Faster indifferentiable hashing to elliptic $\mathbb{F}_q^2$-curves

Dmitrii Koshelev

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

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 $j(E) \not\in \mathbb{F}_q$. This article provides a new constant-time hash function $H : \{0, 1\}^* \to E(\mathbb{F}_q^2)$ indifferentiable from a random oracle. Furthermore, $H$ 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 $\tau : E \to E_b$ of small degree. Therefore the composition $\tau \circ H : \{0, 1\}^* \to \tau(E(\mathbb{F}_q^2))$ 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 $H : \{0, 1\}^* \to G$ 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 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 $H : \{0, 1\}^* \to E_b(\mathbb{F}_q^2)$. Indeed, one of quick methods [1, §8.5] can be applied for computing the cofactor multiplication $[N/\ell] : E_b(\mathbb{F}_q^2) \to G$. 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 $H$ are induced from some map $h : \mathbb{F}_{q^2} \to E_b(\mathbb{F}_{q^2})$, 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 $\eta : \{0, 1\}^* \to \mathbb{F}_{q^2}$ is not indifferentiable.

1web page: https://www.researchgate.net/profile/Dimitri_Koshelev
email: dimitri.koshelev@gmail.com

1
Instead, it is often considered the composition $\mathcal{H} := h^{\otimes 2} \circ \eta^2$ of the map

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

(also called encoding) and the hash function

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

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 $\sqrt{b} \in \mathbb{F}_{q^2}$, that is $2 \mid N$.

Sometimes it is possible to use an $\mathbb{F}_{q^2}$-isogeny $\tau : E \to E_b$ of small degree (the Wahby–Boneh approach [8]). For example, the curve BLS12-381 [8, §2.1] (whose $b = 4(1+i)$ and $[\log_2(q)] = 381$) 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 $h : \mathbb{F}_{q^2} \to E(\mathbb{F}_{q^2})$ 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 $j(E) \notin \mathbb{F}_{q^2}$ there is a 2-sheeted cover $\varphi_0 : H \to E$ from a real (split) hyperelliptic $\mathbb{F}_{q^2}$-curve $H$ (see, e.g., [10, §10.1.1]) of geometric genus 2. Then in §2 we construct a very simple encoding $h : \mathbb{F}_q \to H(\mathbb{F}_q)$ (2) such that the map

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

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

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

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

In other terms, we construct an $\mathbb{F}_q$-isogeny $\phi := \theta^{-1} \circ \varphi : J \to R$ (with the kernel $(\mathbb{Z}/2)^2$) to the Weil restriction $R$ (see, e.g., [10, §3.7]) 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 \(E(\mathbb{F}_\ell) = R(\mathbb{F}_q)\) 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 \(\mathbb{F}_{\ell^2}\), 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 \(\mathbb{F}_{\ell^2}\) 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 3\(n\) exponentiations in \(\mathbb{F}_q\) rather than 4\(n\) 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 \(N = \#E(\mathbb{F}_{\ell^2})\) 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 \(j(E) \not\in \mathbb{F}_q\) (cf. Lemma 1). Fortunately, as shown in the computer algebra system Magma [16] the mentioned curve is \(\mathbb{F}_{\ell^2}\)-isogenous (with the help of an isogeny of degree 7) to the curve \(E\) with

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

where \(\sqrt{21} \not\in \mathbb{F}_q\). Our code [16] also generates the coefficients of \(H\), \(\varphi_0\) and \(E\), \(\tau\) in the generic case.

1 Two-sheeted cover \(\varphi_0: H \to E\)

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

\[
E = E^{(0)}: y^2 = f_0(x) := x^3 + ax + b, \quad E^{(1)}: y^2 = f_1(x) := x^3 + a^9x + b^9.
\]

They are obviously \(\mathbb{F}_{\ell^2}\)-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 \(\mathbb{F}_q\)-isomorphism

\[
\sigma: E \cong E^{(1)} \quad (x, y) \mapsto (\lambda^2x, \lambda^3y),
\]

where

\[
\lambda := \begin{cases} 
  a^{(q-1)/4} = b^{(q-1)/6} & \text{if } j(E) \not\in \{0, 1728\}, \text{ i.e., } ab \neq 0, \\
  a^{(q-1)/4} & \text{if } j(E) = 1728, \text{ i.e., } b = 0, \\
  b^{(q-1)/6} & \text{if } j(E) = 0, \text{ i.e., } a = 0.
\end{cases}
\]

Moreover, \(\lambda \in \mathbb{F}_{\ell^2}\) whenever \(ab \neq 0\), because \(\lambda^3/\lambda^2 = (b/a)^{(q-1)/2}\). The same is true if \(b = 0\) and \(q \equiv 1 \pmod{4}\) (resp. \(a = 0\) and \(q \equiv 1 \pmod{3}\)).
Further, put $A := E \times E^{(l)}$ with the projections $pr_k: A \to E^{(k)}$ for $k \in \mathbb{Z}/2$. As it will become clear later, we need to work with $\pi$-invariant objects, where

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

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 $r_j \not\in \mathbb{F}_q^2$ for $j \in \mathbb{Z}/3$ or, without loss of generality, $r_j^q = r_{j+1}$. For instance, the case $b = 0$ is excluded from our consideration.

We are interested in the isomorphism $\chi: E[2] \cong E^{(l)}[2]$ defined by the bijection $r_j \mapsto r_{j+1}^q$. Its graph $\Gamma \cong (\mathbb{Z}/2)^2$ is clearly $\pi$-invariant, hence the corresponding isogeny $\tilde{\varphi}: A \to A/\Gamma$ 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 $\mathbb{F}_q$-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 $\mathbb{F}_q$-isomorphism $E \cong E^{(l)}$;
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 $f_1(\lambda^2r_j) = 0$. In the case $\lambda^2r_0 = r_1^q$ we get $\lambda^2r_j = r_{j+1}^q$, because $\lambda \in \mathbb{F}_q^2$.

If $\lambda^2r_0 = r_0^q$, then similarly $\lambda^2r_j = r_j^q$. Therefore $\lambda^2r_j = r_{j+1}$ 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 $\omega^2r_{j+2} = r_j^q$, that is $\omega^2r_j = r_j^q$. The case $\lambda^2r_0 = r_0^q$ 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

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

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

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

4
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 $A_j^q = A_{j+1}$. 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

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

where

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

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

\[
(\varphi'_0, \varphi'_1): H' \to A \quad P \mapsto (\varphi'_0(P), \varphi'_1(P)).
\]

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

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

\[
\pm \alpha: H' \xrightarrow{\sim} H' \quad (x, y) \mapsto (-x, \pm y).
\]

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

\[
\pm \alpha: A \xrightarrow{\sim} A \quad (P_0, P_1) \mapsto (\mp P_0, \pm P_1).
\]

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

\[
\pi: H' \to H' \quad (X : Y : Z) \mapsto (Z^q : Y^q : X^q),
\]

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 $i := \sqrt{-1} \not\in \mathbb{F}_q$. 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

$$
\psi: H \Rightarrow H' \quad (X : Y : Z) \mapsto (X + iZ : Y : X - iZ),
$$
$$
\psi^{-1}: H' \Rightarrow H \quad (X : Y : Z) \mapsto \left(\frac{X + Z}{2} : Y : \frac{X - Z}{2i}\right).
$$

Denote by $J$ the Jacobian of $H$. Let us keep the notation for the natural extensions $\psi: J \Rightarrow J'$ and $\psi^{-1}: J' \Rightarrow J$. 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

$$
c = c_0 + c_1 i, \quad d = d_0 + d_1 i, \quad e = e_0 + e_1 i.
$$

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

$$
\varphi_k: H \rightarrow E^{(k)} \quad (x, y) \mapsto (x_0 + (-1)^k x_1 i, y_0 + (-1)^k y_1 i),
$$

where

$$
x_k := \frac{c_k(x^4 - 6x^2 + 1) + (-1)^k 4c_{k+1}x(x^2 - 1)}{(x^2 + 1)^2} + d_k,
$$
$$
y_k := \frac{e_kx(x^2 - 3) + (-1)^k e_{k+1}(3x^2 - 1)}{(x^2 + 1)^3}.
$$

(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, $\psi: J(\mathbb{F}_q) \Rightarrow (J')^\pi$. Besides, $\varphi': A^\pi \Rightarrow (J')^\pi$ (or, equivalently, $\varphi': (J')^\pi \Rightarrow A^\pi$), because $\varphi' \circ \varphi = [2]$ and $A[2] \cap A^\pi$ is the trivial group. Finally, $pr_k: A^\pi \Rightarrow E^{(k)}(\mathbb{F}_q)$ with the inverse maps

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

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 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 $2 \nmid \#E(\mathbb{F}_q)$ 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
The same is true for \( \varphi \).

\[ \text{Remark 1.} \]

For any point \( \varphi \) we obtain \( \varphi(x, y) = (\varphi(x, -y)) \). Hence we do not have to find \( x^{-1} \) before evaluating the covering map \( \varphi \).

Observe that \( \varphi_0 \circ h : \mathbb{F}_q \to E(\mathbb{F}_q) \). 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

\[ \text{Lemma 2.} \]

\[ \text{For any point } P \in H(\mathbb{F}_q) \text{ we have } \#h^{-1}(P) \leq 2 \text{ and hence } q/2 \leq \#\text{Im}(h). \]
Theorem 2. The encoding \( h : \mathbb{F}_q \to H(\mathbb{F}_q) \) 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 \( \left( \frac{t_+}{q} \right) = 1 \) whenever \( x \in X_\pm \) and \( y = y(h(x)) \). Indeed, \( \left( \frac{y}{q} \right) = \left( \frac{\tilde{y}}{q} \right) = 1 \) 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 \( \chi : J(\mathbb{F}_q) \to \mathbb{C}^* \) we see that

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

As a consequence,

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

Here notation \( O(1) \) is used to avoid handling the set \( pr_x^{-1}([0, \infty)) = \{ P_\pm, O_\pm \} \). 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 \( H \to A^1_y \)) we obtain

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

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. \( \square \)

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 \( h^{\otimes 3} : \mathbb{F}_q^3 \to J(\mathbb{F}_q) \) is \( \epsilon \)-statistically indistinguishable [2, Definition 3] from the uniform one, where \( \epsilon := 18^3q^{-1/2} + O(q^{-3/4}) \).

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


