The most efficient indifferentiable hashing to elliptic curves of j-invariant 1728

Dmitrii Koshelev [1]

Computer sciences and networks department, Télécom Paris, France

Abstract. This article makes an important contribution to solving the long-standing problem of whether all elliptic curves can be equipped with a hash function (indifferentiable from a random oracle) whose running time amounts to one exponentiation in the basic finite field $\mathbb{F}_q$. More precisely, we construct a new indifferentiable hash function to any ordinary elliptic $\mathbb{F}_q$-curve E_a of j-invariant 1728 with the cost of extracting one quartic root in $\mathbb{F}_q$. As is known, the latter operation is equivalent to one exponentiation in finite fields with which we deal in practice. In comparison, the previous fastest random oracles to E_a require to perform two exponentiations in $\mathbb{F}_q$. Since it is highly unlikely that there is a hash function to an elliptic curve without exponentiations at all (even if it is supersingular), the new result seems to be unimprovable.

Key words: Calabi–Yau threefolds, double-odd curves, indifferentiable hashing to elliptic curves, j-invariant 1728, pairing-based cryptography.

1 Introduction

Let $\mathbb{F}_q$ be a finite field of $\mathrm{char}(\mathbb{F}_q) > 3$ and $E_a\colon y^2 = x^3 + ax$ be an elliptic $\mathbb{F}_q$-curve whose j-invariant equals 1728. The curves E_a are studied with interest in elliptic cryptography at least at the research level. The point is that (apart from elliptic curves of $j = 0$) they have a non-trivial automorphism group, which leads to more efficient scalar multiplication and pairing computation on them (see details in [1, Sections 6.2.2 and 3.3.2] respectively). This paper focuses on ordinary curves, because supersingular ones pose special challenges for security of discrete logarithm cryptography by virtue of [1, Remark 2.22]. And according to [2, Example V.4.5] the ordinariness of E_a results in the restriction $q \equiv 1 \pmod 4$, i.e., $i := \sqrt{-1} \in \mathbb{F}_q$.

Examples of *pairing-friendly curves* of $j = 1728$ are represented, e.g., in [1, Section 4.5.2]. Curiously, unlike curves of j-invariant 0, some curves E_a (for example, do255e from [3, Section 5.2]) can be so-called *double-odd elliptic curves* [3, 4], that is their order equals two times an odd (prime) number. Double-odd curves are a trade off between prime order curves and *twisted Edwards curves* [1, Section 6.4.1] whose cofactor is always a multiple of four. Thus double-odd curves enjoy simpler *subgroup membership testing* than twisted Edwards ones and, at the same time, faster *complete addition formulas* than prime order ones. These notions are discussed in the remarkable article [5] and in references therein.

[1] Email: dimitri.koshelev@gmail.com
ResearchGate: https://www.researchgate.net/profile/dimitri-koshelev
LinkedIn: https://www.linkedin.com/in/dimitri-koshelev
GitHub: https://github.com/dishport

Many cryptographic protocols (e.g., the popular aggregate BLS signature [6]) use a hash function of the form $H\colon \{0,1\}^* \to E_a(\mathbb{F}_q)$. And if it is necessary, the value of H can be subsequently moved into a prime order subgroup of $E_a(\mathbb{F}_q)$ by *clearing the cofactor* [7, Section 7]. There is the regularly updated draft [7] on the topic of hashing to elliptic curves. Due to [7, Section 10] it is highly desirable and often inevitable that H is *indifferentiable from a random oracle* in sense of Maurer et al. [8, Section 4.2]. By the way, [3, Section 3.7] raises the question of efficient indifferentiable hashing to curves E_a, but that article does not answer this question in an acceptable way.

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

$$e^{\otimes 2}\colon \mathbb{F}_q^2 \to E_a(\mathbb{F}_q) \qquad e^{\otimes 2}(t_0, t_1) := e(t_0) + e(t_1)$$

for some map $e\colon \mathbb{F}_q \to E_a(\mathbb{F}_q)$. Such a map is often called *encoding*. For the given H its indifferentiability follows from [9, Theorem 1] if $\mathfrak{h}$ is indifferentiable and $e^{\otimes 2}$ is *admissible* in the sense of [9, Definition 4]. It is worth noting that the admissibility property in particular requires an encoding e to be *constant-time*, that is, informally speaking, the computation time of its value is independent of an input argument.

The previous state-of-the-art encoding, valid for any curve E_a, is proposed by the author in [10] after a refinement of the work [11]. This encoding e (resp. $e^{\otimes 2}$) can be implemented by extracting one (resp. two) square root(s) in $\mathbb{F}_q$. As is customary (see, e.g., [1, Section 5.1.7]), a square root is expressed via one exponentiation in $\mathbb{F}_q$ at least when $q \not\equiv 1 \pmod 8$. Taking into account the condition $q \equiv 1 \pmod 4$, we obtain $q \equiv 5 \pmod 8$.

This work (again, for any $a \in \mathbb{F}_q^*$) directly provides an admissible map $h\colon \mathbb{F}_q^2 \to E_a(\mathbb{F}_q)$, which requires to extract one quartic root in $\mathbb{F}_q$. We will show that for $q \equiv 5 \pmod 8$ this operation is also nothing but one exponentiation in $\mathbb{F}_q$. In other words, the tensor square is in fact superfluous for curves E_a and hence we get rid of one exponentiation in $\mathbb{F}_q$ in comparison with $e^{\otimes 2}$. Moreover, it is worth emphasizing that h is given by quite simple formulas with small coefficients. Therefore the new result seems interesting both from theoretical and practical points of view.

By definition, pairings act from two groups traditionally denoted by $\mathbb{G}_1$, $\mathbb{G}_2$. As said in [1, Section 3.2.5], in practice, $\mathbb{G}_1 \subset E_a(\mathbb{F}_q)$ for a prime q and $\mathbb{G}_2 \subset E_{a'}(\mathbb{F}_{q^n})$ for some $n \in \mathbb{N}$ and $a' \in \mathbb{F}_{q^n}^*$. Moreover, the extension degree n is often even. In this case, due to [1, Algorithm 5.18] a square root in $\mathbb{F}_{q^n}$ can be expressed via two square roots in $\mathbb{F}_{q^{n/2}}$. To our knowledge, there is no analogous expression for a quartic root in $\mathbb{F}_{q^n}$. So, unlike e, the new map h is not relevant for hashing to $\mathbb{G}_2$ whenever $2 \mid n$. Fortunately, as explained in [12, Section 1.2], in combination with clearing the (large) cofactor $\#E_{a'}(\mathbb{F}_{q^n})/\#\mathbb{G}_2$ it is sufficient to apply $e\colon \mathbb{F}_{q^n} \to E_{a'}(\mathbb{F}_{q^n})$ only once. Thus the best solution is to utilize the map h (resp. e) in the case of $\mathbb{G}_1$ (resp. $\mathbb{G}_2$). And looking at [12, Tables 1-2], the reader can realize the significance of e, h in the general classification of maps to elliptic curves.

An approach to produce h is based on an explicit $\mathbb{F}_q$-parametrization $\varphi\colon \mathbb{A}^2 \dashrightarrow T$ of a (*uni-*)*rational* $\mathbb{F}_q$*-surface* [13, Section 4.9] on some algebraic threefold T, that is $\dim(T) = 3$. Then h is just the composition of φ (restricted to $\mathbb{F}_q$-points) and an auxiliary map $h'\colon T(\mathbb{F}_q) \to E_a(\mathbb{F}_q)$. More concretely, there is an elementary rational $\mathbb{F}_q$-map $\mathcal{E} \dashrightarrow T$ from a threefold enjoying some *elliptic fibration* $\mathcal{E} \to \mathbb{A}^2$ (see, e.g., [14, Section 2]). The desired φ is immediately obtained from an infinite order $\mathbb{F}_q$-section $\psi\colon \mathbb{A}^2 \dashrightarrow \mathcal{E}$ of this fibration.

Ideologically, the described approach is almost the same as in [15], but, of course, with different technique details. In particular, in that article the suggested threefold is itself elliptic, i.e., $T = \mathcal{E}$ in our notation. There provided that $\sqrt{b} \in \mathbb{F}_q$ the author constructs one more admissible map from $\mathbb{F}_q^2$ to the $\mathbb{F}_q$-point group of an ordinary elliptic curve $E_b\colon y^2 = x^3 + b$ (of j-invariant 0). Moreover, this map equally performs only one exponentiation in $\mathbb{F}_q$, namely a cubic root extraction.

There is the long-standing open question of whether every elliptic $\mathbb{F}_q$-curve E has a random oracle $\{0,1\}^* \to E(\mathbb{F}_q)$ with the cost of one exponentiation (cf. [12, Conjecture 1]). Recently, the independent work [16] arose on this topic. It contains an indifferentiable hash function (under the name *SwiftEC*) being a modification of the classical *Shallue–van de Woestijne (SW) encoding* [17]. However, SwiftEC is not relevant for most curves E_a, unlike all ordinary curves E_b and many others of remaining j-invariants.

The SW encoding is based on yet another threefold, although a rational $\mathbb{F}_q$-curve (of geometric genus 0) is taken on it instead of a unirational $\mathbb{F}_q$-surface. Fortunately, in [18, Lemma 3] Skałba provides such a surface and hence a (probably admissible) map $\mathbb{F}_q^2 \to E(\mathbb{F}_q)$ whenever $j(E) \neq 0$. Unfortunately, the *Skałba map* is given by too cumbersome formulas unsuitable as a practical matter. In turn, SwiftEC is produced by means of another surface admitting a simpler rational $\mathbb{F}_q$-parametrization. This is achieved at the price of generality loss.

Interestingly, all the threefolds, appeared in the scientific domain under consideration, turn out to be *Calabi–Yau varieties*, which are applied over the field $\mathbb{C}$ in theoretical physics (see, e.g., [19]). However, since we will work over non-closed fields it is also reasonable to cite a source (such as [20]) on the arithmetic of Calabi–Yau varieties. It is worth noting that one-dimensional Calabi–Yau varieties are exactly elliptic curves. So it is not surprising that their high-dimensional analogue occurs in the context of elliptic cryptography.

2 Geometric results

As said in the introduction, throughout the article we assume that $i := \sqrt{-1} \in \mathbb{F}_q$. Consequently, the curve $E_a\colon y^2 = x^3 + ax$ possesses the $\mathbb{F}_q$-automorphism $[i](x,y) := (-x, iy)$ of order 4. Obviously, $E_a[2] = \{\mathcal{O}, P_0, P_\pm\}$, where

$$\mathcal{O} := (0:1:0), \qquad P_0 := (0,0), \qquad P_\pm := (\pm i\sqrt{a}, 0).$$

Besides, any two $\mathbb{F}_q$-curves of $j = 1728$ are isomorphic (at most over $\mathbb{F}_{q^4}$) by means of the map

$$\sigma_{a,a'}\colon E_a \to E_{a'} \qquad \sigma_{a,a'}(x,y) := (\alpha^2 x, \alpha^3 y),$$

where $\alpha := \sqrt[4]{a'/a}$. As a result, up to an $\mathbb{F}_q$-isomorphism, there are exactly 4 twists for E_a, namely E_{ac^j} for $j \in \mathbb{Z}/4$ and $c \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^2$.

It is suggested to consider the $\mathbb{F}_q$-threefold

$$T := \begin{cases} S_0\colon y_0^2 = x_0^3 + ac(t^3 + at)x_0, \\ S_1\colon y_1^2 = x_1^3 + ac^3(t^3 + at)x_1 \end{cases} \subset \quad \mathbb{A}^5_{(x_0,x_1,y_0,y_1,t)}.$$

It seems that T is birationally $\mathbb{F}_q$-isomorphic to the quotient of $A := E_a \times E_{ac} \times E_{ac^3}$ by the order 4 diagonal automorphism $\delta := [-1] \times [i] \times [i]$. This quotient is similar to the one from [15, Lemma 1]. Since the given fact is not necessary for our purposes, we do not prove it. However, this is a useful observation, because $\mathrm{age}(\delta) = 1$ (as well as for the automorphism $[\omega]^{\times 3}$ from [15, Section 1]), where the *age* is defined in [21]. So by virtue [21, Theorem 13] the quotient A/δ enjoys at least a rational curve over the algebraic closure $\overline{\mathbb{F}_q}$. Thus there is a justified hope of obtaining a rational $\mathbb{F}_q$-surface on T.

Curiously, our T (like the one from [15, Lemma 1]) can be also interpreted as a *Schoen threefold* [22], that is the *fiber product* [23, Section 4.5] of two *rational elliptic surfaces* with a section [13, Chapter 7]. Indeed, $S_j \subset \mathbb{A}^3_{(x_j,y_j,t)}$ are nothing but *singular del Pezzo surfaces* of degree 2 (see, e.g., [24, Section 8.7]) having the projection to t as an elliptic fibration with the section $\mathcal{O}$. Moreover, they are clearly isomorphic over $\mathbb{F}_{q^2}$, hence T fits the definition of a *banana threefold* [25]. To sum up, we see a confirmation that T (or, formally speaking, some of its smooth projective models) is a Calabi–Yau threefold.

The threefold T is embedded in a weighted projective space as follows:

$$\overline{T} = \begin{cases} y_0^2 = x_0^3 y_2 + ac(t^3 + aty_2^2)x_0, \\ y_1^2 = x_1^3 y_2 + ac^3(t^3 + aty_2^2)x_1 \end{cases} \subset \quad \mathbb{P}(1,1,2,2,1,1),$$

where the variables y_0, y_1 are of the weight 2. Further, on the affine chart $t \neq 0$ the threefold $\overline{T}$ possesses the form

$$V := \begin{cases} v_0^2 = u_0^3 v_2 + ac(1 + av_2^2)u_0, \\ v_1^2 = u_1^3 v_2 + ac^3(1 + av_2^2)u_1 \end{cases} \subset \quad \mathbb{A}^5_{(u_0,u_1,v_0,v_1,v_2)}.$$

Thus we have the birational isomorphisms

$$\tau\colon V \dashrightarrow T \qquad \tau := \left(\frac{u_0}{v_2}, \frac{u_1}{v_2}, \frac{v_0}{v_2^2}, \frac{v_1}{v_2^2}, \frac{1}{v_2}\right), \qquad \tau^{-1}\colon T \dashrightarrow V \qquad \tau^{-1} = \left(\frac{x_0}{t}, \frac{x_1}{t}, \frac{y_0}{t^2}, \frac{y_1}{t^2}, \frac{1}{t}\right).$$

We can look at V as a curve in $\mathbb{A}^3_{(v_0,v_1,v_2)}$ given by the intersection of two quadratic surfaces over the rational function field $\mathbb{F}_q(u_0,u_1)$. The existence of an $\mathbb{F}_q(u_0,u_1)$-point on V is not clear, hence we apply the base change $\chi\colon u_j := ct_j^2$, which leads to

$$\mathcal{E} := \begin{cases} v_0^2 = c^3 t_0^6 v_2 + ac^2(1 + av_2^2)t_0^2, \\ v_1^2 = c^3 t_1^6 v_2 + ac^4(1 + av_2^2)t_1^2 \end{cases} \subset \quad \mathbb{A}^5_{(t_0,t_1,v_0,v_1,v_2)}.$$

For the sake of compactness, put $F := \mathbb{F}_q(t_0,t_1)$. At infinity, i.e., in $\mathbb{P}^3 \setminus \mathbb{A}^3_{(v_0,v_1,v_2)}$ there are on $\mathcal{E}$ the F-points

$$\mathcal{P}_{\pm} := (\pm act_0 : ac^2 t_1 : 1 : 0).$$

It is proposed to take $\mathcal{P}_+$ as the neutral element in the *Mordell–Weil group* $\mathcal{E}(F)$.

We will rely on some Magma calculations [26] that can be verified in the free calculator on the official site of this computer algebra system. The next lemmas are proved by means of the reduction to a Weierstrass form of $\mathcal{E}$.

Lemma 1 ([26]). *The F-curve $\mathcal{E}$ is elliptic with the j-invariant*

$$j(\mathcal{E}) = \frac{16(c^2t_0^8t_1^8 + 12a^3c^4t_0^8 - 32a^3c^2t_0^4t_1^4 + 12a^3t_1^8 + 16a^6c^2)^3}{a^3\big((c^2t_0^8 - 4a^3)(ct_0^2 + t_1^2)(ct_0^2 - t_1^2)(t_1^8 - 4a^3c^2)\big)^2}.$$

Lemma 2 ([26]). *The coordinates of the point $\psi := 2\mathcal{P}_-$ are the fractions $v_j(t_0, t_1) :=$ $\mathrm{num}_j/\mathrm{den}$, where*

$$\mathrm{num}_0 := ac(-3c^4t_0^8 + 2c^2t_0^4t_1^4 + t_1^8 + 16a^3c^2)t_0, \qquad \mathrm{num}_1 := ac^2(c^4t_0^8 + 2c^2t_0^4t_1^4 - 3t_1^8 + 16a^3c^2)t_1,$$
$$\mathrm{num}_2 := c^4t_0^8 - 2c^2t_0^4t_1^4 + t_1^8 - 16a^3c^2, \qquad \mathrm{den} := 8a^2c(c^2t_0^4 + t_1^4).$$

The last lemma can be alternatively proved by using the geometric interpretation of the group law for $\mathcal{E}(F)$, described, e.g., in [2, Exercise 3.10]. Similarly, the reader is invited to check that for $\varphi_\pm := (\pm\sqrt{b}, \sqrt{b}, \sqrt{b})$ the point φ from [15, Theorem 1] coincides with $2\varphi_-$ with respect to φ_+ as the zero point. Among other things, the author verified that a base change for the elliptic threefold T from [15, Lemma 1] (in contrast to ours χ) does not yield a visible $\mathbb{F}_q$-section of infinite order if $\sqrt{b} \notin \mathbb{F}_q$. Therefore the restriction $\sqrt{b} \in \mathbb{F}_q$ in that article seems essential.

For v, $x \in \mathbb{F}_q$ and $j \in \mathbb{Z}/2$ we will need the following $\mathbb{F}_q$-curves on $\mathbb{A}^2_{(t_0,t_1)}$:

$$\begin{aligned} &C_j := \mathrm{num}_j/t_j, \qquad C_{2,v} := \mathrm{num}_2 - v\cdot\mathrm{den}, \qquad C_\infty := \mathrm{den}, \\ &D_{j,x} := t_j^4\cdot\mathrm{num}_2\cdot\mathrm{den} - c^{2j-1}x^2(a\cdot\mathrm{num}_2^2 + \mathrm{den}^2), \\ &L_j := t_j. \qquad \text{For uniformity,} \qquad L_2 := \mathbb{P}^2 \setminus \mathbb{A}^2_{(t_0,t_1)}. \end{aligned} \tag{1}$$

Incidentally, the $\mathbb{F}_{q^2}$-involution $(t_0, t_1) \mapsto \big(t_1/\sqrt{c},\ t_0\sqrt{c}\big)$ gives the isomorphisms $C_j \to C_{j+1}$ and $D_{j,x} \to D_{j+1,x}$. Notice that always

$$\deg(C_j) = \deg(C_{2,v}) = 8, \qquad \deg(C_\infty) = 4, \qquad \deg(D_{j,x}) = 16 \tag{2}$$

and in accordance with [27, Section 2.3.3] the arithmetic genera equal

$$p_a(C_j) = p_a(C_{2,v}) = 21, \qquad p_a(C_\infty) = 3, \qquad p_a(D_{j,x}) = 105. \tag{3}$$

In the degenerate cases we obtain

$$C_{2,0} = F_+ \cup F_-, \qquad C_{2,\pm\beta} = \bigcup_{j,k\,\in\,\mathbb{Z}/2} Q_{j,k,\pm}, \qquad C_\infty = \bigcup_{j,k\,\in\,\mathbb{Z}/2} L_{j,k}, \tag{4}$$

where $\beta := (i\sqrt{a})^{-1}$ and

$$F_\pm := c^2t_0^4 - t_1^4 \pm 4a\sqrt{ac}, \qquad L_{j,k} := (-1)^j\sqrt{(-1)^k ic}\cdot t_0 + t_1,$$
$$Q_{j,k,\pm} := ct_0^2 + (-1)^j t_1^2 + (-1)^k 2\sqrt{\pm c}\sqrt[4]{-a^3}.$$

The curves $F_\pm$ are nothing but Fermat quartics, hence they are non-singular of genus 3. By the way, all the lines $L_{j,k}$ intersect at the origin $(0, 0)$.

Theorem 1. *For $v \notin \{0, \pm\beta\}$, $x \notin \{0, \pm i\sqrt{a}\}$ the curves C_j, $C_{2,v}$, $D_{j,x}$ are absolutely irreducible.*

Proof. Since $C_0 \simeq_{\mathbb{F}_{q^2}} C_1$ and $D_{0,x} \simeq_{\mathbb{F}_{q^2}} D_{1,x}$, it is sufficient to pick $j = 0$. Throughout the proof we tacitly use Magma in order to avoid awkward symbolic computations (see [26]). For instance, it is suggested to resort to this system to establish the absolute irreducibility of C_0. Further, we need the algebraic curves

$$C'_{2,v}(t_0, t_1) := C_{2,v}(\sqrt[4]{t_0}, \sqrt[4]{t_1}), \qquad D'_{0,x}(t_0, t_1) := D_{0,x}(\sqrt[4]{t_0}, \sqrt[4]{t_1})$$

of degrees 2 and 4 respectively.

It is readily seen that the conic $C'_{2,v}$ enjoys the point $R := (1 : c^2 : 0) \in L_2$. The projection from it gives rise to the parametrization

$$pr_R\colon C'_{2,v} \dashrightarrow \mathbb{A}^1_s \qquad pr_R := \frac{c^2 t_0 - t_1}{c^2} \qquad \text{s.t.} \qquad pr_R^{-1}\colon \mathbb{A}^1_s \dashrightarrow C'_{2,v} \qquad pr_R^{-1} = (p_{0,v}, p_{1,v}),$$

where

$$p_{0,v} := \frac{c^2s^2 + 8a^2cvs - 16a^3}{16a^2cv}, \qquad p_{1,v} := \frac{c(c^2s^2 - 8a^2cvs - 16a^3)}{16a^2v}.$$

As a result, the curve $C''_{2,v} := \{t_j^4 = p_{j,v}\}_{j=0}^1$ lying in $\mathbb{A}^3_{(t_0,t_1,s)}$ is birationally isomorphic to $C_{2,v}$ (in the sense of [23, Section 9.7]) by means of the projection $pr_{(t_0,t_1)}$. In particular, $C_{2,v}$ is absolutely irreducible if and only if $C''_{2,v}$ is so.

It can easily be checked that for $v \neq \pm\beta$ the discriminants of $p_{j,v} \in \overline{\mathbb{F}_q}[s]$ are non-zero. So $\sqrt{p_{0,v}} \notin K := \overline{\mathbb{F}_q}(s)$ and by virtue of [28, Proposition 3.7.3] the extension $K' := K\big(\sqrt[4]{p_{0,v}}\big)$ is a Kummer one of degree 4. Also, the polynomials $p_{0,v}$, $p_{1,v}$ do not have common roots. Consequently, a root r of $p_{1,v}$ is non-ramified in the extension K'/K. In other words, there are exactly 4 points $R_j := \big(i^j \sqrt[4]{p_{0,v}(r)}, r\big) \in \mathbb{A}^2_{(t_0,s)}$ over r and the equalities $\nu_{R_j}(p_{1,v}) = \nu_r(p_{1,v}) = 1$ hold for the discrete valuations. Let's apply Eisenstein's irreducibility theorem [28, Proposition 3.1.15.(1)] to the polynomial $t_1^4 - p_{1,v} \in K'[t_1]$ and any point R_j. Recall that $C''_{2,v}$ always has the total fraction ring [23, Section 11.10]. In fact, we have just shown that this ring $\overline{\mathbb{F}_q}(C''_{2,v}) = K'\big(\sqrt[4]{p_{1,v}}\big)$ is a field. As is well known, this is equivalent to the absolute irreducibility of $C''_{2,v}$.

Now we proceed to a similar proof in the case of $D_{0,x}$, but intermediate cumbersome formulas will be omitted for brevity. The quartic $D'_{0,x}$ is birationally isomorphic to the non-degenerate conic

$$Q_x := t_0^2 + (a + x^2)t_1^2 + a(a + x^2) \quad \subset \quad \mathbb{A}^2_{(t_0,t_1)}$$

through an anticanonical map $\varphi_{-can}\colon D'_{0,x} \dashrightarrow Q_x$. Note that Q_x has the point $R := (0, i\sqrt{a})$ and, as usual, the projection from it yields a parametrization $pr_R\colon Q_x \dashrightarrow \mathbb{A}^1_s$. It turns out that the map

$$(pr_R \circ \varphi_{-can})^{-1}\colon \mathbb{A}^1_s \dashrightarrow D'_{0,x} \qquad s \mapsto (f_{0,x}, f_{1,x})$$

is given by the functions $f_{j,x} := A_{j,x}/B_x$ such that

$$A_{0,x} := 4i\sqrt{a}x^2(a + x^2)s^2, \qquad B_x := c\big(s^4 - (a + x^2)^2\big),$$

$$A_{1,x} := 4i\sqrt{a}c^2\big(as^4 + 2\sqrt{a}(a + x^2)s^3 + (a + x^2)(2a + x^2)s^2 + 2\sqrt{a}(a + x^2)^2 s + a(a + x^2)^2\big).$$

As a result, the curve $D''_{0,x} := \{B_x t_j^4 = A_{j,x}\}_{j=0}^1$ lying in $\mathbb{A}^3_{(t_0,t_1,s)}$ is birationally isomorphic to $D_{0,x}$ by means of the projection $pr_{(t_0,t_1)}$. In particular, $D_{0,x}$ is absolutely irreducible if and only if $D''_{0,x}$ is so.

It is shown that

$$\mathrm{Res}(A_{1,x}, B_x) = 2^8 a^2 c^{12} x^6 (x^2+a)^8 (x^2-8a), \qquad \Delta(A_{1,x}) = -2^{16} a^7 c^{12} x^2 (a+x^2)^6 (x^2-8a),$$

where Res, Δ stand for the resultant and discriminant respectively. So we restrict ourselves to $x \notin \{0,\ \pm i\sqrt{a},\ \pm 2\sqrt{2a}\}$. Since trivially $\sqrt{f_{0,x}} \notin K := \overline{\mathbb{F}}_q(s)$, the extension $K' := K\big(\sqrt[4]{f_{0,x}}\big)$ is a Kummer one of degree 4. The polynomials $A_{0,x}$, $A_{1,x}$, B_x do not have common roots in pairs. Consequently, a root r of $A_{1,x}$ is non-ramified in the extension K'/K. In other words, there are exactly 4 points $R_j := \big(i^j \sqrt[4]{f_{0,x}(r)}, r\big) \in \mathbb{A}^2_{(t_0,s)}$ over r and the equalities $\nu_{R_j}(f_{1,x}) = \nu_r(f_{1,x}) = 1$ hold for the discrete valuations. As above, it remains to apply Eisenstein's irreducibility theorem to the polynomial $t_1^4 - f_{1,x} \in K'[t_1]$ and any point R_j. Finally, the case $x = \pm 2\sqrt{2a}$ is immediately processed by Magma. $\square$

3 New hash function

This section clarifies how the rational $\mathbb{F}_q$-map $\varphi := \tau \circ \chi \circ \psi\colon \mathbb{A}^2_{(t_0,t_1)} \dashrightarrow T$ (from the previous one) results in a constant-time map $h\colon (\mathbb{F}_q^*)^2 \to E_a(\mathbb{F}_q)$. First of all, for an element $\gamma \in \mathbb{F}_q^*$ denote by $\big(\frac{\gamma}{q}\big)_4 := \gamma^{(q-1)/4}$ the *quartic residue symbol* [29, Section 4.B], which is evidently a group homomorphism $\mathbb{F}_q^* \to \{i^j\}_{j=0}^3$. Note that $\big(\frac{\gamma}{q}\big)_4 = \pm 1$ if and only if $\sqrt{\gamma} \in \mathbb{F}_q$. Moreover, $\big(\frac{\gamma}{q}\big)_4 = 1$ if and only if $\sqrt[4]{\gamma} \in \mathbb{F}_q$.

To be definite, we assign $i := \big(\frac{c}{q}\big)_4$ for a fixed quadratic non-residue $c \in \mathbb{F}_q^*$. Also, for the sake of compactness, let $f := t^3 + at$ and hence $T = \{y_j^2 = x_j^3 + ac^{2j+1} f x_j\}_{j=0}^1$. Notice that the isomorphism $\sigma_{ac^{2j+1}f,\, a}$ is defined over $\mathbb{F}_q$ whenever $\big(\frac{f}{q}\big)_4 = (-1)^{j+1} i$. One of crucial components of h is the auxiliary map

$$h'\colon T(\mathbb{F}_q) \to E_a(\mathbb{F}_q) \qquad h'(x_0, x_1, y_0, y_1, t) := \begin{cases} \big(t,\ \sqrt{f}\big) & \text{if} \quad \sqrt{f} \in \mathbb{F}_q, \\ \sigma_{acf,\, a}\big(x_0,\ y_0\big) & \text{if} \quad \big(\frac{f}{q}\big)_4 = -i, \\ \sigma_{ac^3 f,\, a}\big(x_1,\ y_1\big) & \text{if} \quad \big(\frac{f}{q}\big)_4 = i. \end{cases}$$

Unfortunately, in this form the value of h' is computed no faster than using two exponentiations in $\mathbb{F}_q$: the first for $\big(\frac{f}{q}\big)_4$ and the second for $\sqrt{f}$, $\sqrt[4]{cf}$, or $\sqrt[4]{c^3 f}$ respectively. Instead, below we give an equivalent definition of h' (up to the automorphisms $[i]^j$, where $j \in \mathbb{Z}/4$).

We will restrict ourselves to the case $q \equiv 5 \pmod 8$ justified in the introduction. The next lemma is useful itself.

Lemma 3. *Consider the numbers*

$$(r, n, k) := \begin{cases} \Big(1,\ \dfrac{3q+1}{16},\ \dfrac{q-5}{16}\Big) & \text{if} \quad q \equiv 5 \pmod{16}, \\ \Big(3,\ \dfrac{q+3}{16},\ \dfrac{q-13}{16}\Big) & \text{if} \quad q \equiv 13 \pmod{16}. \end{cases}$$

For $\gamma \in \mathbb{F}_q^*$ and $\theta := \gamma^n$ we have $\theta^4 = \big(\frac{\gamma}{q}\big)_4^{-r} \cdot \gamma$. In particular, $\sqrt[4]{\gamma} \in \mathbb{F}_q$ if and only if $\theta^4 = \gamma$. Moreover, for $\gamma = u/v$ (with $u,\ v \in \mathbb{F}_q^*$) there are the equalities

$$\theta = \begin{cases} uv^3 (u^3 v^{13})^k & \text{if} \quad q \equiv 5 \pmod{16}, \\ uv^{11} (uv^{15})^k & \text{if} \quad q \equiv 13 \pmod{16}. \end{cases}$$

Proof. If $q \equiv 5 \pmod{16}$, then

$$\theta^4 = \gamma^{4n} = \gamma^{(3q+1)/4} = \gamma^{3(q-1)/4}\cdot\gamma = \left(\frac{\gamma}{q}\right)_4^3\cdot\gamma,$$

$$\theta = (u/v)^n = u^n v^{q-1-n} = u\cdot u^{3k} v^{(13q-17)/16} = uv^3(u^3v^{13})^k.$$

In turn, if $q \equiv 13 \pmod{16}$, then

$$\theta^4 = \gamma^{4n} = \gamma^{(q+3)/4} = \gamma^{(q-1)/4}\cdot\gamma = \left(\frac{\gamma}{q}\right)_4\cdot\gamma,$$

$$\theta = (u/v)^n = u^n v^{q-1-n} = u\cdot u^{k} v^{(15q-19)/16} = uv^{11}(uv^{15})^k.$$

The lemma is proved. $\square$

By the way, the substitution $\gamma = i$ in this lemma gives $\left(\frac{i}{q}\right)_4 = i^r$. At the same time, for $\gamma = f$ (that is $\theta = f^n$) and $j \in \mathbb{Z}/4$ we obtain the criteria

$$\left(\frac{f}{q}\right)_4 = i^{-jr} \qquad \Leftrightarrow \qquad \left(\frac{f}{q}\right)_4 = \left(\frac{i}{q}\right)_4^{-j} \qquad \Leftrightarrow \qquad \left(\frac{i^j f}{q}\right)_4 = 1 \qquad \Leftrightarrow \qquad \theta^4 = i^j f.$$

Therefore

$$j \in \{0, 2\} \qquad \Leftrightarrow \qquad \sqrt{f} \in \mathbb{F}_q \qquad \Leftrightarrow \qquad \theta^4 = \pm f \qquad \Leftrightarrow \qquad \sqrt{f} = \theta^2/\sqrt{\pm 1}.$$

Further, when $j \in \{1, 3\}$, the isomorphism $\sigma_{ac^j f,\, a}$ is defined over $\mathbb{F}_q$ if and only if

$$\sqrt[4]{c^j f} \in \mathbb{F}_q \qquad \Leftrightarrow \qquad \left(\frac{f}{q}\right)_4 = \left(\frac{c}{q}\right)_4^{-j} \qquad \Leftrightarrow \qquad \left(\frac{f}{q}\right)_4 = i^{-j} \qquad \Leftrightarrow \qquad \theta^4 = i^{jr} f.$$

On the other hand, in accordance with Lemma 3 the condition $\sqrt[4]{c^j f} \in \mathbb{F}_q$ exactly means that $\sqrt[4]{c^j f} = d^j\theta$, where $d := c^n$.

Thus h' can be represented in the form

$$h'_m\colon T(\mathbb{F}_q) \to E_a(\mathbb{F}_q) \qquad h'_m(x_0, x_1, y_0, y_1, t) = \begin{cases} [i]^m\left(t,\ \dfrac{\theta^2}{\sqrt{\pm 1}}\right) & \text{if} \quad \theta^4 = \pm f, \\ \left(\dfrac{x_0}{(d\theta)^2}, \dfrac{y_0}{(d\theta)^3}\right) & \text{if} \quad \theta^4 = i^r f, \\ \left(\dfrac{x_1}{(d^3\theta)^2}, \dfrac{y_1}{(d^3\theta)^3}\right) & \text{if} \quad \theta^4 = -i^r f, \end{cases}$$

where $m \in \mathbb{Z}/4$. Obviously, the degenerate case $f = \theta = 0$ is processed by the first condition. More concretely, denote by m the position number of an element $t_0 \in \mathbb{F}_q^*$ in the set $\{i^j t_0\}_{j=0}^3$ 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. Finally, we come to the desired map

$$h\colon (\mathbb{F}_q^*)^2 \to E_a(\mathbb{F}_q) \qquad h(t_0, t_1) := \begin{cases} \mathcal{O} & \text{if} \quad (num_2\cdot den)(t_0, t_1) = 0, \\ (h'_m \circ \varphi)(t_0, t_1) & \text{otherwise.} \end{cases}$$

It is worth emphasizing that due to Lemma 3 the value θ can be computed with the cost of one exponentiation in $\mathbb{F}_q$ even if f is given as a fraction. Besides, in the definition of h'_m the quartic residue symbol does not appear. Further, by returning the value of h in (weighted) projective coordinates (as preferred in practice [1, Sections 2.3.2 and 3.3.2]), we entirely avoid inversions in the field. Also, the constants i, d are found once at the precomputation stage. Calculating the value θ every time no matter whether $num_2 \cdot den \cdot f = 0$ or not, we eventually obtain

Remark 1. *At least when $q \equiv 5 \pmod 8$, the map h is computed in constant time of one exponentiation in $\mathbb{F}_q$.*

4 Indifferentiability from a random oracle

For the sake of compactness, we introduce the reducible curves

$$\begin{aligned} D_x &:= C_{2,x^{-1}} \cup C_{2,-x^{-1}} \cup D_{0,x} \cup D_{1,x}, & C_{\mathcal{O}} &:= C_{2,0} \cup C_\infty, \\ C_\pm &:= C_0 \cup C_1 \cup C_{2,\beta} \cup C_{2,-\beta}, & L &:= L_0 \cup L_1 \cup L_2 \end{aligned}$$

consisting of the curves (1).

Theorem 2. *For any point $P = (x, y) \in E_a(\mathbb{F}_q) \setminus E_a[2]$ we have*

$$h^{-1}\big(\{[i]^j(P)\}_{j=0}^3\big) = D_x(\mathbb{F}_q) \setminus L.$$

In turn,

$$h^{-1}(\mathcal{O}) = C_{\mathcal{O}}(\mathbb{F}_q) \setminus L, \qquad h^{-1}(P_0) = \emptyset, \qquad \text{and} \qquad h^{-1}\big(\{P_\pm\}\big) = C_\pm(\mathbb{F}_q) \setminus L$$

if $\sqrt{a} \in \mathbb{F}_q$.

Proof. Recall that the encoding h is defined via $\varphi = (x_0, x_1, y_0, y_1, t)\colon \mathbb{A}^2_{(t_0,t_1)} \dashrightarrow T$, where

$$x_j = \frac{ct_j^2}{v_2}, \qquad y_j = \frac{v_j}{v_2^2}, \qquad t = \frac{1}{v_2}, \qquad v_0, v_1, v_2 \in \mathbb{F}_q(t_0, t_1).$$

We assume everywhere that $t_j \in \mathbb{F}_q^*$.

First, the condition $h(t_0, t_1) = \mathcal{O}$ means by definition that $(t_0, t_1) \in C_{\mathcal{O}}$. Further, suppose that $(x, 0) = h(t_0, t_1) \in E_a[2] \setminus \{\mathcal{O}\}$. Then $y_0 y_1 = 0$ (i.e., $v_0 v_1 = 0$) or $f = 0$ (i.e., $t \in \{0, \pm i\sqrt{a}\}$). The case $x = 0$ does not occur, because $x_j, t \neq 0$ (or, equivalently, $t_j, \mathrm{den} \neq 0$). In turn, under the condition $x = \pm i\sqrt{a} \in \mathbb{F}_q$ we obtain $(t_0, t_1) \in C_\pm$ as stated in the theorem.

Now let's study the general case $P = (x, y) = h(t_0, t_1) \notin E_a[2]$. Whenever $\sqrt{f} \in \mathbb{F}_q$, we have $P = [i]^m(t, \sqrt{f})$. In other words, $(t_0, t_1) \in C_{2,x^{-1}} \cup C_{2,-x^{-1}}$. Next, assume that $\big(\frac{f}{q}\big)_4 = (-1)^{j+1} i$ and $P = \sigma_{ac^{2j+1}f,\, a}(x_j, y_j)$. There is the sequence of criteria

$$P = \sigma_{ac^{2j+1}f,\, a}(x_j, y_j) \quad \Leftrightarrow \quad x_j = \sqrt{c^{2j+1}f} \cdot x \quad \Leftrightarrow \quad ct_j^2 = v_2\sqrt{c^{2j+1}f} \cdot x \quad \Leftrightarrow \quad t_j^4 = v_2^2 c^{2j-1} f x^2$$

$$\Leftrightarrow \quad t_j^4 = v_2 c^{2j-1}\Big(\frac{1}{v_2^2} + a\Big)x^2 \quad \Leftrightarrow \quad t_j^4 v_2 = c^{2j-1}(1 + av_2^2)x^2 \quad \Leftrightarrow \quad (t_0, t_1) \in D_{j,x}.$$

Thus $P = h(t_0, t_1)$ if and only if $(t_0, t_1) \in D_x$. ∎

Lemma 4. *For two $\mathbb{F}_q$-curves C, $C' \subset \mathbb{P}^2$ without common components there are the inequalities*

$$\#C(\mathbb{F}_q) + \#C'(\mathbb{F}_q) - \deg(C)\deg(C') \ \leqslant\ \#(C \cup C')(\mathbb{F}_q) \ \leqslant\ \#C(\mathbb{F}_q) + \#C'(\mathbb{F}_q).$$

Also, for $C' = L$ we have

$$\#C(\mathbb{F}_q) - 3\deg(C) \ \leqslant\ \#(C \setminus L)(\mathbb{F}_q).$$

Proof. For the first part, it is sufficient to apply a weak version of Bezout's theorem [30, Section 5.3] and the inclusion-exclusion principle:

$$\#(C \cap C')(\mathbb{F}_q) \leqslant \deg(C)\deg(C'), \qquad \#(C \cup C')(\mathbb{F}_q) = \#C(\mathbb{F}_q) + \#C'(\mathbb{F}_q) - \#(C \cap C')(\mathbb{F}_q).$$

Applying the trivial formula

$$\#C(\mathbb{F}_q) - \#(C \cap L)(\mathbb{F}_q) \ =\ \#(C \setminus L)(\mathbb{F}_q)$$

and Bezout's theorem again, we get the second part. □

Corollary 1. *For any point $P \in E_a(\mathbb{F}_q) \setminus E_a[2]$ we have*

$$\#h^{-1}(P) = \#h^{-1}\big([i](P)\big), \qquad |\#h^{-1}(P) - q| \leqslant 126\sqrt{q} + 243.$$

In turn,

$$\#h^{-1}(\mathcal{O}) \leqslant 6q + 12\sqrt{q} + 3, \qquad \#h^{-1}(P_0) = 0, \qquad \textit{and}$$
$$q - 42\sqrt{q} - 239 \ \leqslant\ \#h^{-1}(P_+) = \#h^{-1}(P_-) \ \leqslant\ 5q + 42\sqrt{q} + 5$$

if $\sqrt{a} \in \mathbb{F}_q$.

Proof. All the inequalities follow from Theorem 2, Lemma 4, and the *Weil–Aubry–Perret inequality*

$$|\#C(\mathbb{F}_q) - (q+1)| \leqslant 2p_a(C)\sqrt{q} \qquad \text{[31, Corollary 2.4]}$$

for the number of $\mathbb{F}_q$-points on a projective (possibly singular) absolutely irreducible $\mathbb{F}_q$-curve C. Let us apply these results below without further mentioning.

Obviously, $\#h^{-1}(P_0) = 0$. Besides, according to the decompositions (4) we obtain

$$\#C_{2,0}(\mathbb{F}_q) \leqslant 2(q + 1 + 6\sqrt{q}), \qquad \#C_\infty(\mathbb{F}_q) \leqslant 4q + 1.$$

We can not provide non-trivial lower bounds, because the components of $C_{2,0}$, C_∞ may be $\mathbb{F}_q$-conjugate. Therefore there is only the upper bound

$$\#h^{-1}(\mathcal{O}) \ =\ \#(C_\mathcal{O} \setminus L)(\mathbb{F}_q) \ \leqslant\ \#C_\mathcal{O}(\mathbb{F}_q) \ \leqslant\ \#C_{2,0}(\mathbb{F}_q) + \#C_\infty(\mathbb{F}_q) \ \leqslant\ 6q + 12\sqrt{q} + 3.$$

From now on, we focus on the case $P = (x, y) = h(t_0, t_1) \notin \{P_0, \mathcal{O}\}$, where $t_j \in \mathbb{F}_q^*$ as usual. Notice that x_j/t_j^2, y_j/t_j, $t \in \mathbb{F}_q(t_0^4, t_1^4)$ and, in particular, $f \in \mathbb{F}_q(t_0^4, t_1^4)$. We conclude that

$$\varphi(it_0, t_1) = (-x_0, x_1, iy_0, y_1, t), \qquad \varphi(t_0, it_1) = (x_0, -x_1, y_0, iy_1, t)$$

and therefore

$$[i](P) = \begin{cases} h(it_0, t_1) & \text{if} \quad \left(\frac{f}{q}\right)_4 = -i, \\ h(t_0, it_1) & \text{if} \quad \left(\frac{f}{q}\right)_4 = i. \end{cases}$$

Also, in the case $\sqrt{f} \in \mathbb{F}_q$ the weaker property

$$\{[i]^j(P)\}_{j=0}^3 = h\big(\{(i^j t_0, t_1)\}_{j=0}^3\big)$$

still holds by using the position number m of t_0. Taking into account that D_x, $C_\pm \in \mathbb{F}_q[t_0^4, t_1^4]$, we eventually get

$$\#h^{-1}(P) = \#h^{-1}\big([i](P)\big) \qquad \text{and so} \qquad 4{\cdot}\#h^{-1}(P) = \#(D_x \setminus L)(\mathbb{F}_q)$$

if $P \notin E_a[2]$ as well as

$$\#h^{-1}(P_+) = \#h^{-1}(P_-) \qquad \text{and so} \qquad 2{\cdot}\#h^{-1}(P_\pm) = \#(C_\pm \setminus L)(\mathbb{F}_q)$$

if $\sqrt{a} \in \mathbb{F}_q$.

Equalities (2) result in the ones

$$\deg(C_0 \cup C_1) = \deg(C_{2,\beta} \cup C_{2,-\beta}) = 16 \qquad \text{and hence} \qquad \deg(C_\pm) = 32.$$

As a result, for

$$N := \#C_0(\mathbb{F}_q) + \#C_1(\mathbb{F}_q) + \#C_{2,\beta}(\mathbb{F}_q) + \#C_{2,-\beta}(\mathbb{F}_q)$$

it is true that

$$N - 384 \;=\; N - 2{\cdot}8^2 - 16^2 \;\leqslant\; \#(C_0 \cup C_1)(\mathbb{F}_q) + \#(C_{2,\beta} \cup C_{2,-\beta})(\mathbb{F}_q) - 16^2 \;\leqslant\; \#C_\pm(\mathbb{F}_q).$$

At the same time, by virtue of Equalities (3), (4) and Theorem 1 we obtain

$$|\#C_j(\mathbb{F}_q) - (q+1)| \leqslant 42\sqrt{q}, \qquad \#C_{2,\pm\beta}(\mathbb{F}_q) \leqslant 4(q+1).$$

We can not provide a non-trivial lower bound for $\#C_{2,\pm\beta}(\mathbb{F}_q)$, because the conics $Q_{j,k,\pm}$ may be $\mathbb{F}_q$-conjugate. Thus

$$2q - 84\sqrt{q} - 478 \;=\; 2(q + 1 - 42\sqrt{q}) - 384 - 3{\cdot}32 \;\leqslant$$

$$\#C_\pm(\mathbb{F}_q) - 3{\cdot}32 \;\leqslant\; \#(C_\pm \setminus L)(\mathbb{F}_q) \;\leqslant\; \#C_\pm(\mathbb{F}_q) \;\leqslant\; N \;\leqslant\; 10q + 84\sqrt{q} + 10.$$

Eventually, we establish the desired inequalities

$$q - 42\sqrt{q} - 239 \;\leqslant\; \#h^{-1}(P_\pm) \;\leqslant\; 5q + 42\sqrt{q} + 5.$$

Equalities (2) result in the ones

$$\deg(C_{2,x^{-1}} \cup C_{2,-x^{-1}}) = 16, \qquad \deg(D_{0,x} \cup D_{1,x}) = 32, \qquad \text{and hence} \qquad \deg(D_x) = 48.$$

As a result, for

$$N_x := \#C_{2,x^{-1}}(\mathbb{F}_q) + \#C_{2,-x^{-1}}(\mathbb{F}_q) + \#D_{0,x}(\mathbb{F}_q) + \#D_{1,x}(\mathbb{F}_q)$$

it is true that

$$N_x - 832 \;=\; N_x - 8^2 - 16^2 - 16{\cdot}32 \;\leqslant\; \#(C_{2,x^{-1}} \cup C_{2,-x^{-1}})(\mathbb{F}_q) + \#(D_{0,x} \cup D_{1,x})(\mathbb{F}_q) - 16{\cdot}32$$

$\leqslant \#D_x(\mathbb{F}_q)$. At the same time, by virtue of Equalities (3) and Theorem 1 we obtain

$$|\#C_{2,\pm x^{-1}}(\mathbb{F}_q) - (q+1)| \leqslant 42\sqrt{q}, \qquad |\#D_{j,x}(\mathbb{F}_q) - (q+1)| \leqslant 210\sqrt{q}.$$

Thus

$$4q - 504\sqrt{q} - 972 \;=\; 4(q+1) - 504\sqrt{q} - 832 - 3{\cdot}48 \;\leqslant$$
$$\#D_x(\mathbb{F}_q) - 3{\cdot}48 \;\leqslant\; \#(D_x \setminus L)(\mathbb{F}_q) \;\leqslant\; \#D_x(\mathbb{F}_q) \;\leqslant\; N_x \;\leqslant\; 4(q+1) + 504\sqrt{q}$$

Eventually, we establish the inequalities

$$|4{\cdot}\#h^{-1}(P) - 4q| \leqslant 504\sqrt{q} + 972 \qquad \text{and hence} \qquad |\#h^{-1}(P) - q| \leqslant 126\sqrt{q} + 243.$$

The corollary is proved. □

Corollary 2. *The distribution on $E_a(\mathbb{F}_q)$ defined by h is ϵ-statistically indistinguishable from the uniform one* [9, Definition 3]*, where $\epsilon := 2^7 q^{-1/2} + O(q^{-1})$.*

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

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

where

$$\gamma(P) := \left|\frac{\#h^{-1}(P)}{(q-1)^2} - \frac{1}{q-1}\right| = \frac{|\#h^{-1}(P) - (q-1)|}{(q-1)^2}.$$

If $P \notin E_a[2]$ from Corollary 1 we immediately obtain

$$\gamma(P) \leqslant \frac{126\sqrt{q} + 244}{(q-1)^2} \qquad \text{and so} \qquad \delta(P) = \frac{2^7}{q^{3/2}} + O\Big(\frac{1}{q^2}\Big).$$

Besides, it is readily seen that $\delta(P_0)$, $\delta(P_\pm)$, $\delta(\mathcal{O}) \in O(q^{-1})$. Thus

$$\sum_{P \in E_a(\mathbb{F}_q)} \delta(P) \;\leqslant\; \big(q + 2\sqrt{q} + 1 - \#E_a(\mathbb{F}_q)[2]\big)\Big(\frac{2^7}{q^{3/2}} + O\Big(\frac{1}{q^2}\Big)\Big) + \sum_{P \in E_a(\mathbb{F}_q)[2]} \delta(P) \;=\; \frac{2^7}{q^{1/2}} + O\Big(\frac{1}{q}\Big).$$

The corollary is proved. □

Probably, the coefficient 2^7 may be reduced even more by analysing singularities of the curves $C_{2,v}$, $D_{j,x}$. For simplicity of the exposition, this analysis is omitted, because the value $2^7 q^{-1/2}$ is still negligible for q of a cryptographic size.

For $t_1 \in \mathbb{F}_q^*$ consider the encoding $h_{t_1} : \mathbb{F}_q^* \to E_a(\mathbb{F}_q)$ of the form $h_{t_1}(t_0) := h(t_0, t_1)$. Clearly, [9, Algorithm 1] still works well in the case of h. Indeed, for $P \in E_a(\mathbb{F}_q)$ pick uniformly at random $t_1 \in \mathbb{F}_q^*$ and then find uniformly at random $t_0 \in h_{t_1}^{-1}(P)$. For instance, when $P \notin E_a[2]$, the latter consists in computing a non-zero $\mathbb{F}_q$-root (if any) of one of the four polynomials $C_{2,\pm x^{-1}}$, $D_{j,x} \in \mathbb{F}_q[t_0^4]$ chosen randomly. We eventually obtain

Remark 2. *The map h is samplable* [9, Definition 4].

Remarks 1, 2 and Corollary 2 imply that h is an admissible map. Finally, using [9, Theorem 1], we establish

Corollary 3. *Consider the composition $H := h \circ \mathfrak{h}\colon \{0,1\}^* \to E_a(\mathbb{F}_q)$ 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.*

If in the given corollary one desires to use a random oracle of the form $\mathfrak{h}\colon \{0,1\}^* \to \mathbb{F}_q^2$, the map h can be (manually) extended to $\mathbb{F}_q^2$, e.g., as for h from [15, Section 2]. It is clear that such an extension does not affect the admissibility of our h. On the other hand, it is not more difficult to construct a random oracle $\mathfrak{h}\colon \{0,1\}^* \to (\mathbb{F}_q^*)^2$, acting by analogy with [9, Lemma 14 and Remark 1]. Indeed, the value of an indifferentiable hash function $\{0,1\}^* \to \mathbb{F}_q$ is equal to 0 with a negligible probability. Even so, it is suggested to return, e.g., 1. It follows easily that the indifferentiability still holds.

Acknowledgements. The author is grateful to Trepalin A. for answering some of his questions on rational surfaces over finite fields.

References

[1] El Mrabet N., Joye M., *Guide to pairing-based cryptography*, Cryptography and Network Security Series, Chapman and Hall/CRC, New York, 2017.

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

[3] Pornin T., *Double-odd elliptic curves*, https://eprint.iacr.org/2020/1558, 2020.

[4] Pornin T. et al., *Double-odd elliptic curves*, https://doubleodd.group.

[5] Hamburg M., "Decaf: Eliminating cofactors through point compression", Advances in Cryptology – CRYPTO 2015, LNCS, **9215**, eds. Gennaro R., Robshaw M., Springer, Berlin, Heidelberg, 2015, 705–723.

[6] Boneh D. et al., *BLS signatures*, https://datatracker.ietf.org/doc/draft-irtf-cfrg-bls-signature, 2022.

[7] Faz-Hernandez A. et al., *Hashing to elliptic curves*, https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve, 2022.

[8] Maurer U. M., Renner R., Holenstein C., "Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology", Theory of Cryptography Conference 2004, LNCS, **2951**, eds. Naor M., Springer, Berlin, Heidelberg, 2004, 21–39.

[9] Brier E. et al., "Efficient indifferentiable hashing into ordinary elliptic curves", Advances in Cryptology — CRYPTO 2010, LNCS, **6223**, eds. Rabin T., Springer, Berlin, Heidelberg, 2010, 237–254.

[10] Koshelev D., *Optimal encodings to elliptic curves of j-invariants* 0*,* 1728, https://eprint.iacr.org/2021/1034, 2021.

[11] Koshelev D., "Hashing to elliptic curves of j-invariant 1728", *Cryptography and Communications*, **13**:4 (2021), 479–494.

[12] Koshelev D., *Some remarks on how to hash faster onto elliptic curves*, https://eprint.iacr.org/2021/1082, 2021.

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

[14] Hulek K., Kloosterman R., “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] Koshelev D., “Indifferentiable hashing to ordinary elliptic $\mathbb{F}_q$-curves of $j = 0$ with the cost of one exponentiation in $\mathbb{F}_q$”, *Designs, Codes and Cryptography*, **90**:3 (2022), 801–812.

[16] Chávez-Saab J., Rodriguez-Henriquez F., Tibouchi M., *SwiftEC: Shallue–van de Woestijne indifferentiable function to elliptic curves. Faster indifferentiable hashing to most elliptic curves*, https://eprint.iacr.org/2022/759, 2022.

[17] Shallue A., van de Woestijne C. E., “Construction of rational points on elliptic curves over finite fields”, ANTS 2006, LNCS, **4076**, eds. Hess F., Pauli S., Pohst M., Springer, Berlin, Heidelberg, 2006, 510–524.

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

[19] Hübsch T., *Calabi–Yau manifolds: A bestiary for physicists*, World Scientific, Singapore, 1992.

[20] Yui N., “The arithmetic of certain Calabi–Yau varieties over number fields”, The Arithmetic and Geometry of Algebraic Cycles, NATO Science Series, **548**, eds. Gordon B. B. et al., Springer, Dordrecht, 2000, 515–560.

[21] Im B.-H., Larsen M., “Rational curves on quotients of abelian varieties by finite groups”, *Mathematical Research Letters*, **22**:4 (2015), 1145–1157.

[22] Schoen C., “On fiber products of rational elliptic surfaces with section”, *Mathematische Zeitschrift*, **197**:2 (1988), 177–199.

[23] Görtz U., Wedhorn T., *Algebraic geometry I: Schemes*, Studium Mathematik - Master, Springer, Wiesbaden, 2020.

[24] Dolgachev I. V., *Classical algebraic geometry: A modern view*, Cambridge University Press, Cambridge, 2012.

[25] Bryan J., appendix with Pietromonaco S., “The Donaldson–Thomas partition function of the banana manifold”, *Algebraic Geometry*, **8**:2 (2021), 133–170.

[26] Koshelev D., *Magma code*, https://github.com/dishport/The-most-efficient-indifferentiable-hashing-to-elliptic-curves-of-j-invariant-1728, 2021.

[27] Tsfasman M., Vlăduţ S., Nogin D., *Algebraic geometric codes: Basic notions*, Mathematical Surveys and Monographs, **139**, American Mathematical Society, Providence, 2007.

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

[29] Cox D. A., *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, Pure and Applied Mathematics, John Wiley & Sons, New York, 2011.

[30] Fulton W., *Algebraic curves: An introduction to algebraic geometry*, Addison-Wesley, Boston, 2008.

[31] Aubry Y., Perret M., “A Weil theorem for singular curves”, Arithmetic, Geometry, and Coding Theory, Proceedings in Mathematics, eds. Pellikaan R., Perret M., Vlăduţ S. G., De Gruyter, Berlin, 1996, 1–7.