functions $f_0 := x$ and $f_j := x/t$ (for $j \in \{1, 2\}$) on the curves C_i.

In this paragraph $q \equiv 4 \pmod 9$ and for $t \in T_0$ we put $h(t) := \big(\theta(t), y_0(t)\big)$, that is the x-coordinate is not multiplied by ω^n. Also, without loss of generality suppose that $\left(\frac{c_j}{q}\right)_3 = \omega^{j(8q-5)/9}$. These assumptions are necessary in order to $\left(\frac{f_i}{q}\right)_3 = 1$ whenever $t \in T_i$ and $x = x\big(h(t)\big)$. We use this in our proof of the following theorem. However we do not state that the previous definition of h (or that for $q \equiv 10 \pmod{27}$) leads to the hash function $H\colon \{0,1\}^* \to E_b(\mathbb{F}_q)$ differentiable from a random oracle.

Theorem 3. *The new encoding $h\colon \mathbb{F}_q \to E_b(\mathbb{F}_q)$ is B-well-distributed in the sense of* [17, Definition 1]*, where $B := 156 + O(q^{-1/2})$.*

Proof. Fix a non-trivial character $\chi\colon E_b(\mathbb{F}_q) \to \mathbb{C}^*$. Note that

$$\sum_{t\in T_i} \chi\big(h(t)\big) = \sum_{P\in C_i'(\mathbb{F}_q)} \frac{1 + \left(\frac{f_i(P)}{q}\right)_3 + \left(\frac{f_i^2(P)}{q}\right)_3}{3} \cdot \chi\big(\rho_i(P)\big) + O(1).$$

Here notation $O(1)$ is used to avoid handling a finite number of ramification points (with respect to π_i) and those from $\pi_i^{-1}\big(\{0, \infty\}\big)$. As a consequence,

$$\left|\sum_{t\in T_i} \chi\big(h(t)\big)\right| \leqslant \frac{1}{3} \sum_{k\in\{0,1,2\}} \left|\sum_{P\in C_i'(\mathbb{F}_q)} \Big(\frac{f_i^k(P)}{q}\Big)_3 \cdot \chi\big(\rho_i(P)\big)\right| + O(1).$$

It can easily be checked that [17, Theorem 7] remains valid if the Legendre symbol is replaced by the cubic residue symbol. And we can use it with respect to ρ_i because of Lemma 4. Therefore according to Lemma 3 and the fact that

$$\deg(x) = \deg(pr_x \circ \rho_i) = 12, \qquad \deg(x/t) = \deg(x) + \deg(t) = 15$$

(where pr_x is the projection $E_b \to \mathbb{A}^1_x$) we obtain

$$\left|\sum_{P\in C_i'(\mathbb{F}_q)} \Big(\frac{f_i^k(P)}{q}\Big)_3 \cdot \chi\big(\rho_i(P)\big)\right| \leqslant 2\big(g(C_i') - 1 + k\deg(f_i)\big)\sqrt{q} \leqslant \begin{cases} 24(1+k)\sqrt{q} & \text{if} \quad i = 0, \\ 6(4+5k)\sqrt{q} & \text{if} \quad i \in \{1, 2\}. \end{cases}$$

Thus

$$\left|\sum_{t\in T_i}\chi\big(h(t)\big)\right| \leqslant O(1) + \begin{cases} 48\sqrt{q} & \text{if} \quad i = 0, \\ 54\sqrt{q} & \text{if} \quad i \in \{1,2\} \end{cases}$$

and hence

$$\left|\sum_{t\in \mathbb{F}_q}\chi\big(h(t)\big)\right| \leqslant \sum_{i\in\{0,1,2\}}\left|\sum_{t\in T_i}\chi\big(h(t)\big)\right| + O(1) \leqslant 156\sqrt{q} + O(1).$$

The theorem is proved. □

From [17, Corollary 4] it immediately follows that

Corollary 1. *The distribution on $E_b(\mathbb{F}_q)$ defined by $h^{\otimes 2}$ is ϵ-statistically indistinguishable from the uniform one* [2, Definition 3]*, where $\epsilon := 156^2 q^{-1/2} + O(q^{-3/4})$.*

According to Remark 1 the encoding $h^{\otimes 2}$ is efficiently computable in constant time (of two exponentiations in $\mathbb{F}_q$). In turn, [2, Algorithm 1] is readily modified, so $h^{\otimes 2}$ is also *samplable* [2, Definition 4]. Therefore we establish

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

Acknowledgements. The author expresses his deep gratitude to his scientific advisor M. Tsfasman.

References

[1] N. El Mrabet, M. Joye, *Guide to Pairing-Based Cryptography*, Cryptography and Network Security Series, Chapman and Hall/CRC, New York, 2016.

[2] E. Brier et al., "Efficient indifferentiable hashing into ordinary elliptic curves", Advances in Cryptology — CRYPTO 2010, **6223** (2010), 237–254.

[3] A. Faz-Hernandez et al., *Hashing to elliptic curves*, CFRG Internet-draft, 2020.

[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.

[6] D. Koshelev, *Hashing to elliptic curves of j-invariant* 1728, ePrint IACR 2019/1294.

[7] D. Koshelev, "Hashing to elliptic curves of $j = 0$ and Mordell–Weil groups", *Mathematical Notes*, **108(5)** (2020), 748–751.

[8] Y. El Housni, A. Guillevic, *Optimized and secure pairing-friendly elliptic curves suitable for one layer proof composition*, ePrint IACR 2020/351.

[9] 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.

[10] L. Washington, *Elliptic curves: number theory and cryptography*, Discrete Mathematics and Its Applications, Chapman & Hall, London, 2008.

[11] 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.

[12] D. Koshelev, *Magma code*, https://github.com/dishport/Efficient-indifferentiable-hashing-to-elliptic-curves-of-j-0-provided-that-b-is-a-quadratic-residue, 2020.

[13] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, **151**, Springer, New York, 1994.

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

[15] A. Dudeanu, G.-R. Oancea, S. Iftene, "An x-coordinate point compression method for elliptic curves over $\mathbb{F}_p$", Inter. Symp. on Symb. and Num. Algor. for Scientific Comp., 2010, 65–71.

[16] 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.

[17] R. Farashahi et al., "Indifferentiable deterministic hashing to elliptic and hyperelliptic curves", *Mathematics of Computation*, **82(281)** (2013), 491–512.