Optimal encodings to elliptic curves of j-invariants 0, 1728

Dmitrii Koshelev [1]

Computer sciences and networks department, Télécom Paris

Abstract. This article provides new constant-time encodings $\mathbb{F}_q^* \to E(\mathbb{F}_q)$ to ordinary elliptic $\mathbb{F}_q$-curves E of j-invariants 0, 1728 having a small prime divisor of the Frobenius trace. Therefore all curves of $j = 1728$ are covered. This is also true for the Barreto–Naehrig curves BN512, BN638 from the international cryptographic standards ISO/IEC 15946-5, TCG Algorithm Registry, and FIDO ECDAA Algorithm. Many $j = 1728$ curves as well as BN512, BN638 do not have $\mathbb{F}_q$-isogenies of small degree from other elliptic curves. So, in fact, only universal SW (Shallue–van de Woestijne) encoding was previously applicable to them. However this encoding (in contrast to ours) can not be computed at the cost of one exponentiation in the field $\mathbb{F}_q$.

Key words: congruent elliptic curves, encodings to (hyper)elliptic curves, isogenies, j-invariants 0, 1728, median value curves, optimal covers, Weil pairing

Introduction

Let $\mathbb{F}_q$ be a finite field of characteristic $p > 5$ and $E = E_{a,b}\colon y^2 = x^3 - ax + b$ be an elliptic $\mathbb{F}_q$-curve. Many protocols of elliptic cryptography use a *hash function* [1, §3] of the form $\mathcal{H}\colon \{0,1\}^* \to E(\mathbb{F}_q)$. It is often constructed with the help of an auxiliary map $h\colon \mathbb{P}^1(\mathbb{F}_q) \to E(\mathbb{F}_q)$, called *encoding*, such that $\#\mathrm{Im}(h) \geqslant (q+1)/n$ for some $n \in \mathbb{N}$. Clearly, the smaller the value n, the better, because h covers more $\mathbb{F}_q$-points. By the way, Hasse's bound says that $|t| \leqslant 2\sqrt{q}$ for $N := \#E(\mathbb{F}_q)$ and the Frobenius trace $t = q + 1 - N$. Good surveys on how to hash into elliptic curves are represented in [2, §8], [3].

In practice, h needs to be computed in constant time, otherwise it is vulnerable to timing attacks [2, §8.2.2, §12.1.1]. Besides, it is more convenient to restrict h to the multiplicative group $\mathbb{F}_q^*$, because, as a rule, $h(0)$, $h(\infty)$ are points of small orders. There are (e.g., in [3, §5]) standard hash functions $\eta\colon \{0,1\}^* \to \mathbb{F}_q^*$, hence the composition $\mathcal{H} = h \circ \eta$ gives the desired hash function. If we additionally require $\mathcal{H}$ to be a *random oracle* [1, §3.7], then according to [4] it is enough to apply h twice, varying η, and to sum the resulting points. In this case, h must be *well-distributed*, but we do not know of a single natural example that would not be like this.

There is the *SW encoding* [2, §8.3.4], [3, §6.6.1], which is applicable to any elliptic curve. However at least several exponentiations in $\mathbb{F}_q$ are required to evaluate it. In turn, all other known encodings, including those constructed in this article, make do with only one if implemented correctly. This is what we mean whenever we talk about the encoding efficiency in this article. At first glance, such speedup seems insignificant, but some modern cryptographic

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

protocols (like the aggregated BLS signature [5]) call the hash function $\mathcal{H}$ many times. So the cumulative gain is large.

If j-invariant of E is different from 0, 1728, i.e., $ab \neq 0$, then one can apply the *simplified SWU encoding* h (see, e.g., [6, §2.4, §4.1]), which seems significantly unimprovable. Also, consider the curves $E_b\colon y^2 = x^3 + b$ and $E_a\colon y^2 = x^3 - ax$ of j-invariants 0, 1728 respectively. Having an $\mathbb{F}_q$-isogeny of small degree $\varphi\colon E \to E_b$ (resp. $\varphi\colon E \to E_a$) that is vertical (i.e., $j(E) \neq 0, 1728$), we obviously obtain the fast encoding $\varphi \circ h$ to E_b (resp. E_a). This was first seen in [6, §4]. In particular, it is a simple exercise that such an isogeny of degree 2 exists if and only if $\sqrt[3]{b} \in \mathbb{F}_q$ (resp. $\sqrt{a} \in \mathbb{F}_q$). Therefore, without loss of generality, we can focus only on curves E_b, E_a not satisfying the last conditions. We have to process such curves as well, because among them exist many *pairing-friendly* ones [2, §4], [7].

For $q \equiv 2 \pmod 3$ (resp. $q \equiv 3 \pmod 4$) there is in [2, §8.3.2] (resp. [8]) a bijective encoding to E_b (resp. E_a). The former is said to be the *Boneh–Franklin encoding*. The given curves are so-called *median value curves* [9, §3.4], that is for them $N = q + 1$ or, equivalently, $t = 0$. As a consequence of [1, Theorem 9.11.2], they are supersingular. Although there are supersingular curves E_b, E_a with other orders N, to be definite in this article we will deal only with ordinary curves. The fact is that in pre-quantum cryptography supersingular ones are considered to be weak [2, §4.3, §9.1.3]. However, many of our results for E_b (resp. E_a) seem to hold true if $q \equiv 1 \pmod 3$ (resp. $q \equiv 1 \pmod 4$).

It is natural to wonder about non-constant $\mathbb{F}_q$-covers $\varphi\colon C \to E$ (for various elliptic curves E) of small degree by smooth curves C of greater genus g for which there is an efficient encoding $\mathbb{P}^1(\mathbb{F}_q) \to C(\mathbb{F}_q)$. To our knowledge, there are two types of such curves, namely *cyclic trigonal curves* T, also known as *trielliptic*, (see, e.g., [10, §2]) for $q \equiv 2 \pmod 3$ and so-called *odd hyperelliptic curves* H [8, §2] for $q \equiv 3 \pmod 4$. One of covers of the first type is implicitly proposed by Icart in [11, §2] (see also [12]). In turn, covers of the second type (with $g = \deg(\varphi) = 2$) are constructed by Fouque–Joux–Tibouchi in [13, §3] under the additional condition $4 \mid N$. The encodings to T, H are trivial generalizations of the encodings to the median value curves E_b, E_a respectively. Unlike T, the curves H also have $\#H(\mathbb{F}_q) = q + 1$. However they are not necessarily supersingular, because in contrast to the genus 1 case this property equally depends on $\#H(\mathbb{F}_{q^2})$ (cf. [9, Example 3.15]).

Recall a series of notions and results, which can be found in [14, §1], [15, §1-2]. Elliptic $\mathbb{F}_q$-curves E, E' are called *n-congruent* (where $p \nmid n \in \mathbb{N}$) if there is an isomorphism $\tau\colon E[n] \xrightarrow{\sim} E'[n]$ of the Frobenius modules. Then τ is said to be an *anti-isometry* (and E, E' are *reversely n-congruent*) with respect to the Weil pairing e_n whenever $e_n\big(\tau(P_0), \tau(P_1)\big) = e_n^{-1}(P_0, P_1)$ for all points $P_0, P_1 \in E[n]$. The last identity exactly means that the graph Γ_τ of τ is a *maximal isotropic subgroup* with respect to the Weil pairing on $A := E \times E'$. Therefore the quotient map $\widehat{\Phi}\colon A \to A/\Gamma_\tau$ is an $\mathbb{F}_q$-isogeny to a *principally polarized* abelian surface A/Γ_τ. The mentioned construction is also referred to as *gluing* (or *tying*) E, E' *along their n-torsion subgroups via* τ.

If A/Γ_τ is isomorphic as PPAS to the Jacobian J of some curve H, then τ is called *irreducible*. There is in [14, §2] the powerful Kani criterion of irreducibility. In this case, the dual isogeny $\Phi\colon J \to A$ is the natural extension of some $\mathbb{F}_q$-covers $\varphi\colon H \to E$, $\varphi'\colon H \to E'$ of degree n. Moreover, they are *optimal*, i.e., there is no decomposition into non-trivial $\mathbb{F}_q$-covers $H \to F$, $F \to E$ (resp. $F \to E'$) for some elliptic curve F. In the literature one may also encounter the terms *maximal*, or vice versa, *minimal*. In addition to the optimality, φ, φ'

are *complementary covers* to each other in the sense of [15, §2]. Conversely, any pair of such covers induces an $\mathbb{F}_q$-isogeny $\Phi\colon J \to A$ and hence its dual $\widehat{\Phi}\colon A \to J$. Besides, the kernel of $\widehat{\Phi}$ is the graph Γ_τ of some (irreducible) $\mathbb{F}_q$-anti-isometry $\tau\colon E[n] \xrightarrow{\sim} E'[n]$.

From now on let $E'\colon cy^2 = x^3 - ax + b \simeq_{\mathbb{F}_q} E_{ac^2,bc^3}$ denote the quadratic twist of E (unique up to an $\mathbb{F}_q$-isomorphism), where $c \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^2$. Surprisingly, for $E = E_a$ and $q \equiv 3 \pmod 4$ this twist is trivial, i.e., $E \simeq_{\mathbb{F}_q} E'$, because, without loss of generality, take $c = -1$. If we are not mistaken, this is the only possible counterexample, that is why authors often forget to say about it. A correct equation of the non-trivial quadratic twist of E_a and other useful information about twists (not necessarily quadratic) of elliptic curves are provided in [16, §X.5-X.6]. As is known (e.g., from [1, Exercise 9.5.4]), $-t$ is the Frobenius trace of E'. Consequently, the curves E, E' are not $\mathbb{F}_q$-isogenous whenever $t \neq 0$ as assumed above. Therefore this pair of curves is never *trivial*, that is a congruence $E[n] \xrightarrow{\sim} E'[n]$ (if any) is not the restriction of an $\mathbb{F}_q$-isogeny $E \to E'$.

In the new terms, the Fouque–Joux–Tibouchi approach consists of tying E, E' (with the restrictions on q, N) along the subgroup $E[2] = E'[2]$ via an irreducible $\mathbb{F}_q$-(anti)-isometry τ. Curiously, for the curves E_b, E_a such τ exists if and only if, as before, $\sqrt[3]{b} \in \mathbb{F}_q$, $\sqrt{a} \in \mathbb{F}_q$ respectively (see §3.1, §2.1). In fact, by virtue of [17, Proposition 3] the required τ is easily constructed depending on $\#E(\mathbb{F}_q)[2]$ for all elliptic $\mathbb{F}_q$-curves E of $j \neq 0, 1728$. The fact is that they do not have non-trivial automorphisms, hence any non-identical τ is automatically irreducible.

The given article tries to extend the considered approach to greater degrees n in order to cover remaining curves E_b, E_a. First of all, we analyse in what situation this is possible. Fortunately, for any curve E_a it is sufficient to take $n \leqslant 4$ due to §2 (the general case $n = 4$ is treated in §2.3). At the same time, for curves E_b the situation is more complicated. Among other things, we generalize in §4 the class of odd hyperelliptic curves to a much wider one of median value curves. Moreover, for every representative H of this class we still have an efficient encoding $h\colon \mathbb{P}^1(\mathbb{F}_q) \xrightarrow{\sim} H(\mathbb{F}_q)$. We are interested in the smallest possible n, because obviously $\#\mathrm{Im}(\varphi \circ h) \geqslant (q+1)/n$, not to mention that for smaller n formulas of the cover φ are more compact and faster to compute.

We explain in §3.3 that, dealing with curves E_b, it is enough to restrict ourselves to prime degrees $\ell = n \geqslant 5$. In accordance with our Theorem 1 degree ℓ (optimal) covers $\varphi\colon H \to E_b$, $\varphi'\colon H \to E_b'$ exist if and only if $\ell \mid t$. Unfortunately, there are curves E_b (even pairing-friendly) without small divisors of t. Nevertheless, in §3.2 we study in detail the case $\ell = 5$, which is valid for some standardized *Barreto–Naehrig* $\mathbb{F}_p$-*curves* [2, Example 4.2]. It is about BN512 ($b = 3$) and BN638 ($b = 257$) from the standards [18], [19, §5.2.8], [20, §4.1]. By means of [1, Theorem 25.4.6] we determine that the smallest (prime) degree of a vertical $\mathbb{F}_p$-isogeny for BN512 (resp. BN638) equals 1291 (resp. 1523). Thus our new encodings are the best known ones, as far as we know.

We essentially improve results from our article [21] (resp. [22]), where we implicitly provide non-optimal $\mathbb{F}_q$-covers of degree 8 (resp. 20) to the curves E_a, E_a' (resp. E_b, E_b' for the case $5 \mid t$). We did not notice this circumstance earlier. So in the light of the current article our previous ones lose relevance. By the way, there we use the language of rational $\mathbb{F}_q$-curves (and their parametrizations) on the *Kummer surface* $A/[-1]$. However, as is known (e.g., from [23]), it is equivalent to the language of $\mathbb{F}_q$-covers by hyperelliptic curves (not necessarily of genus 2).

1 Preliminaries

We continue to work with an ordinary elliptic curve $E\colon y^2 = x^3 - ax + b$ over a finite field $\mathbb{F}_q$ of characteristic $p > 5$. As is customary, let us use the same symbol for $E \subset \mathbb{A}^2_{(x,y)}$ and $E \cup \mathcal{O} \subset \mathbb{P}^2$, where $\mathcal{O} := (0 : 1 : 0)$. As said before, $E'\colon cy^2 = x^3 - ax + b$, where $c \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^2$, stands for the (non-trivial) quadratic twist of E. In formulas instead of E' we will use the fairly standard notation E^c in order to stress the choice c. The corresponding $\mathbb{F}_{q^2}$-isomorphism has the form

$$\sigma\colon E \xrightarrow{\sim} E^c \qquad (x, y) \mapsto (x, y/\sqrt{c}).$$

Let t (resp. $-t$) be the Frobenius trace of E (resp. E'). Recall that $p \nmid t$ for ordinary curves according to one of their equivalent definitions. Since the traces of n-congruent elliptic curves coincide modulo n, we obtain the elementary

Lemma 1. *If the curves E, E' are n-congruent for $n \in \mathbb{N}$ such that $p \nmid n$, then $n \mid 2t$.*

Also, we have

Theorem 1. *For every prime $\ell \neq 2, p$ the following statements are equivalent:*

1. *$\ell \mid t$;*
2. *the curves E, E' are reversely ℓ-congruent;*
3. *there is an irreducible $\mathbb{F}_q$-anti-isometry $E[\ell] \simeq E'[\ell]$;*
4. *E has a vertical (in the sense of* [1, Definition 25.4.2]*) degree ℓ isogeny defined over $\mathbb{F}_{q^2}$, but not over $\mathbb{F}_q$.*

Proof. Denote by Fr, Fr$'$ the Frobenius endomorphisms on E, E' respectively. By definition, the curves are ℓ-congruent if and only if there is a group isomorphism $\tau\colon E[\ell] \xrightarrow{\sim} E'[\ell]$ such that $\mathrm{Fr}' \circ \tau = \tau \circ \mathrm{Fr}$. Since $E[\ell] \simeq E'[\ell] \simeq (\mathbb{Z}/\ell)^2$ as abstract groups, we can represent the maps Fr, Fr$'$, τ by means of matrices $\mathrm{M}_{\mathrm{Fr}}, \mathrm{M}_{\mathrm{Fr}'}, \mathrm{M}_\tau \in \mathrm{GL}_2(\mathbb{Z}/\ell)$. Given a basis $\{P_0, P_1\}$ of $E[\ell]$ it is natural to take $\{\sigma(P_0), \sigma(P_1)\}$ as a basis of $E'[\ell]$. Without loss of generality, assume that M_{Fr} is the rational canonical form (also known as the Frobenius normal form). Since the characteristic polynomial of Fr equals $\chi_{\mathrm{Fr}}(x) = x^2 - tx + q$ and $\mathrm{Fr}' \circ \sigma = -\sigma \circ \mathrm{Fr}$, we obtain

$$\mathrm{M}_{\mathrm{Fr}} = \lambda \mathrm{I}_2 \qquad \text{or} \qquad \mathrm{M}_{\mathrm{Fr}} = \begin{pmatrix} 0 & -q \\ 1 & t \end{pmatrix}, \qquad \mathrm{M}_{\mathrm{Fr}'} = -\mathrm{M}_{\mathrm{Fr}}, \qquad \mathrm{M}_\tau = \begin{pmatrix} m_0 & m_1 \\ m_2 & m_3 \end{pmatrix}$$

for the unit matrix I_2 and some $\lambda, m_k \in \mathbb{Z}/\ell$, $\lambda \neq 0$. As is known, M_{Fr} depends on whether χ_{Fr} coincides with the minimal polynomial of Fr.

By abuse of notation, all the next equations are modulo ℓ. The condition $\mathrm{Fr}' \circ \tau = \tau \circ \mathrm{Fr}$ means that $-\mathrm{M_{Fr}} \cdot \mathrm{M}_\tau = \mathrm{M}_\tau \cdot \mathrm{M_{Fr}}$, i.e., $\mathrm{M_{Fr}} \neq \lambda \mathrm{I}_2$ and

$$\begin{cases} -qm_2 = -m_1, \\ -qm_3 = qm_0 - tm_1, \\ m_0 + tm_2 = -m_3, \\ m_1 + tm_3 = qm_2 - tm_3. \end{cases} \Leftrightarrow \begin{cases} m_1 = qm_2, \\ -qm_3 = qm_0 - tqm_2, \\ m_0 + tm_2 = -m_3, \\ 2tm_3 = 0. \end{cases} \Leftrightarrow \begin{cases} m_1 = qm_2, \\ -m_3 = m_0 - tm_2, \\ -m_3 = m_0 + tm_2, \\ tm_3 = 0. \end{cases} \Leftrightarrow \begin{cases} m_1 = qm_2, \\ m_0 = -m_3, \\ t = 0. \end{cases}$$

The fact $\mathrm{tr}(\lambda \mathrm{I}_2) = 2\lambda \neq 0$ implies that 1 $\Leftrightarrow$ 2 whenever $\mathrm{M_{Fr}} = \lambda \mathrm{I}_2$. In opposite case, it remains to prove the implication 1 $\Rightarrow$ 2. Notice that the congruence τ is an anti-isometry if and only if $\det(\mathrm{M}_\tau) = -1$. For m_0, m_1 from the last linear system we get $\det(\mathrm{M}_\tau) = -(m_3^2 + qm_2^2)$, hence it is sufficient to assign $m_2 = 0$, $m_3 = 1$.

Putting $F := E'$ in [24, Lemma 4.5], we conclude that τ is never reducible, because the isomorphism $\sigma\colon E[\ell] \xrightarrow{\sim} E'[\ell]$ is Frobenius equivariant only for $\ell = 2$. Therefore we established the criterion 2 $\Leftrightarrow$ 3.

Further, we show the equivalence 1 $\Leftrightarrow$ 4. Let us freely use results from [1, §25.4.1]. Denote by f_0 the conductor of the endomorphism ring $\mathrm{End}(E)$ and by $D < 0$ the discriminant of the imaginary quadratic field $\mathrm{End}(E) \otimes \mathbb{Q}$. The discriminant of χ_{Fr} equals $D_1 = t^2 - 4q = Df_1^2$, where $f_1 \in \mathbb{N}$ (s.t. $f_0 \mid f_1$) is the conductor of the order $\mathbb{Z}[\mathrm{Fr}]$. Since over $\mathbb{F}_{q^2}$ the Frobenius endomorphism Fr^2 has the trace $t_2 = t^2 - 2q$ [1, Exercise 9.10.9], the discriminant of its characteristic polynomial equals $t_2^2 - 4q^2 = D_1 t^2 = Df_2^2$, where $f_2 = f_1 t$ is the conductor of $\mathbb{Z}[\mathrm{Fr}^2]$. In other words, $t = \left[\mathbb{Z}[\mathrm{Fr}] : \mathbb{Z}[\mathrm{Fr}^2]\right]$.

Our next reasoning is based on [1, Theorem 25.4.6]. Assume that E has a degree ℓ vertical $\mathbb{F}_{q^2}$-isogeny not defined over $\mathbb{F}_q$. It is descending, because the (unique) ascending isogeny of E (if it exists) is always defined over $\mathbb{F}_q$. As a result, $\ell \mid \frac{f_2}{f_0}$ and $\ell \nmid \frac{f_1}{f_0}$, hence $\ell \mid t$. Conversely, from $\ell \mid t$ it follows that $\ell \mid \frac{f_2}{f_0}$. By our assumption, $\ell \neq 2, p$, hence ℓ does not divide simultaneously f_1 and t (look at the formula for D_1). Thus we have the desired isogeny. $\square$

2 Covers $\varphi\colon H \to E_a$, $\varphi'\colon H \to E'_a$

Throughout all this section we deal with curves $E_a\colon y^2 = x^3 - ax$ over a finite field $\mathbb{F}_q$ such that $q \equiv 1 \pmod 4$ or, equivalently, $i := \sqrt{-1} \in \mathbb{F}_q$. The formulas of covers represented below are immediately verified in Magma [25].

2.1 Degree $n = 2$

This case is well studied in the literature, but we shortly discuss it for the sake of completeness. There is on E_a the order 4 automorphism $[i]\colon (x, y) \mapsto (-x, iy)$, which is known to generate $\mathrm{Aut}(E_a)$. Regardless of a quadratic non-residue c, obviously,

$$E_a[2] = E_a^c[2] = \{P_0, P_\pm, \mathcal{O}\}, \qquad \text{where} \qquad P_0 := (0, 0), \qquad P_\pm := (\pm\sqrt{a}, 0).$$

Also, note that $[i](P_0) = P_0$ and $[i](P_\pm) = P_\mp$.

If $\sqrt{a} \in \mathbb{F}_q$, that is $E_a[2] \subset E_a(\mathbb{F}_q)$, then we have the $\mathbb{F}_q$-(anti)-isometry

$$\tau\colon E_a[2] \xrightarrow{\sim} E_a^c[2] \qquad P_0 \mapsto P_+, \qquad P_+ \mapsto P_0, \qquad P_- \mapsto P_-.$$

This isometry is irreducible according to [17, Proposition 3], because it is not the restriction of an element from $\mathrm{Aut}(E_a)$. Using the given proposition also in the opposite case, we obtain

Lemma 2. *There is an irreducible $\mathbb{F}_q$-(anti)-isometry $E_a[2] \simeq E'_a[2]$ if and only if $\sqrt{a} \in \mathbb{F}_q$.*

Moreover, after simplifying the formulas of [17, Proposition 4] applied to τ, we get the quadratic $\mathbb{F}_q$-covers

$$\varphi\colon H \to E_a \qquad (x,y) \mapsto \left(\frac{\sqrt{a}(cx^2-2)}{-3cx^2},\ \frac{2\sqrt{a}}{3^2c^2x^3}\cdot y \right),$$

$$\varphi'\colon H \to E_a^c \qquad (x,y) \mapsto \left(\frac{\sqrt{a}(2cx^2-1)}{3},\ \frac{2\sqrt{a}}{3^2c}\cdot y \right)$$

by the genus 2 curve

$$H : y^2 = 3c\sqrt{a}(2c^3x^6 - 3c^2x^4 - 3cx^2 + 2).$$

2.2 Degree $n = 3$

Due to §2.1 hereafter we suppose that $c = a \notin (\mathbb{F}_q^*)^2$. In addition to the Legendre symbol $\left(\frac{x}{q}\right) = x^{(q-1)/2}$ for $x \in \mathbb{F}_q^*$, we will need the 4-th power residue one $\left(\frac{x}{q}\right)_4 := x^{(q-1)/4}$.

Lemma 3. *Under the condition $\sqrt{a} \notin \mathbb{F}_q$ there is an irreducible $\mathbb{F}_q$-anti-isometry $E_a[3] \simeq E'_a[3]$ if and only if $\sqrt{3}, \sqrt{2\sqrt{3}} \in \mathbb{F}_q$.*

Proof. As is known (e.g., from [16, Proposition X.5.4]), among all curves of $j = 1728$ the quadratic twist $E_{a'}$ of E_a (for $a' \in \mathbb{F}_q^*$) is uniquely characterized by the equality $\left(\frac{a'/a}{q}\right)_4 = -1$. Consequently, by virtue of [26, Theorem 1.1] the curves E_a, E'_a are reversely 3-congruent if and only if exists a point $(\lambda : \mu) \in \mathbb{P}^1(\mathbb{F}_q)$ such that $B^+(\lambda,\mu) = 0$ and $\left(\frac{A^-(\lambda,\mu)/c_4}{q}\right)_4 = -1$, where $c_4 := a/27$.

It is readily checked that for $c_6 = 0$ we have

$$A^-(x,y) = -\frac{4}{c_4^3}(x^4 - 6c_4x^2y^2 - 3c_4^2y^4), \qquad B^+(x,y) = 6c_4^2xy(x^4 + 3c_4^2y^4).$$

First, $A^-(0,1) = 12/c_4$ and $A^-(1,0) = -4/c_4^3$. Therefore

$$\left(\frac{A^-(0,1)/c_4}{q}\right)_4 = \left(\frac{12c_4^2}{q}\right)_4 = \left(\frac{4a^2/3}{q}\right)_4, \qquad \left(\frac{A^-(1,0)/c_4}{q}\right)_4 = \left(\frac{-4}{q}\right)_4 = \left(\frac{2i}{q}\right).$$

Since $(i+1)^2 = 2i$, the last symbol equals 1. In turn, $\left(\frac{4a^2/3}{q}\right)_4 = -1$ if and only if $\sqrt{3} \in \mathbb{F}_q$ and $\left(\frac{2a/\sqrt{3}}{q}\right) = \left(\frac{2\sqrt{3}a}{q}\right) = -1$, that is $\sqrt{2\sqrt{3}} \in \mathbb{F}_q$.

Second, let $\lambda^4 = -3c_4^2$, that is $\lambda^2 = \pm i\sqrt{3}c_4$. Then

$$A^-(\lambda,1) = -2^43\omega^k/c_4, \qquad \left(\frac{A^-(\lambda,1)/c_4}{q}\right)_4 = \left(\frac{-3c_4^2}{q}\right)_4,$$

where $1 \leqslant k \leqslant 2$. The symbol $\left(\frac{-3c_4^2}{q}\right)_4 = -1$ if and only if $\sqrt{3} \in \mathbb{F}_q$ and $\left(\frac{i\sqrt{3}c_4}{q}\right) = -1$. However in this case $\lambda \notin \mathbb{F}_q$. Finally, the lemma is proved according to the equivalence 2 $\Leftrightarrow$ 3 of Theorem 1. □

Based on this lemma we find the cubic $\mathbb{F}_q$-covers (where $s := \sqrt{2\sqrt{3}}$)

$$\varphi\colon H \to E_a \qquad (x,y) \mapsto \left(\frac{3(2x^3 - \sqrt{3}ax)}{sa},\ \frac{s(2\sqrt{3}x^2 - a)}{2^2a^2}\cdot y\right),$$
$$\varphi'\colon H \to E_a^a \qquad (x,y) \mapsto \left(\frac{sx^3}{3(\sqrt{3}x^2 - 2a)},\ \frac{x^3 - 2\sqrt{3}ax}{3sa(\sqrt{3}x^2 - 2a)^2}\cdot y\right)$$

by the genus 2 curve

$$H\colon y^2 = 2sa(2\sqrt{3}x^5 - 7ax^3 + 2\sqrt{3}a^2x).$$

Similar formulas are contained in [27, Algorithm 5.4, Appendix A] (even for any pair of elliptic curves glued along their 3-torsion subgroups via an irreducible anti-isometry).

The implication 3 ⇒ 4 of Theorem 1 allowed us to derive our formulas in the same way as in §2.3. In order to save space let us not repeat the intermediate computations. The only difference is that, in contrast to §2.3, the endomorphism $e = [2]$ (up to $\mathrm{Aut}(E_a)$), because $\deg(\widetilde{\varphi}) = \deg(\widetilde{\varphi}') = 12$ and curves E_a do not possess cyclic endomoprhisms of degree 4.

2.3 Degree $n = 4$

Theorem 2. *Under the condition $\sqrt{a} \notin \mathbb{F}_q$ there is always an irreducible $\mathbb{F}_q$-anti-isometry $E_a[4] \simeq E_a'[4]$. Moreover, we have the optimal $\mathbb{F}_q$-covers*

$$\varphi\colon H \to E_a \qquad (x,y) \mapsto \left(\frac{2^4ia^2x}{3(3x^2 - a)^2},\ \frac{2(i-1)a(3^2x^2 + a)}{3^2(3x^2 - a)^3}\cdot y\right),$$
$$\varphi'\colon H \to E_a^a \qquad (x,y) \mapsto \left(\frac{2^4iax^3}{3(x^2 - 3a)^2},\ \frac{2(i-1)(x^3 + 3^2ax)}{3^2(x^2 - 3a)^3}\cdot y\right)$$

by the genus 2 curve

$$H\colon y^2 = 2{\cdot}3a(3^2x^5 - 2{\cdot}7ax^3 + 3^2a^2x).$$

Proof. The existence of an $\mathbb{F}_q$-anti-isometry $\tau\colon E_a[4] \xrightarrow{\sim} E_a'[4]$ stems from [15, Corollary 7.4]. Indeed, the discriminant $D(x^3 - ax) = 2^6a^3 \notin (\mathbb{F}_q^*)^2$. Now let's start to derive (using Magma [25]) the described formulas, thereby showing the irreducibility of some τ. For this purpose one can apply the Fisher approach [28, §3], but we propose a more elegant one, in our view.

The beginning is as in [21, §3], but here we prefer to work at the level of abelian surfaces rather than Kummer ones. First of all, with the help of *Vélu's formulas* [1, 25.1.1] we explicitly write out the $\mathbb{F}_q$-conjugate isogenies $\widehat{\varphi_\pm}\colon E_a \to E_\pm := E_a/P_\pm$ to the elliptic curves

$$E_\pm\colon y^2 = x^3 - 11ax \mp 2{\cdot}7a\sqrt{a}$$

of j-invariant $(2{\cdot}3{\cdot}11)^3$. Note that

$$E_+[2] = \{Q_0^{(0)}, Q_\pm^{(0)}, \mathcal{O}\}, \qquad E_-[2] = \{Q_0^{(1)}, Q_\pm^{(1)}, \mathcal{O}\},$$

where

$$Q_0^{(k)} := \big((-1)^{(k+1)}2\sqrt{a},\ 0\big), \qquad Q_\pm^{(k)} := \big((-1)^k(1 \pm 2\sqrt{2})\sqrt{a},\ 0\big).$$

Again applying Vélu's formulas to $Q_0^{(k)}$, we determine the dual isogenies

$$\varphi_\pm\colon E_\pm \to E_a \qquad (x,y) \mapsto \left(\frac{(x \pm \sqrt{a})^2}{2^2(x \pm 2\sqrt{a})},\ \frac{x^2 \pm 2^2\sqrt{a}x + 3a}{2^3(x \pm 2\sqrt{a})^2} \cdot y \right).$$

Further, making use of [17, Proposition 4] with respect to the irreducible (anti)-isometry

$$\tau\colon E_+[2] \xrightarrow{\sim} E_-[2] \qquad\qquad Q_0^{(0)} \mapsto Q_0^{(1)}, \qquad Q_\pm^{(0)} \mapsto Q_\mp^{(1)},$$

we obtain quadratic covers $\chi'_\pm\colon H' \to E_\pm$. This isometry is π-invariant in the sense of [29, §1] regardless of whether $\sqrt{2} \in \mathbb{F}_q$ or not. Consequently, the genus 2 curve H' is also π-invariant. Thus it is isomorphic to some $\mathbb{F}_q$-curve H by means of the isomorphism $\psi\colon H \xrightarrow{\sim} H'$ from [29, §1] (substitute $\sqrt{a}$ instead of i). After simplifying the formulas of $\chi_\pm := \chi'_\pm \circ \psi$, we get the desired equation of H and the $\mathbb{F}_q$-conjugate covers

$$\chi_\pm\colon H \to E_\pm \qquad (x,y) \mapsto \left(\frac{\mp 2\sqrt{a}(3x^2 \pm 5\sqrt{a}x + 3a)}{3(x \pm \sqrt{a})^2},\ \frac{\mp\sqrt{a}}{3^2(x \pm \sqrt{a})^3} \cdot y \right).$$

Based on the auxiliary $\mathbb{F}_q$-conjugate covers $\theta_\pm := \varphi_\pm \circ \chi_\pm$ of degree 4, we obtain the $\mathbb{F}_q$-morphisms

$$\widetilde{\varphi}\colon H \to E_a \qquad P \mapsto \theta_+(P) + \theta_-(P), \qquad\qquad \widetilde{\varphi}'\colon H \to E_a^a \qquad P \mapsto \sigma\big(\theta_+(P) - \theta_-(P)\big).$$

Using the classical addition-subtraction formulas on elliptic curves (e.g., from [1, §9.1]), we actually get the $\mathbb{F}_q$-covers

$$\widetilde{\varphi}\colon H \to E_a \qquad \begin{cases} X_0 := \dfrac{(3^2x^2 + a)^2(3^2x^4 - 2\cdot 7ax^2 + 3^2a^2)}{2^5 3ax(3x^2 - a)^2}, \\[2ex] Y_0 := \dfrac{(3^6x^8 - 2^2 3^5 ax^6 + 2\cdot 3^5 a^2x^4 - 2^2 7\cdot 13a^3x^2 + 3^2a^4)(3^2x^2 + a)}{2^8 3^2 a^2x^2(3x^2 - a)^3}\cdot y, \end{cases}$$

$$\widetilde{\varphi}'\colon H \to E_a^a \qquad \begin{cases} X_1 := \dfrac{(x^2 + 3^2a)^2(3^2x^4 - 2\cdot 7ax^2 + 3^2a^2)}{2^5\cdot 3x^3(x^2 - 3a)^2}, \\[2ex] Y_1 := \dfrac{(3^2x^8 - 2^2 7\cdot 13ax^6 + 2\cdot 3^5 a^2x^4 - 2^2 3^5 a^3x^2 + 3^6a^4)(x^2 + 3^2a)}{2^8 3^2 ax^5(x^2 - 3a)^3}\cdot y. \end{cases}$$

Moreover, $\deg(\widetilde{\varphi}) = \deg(\widetilde{\varphi}') = \deg(X_k) = 8$. Functions similar to X_0, X_1 are given in [21, §3.1]. There we stop at this stage, however it turns out that $\widetilde{\varphi}$, $\widetilde{\varphi}'$ are not optimal covers. More precisely, below we prove that over $\mathbb{F}_q$ exist elliptic curves E, E', isomorphisms $\eta\colon E \xrightarrow{\sim} E_a$, $\eta'\colon E' \xrightarrow{\sim} E_a^a$, and degree 4 covers $\overline{\varphi}\colon H \to E$, $\overline{\varphi}'\colon H \to E'$ such that

$$\varphi = \eta \circ \overline{\varphi}, \qquad \widetilde{\varphi} = [i] \circ e \circ \varphi, \qquad\qquad \varphi' = \eta' \circ \overline{\varphi}', \qquad \widetilde{\varphi}' = [i] \circ e \circ \varphi'.$$

Here

$$e\colon E_a \to E_a = E_a/P_0 \qquad (x,y) \mapsto \left(\frac{i(x^2 - a)}{2x},\ \frac{(1-i)(x^2 + a)}{(2x)^2} \cdot y \right)$$

is the unique (up to $\mathrm{Aut}(E_a)$) endomorphism on E_a of degree 2. In order not to complicate the notation we equally denote by e the same endomorphism on E'_a.

First of all, there are the decompositions

$$x_0 := \frac{x}{(3x^2-a)^2}, \qquad X_0 = \frac{2^8a^3x_0^2+3^2}{2^5 3ax_0}, \qquad x_1 := \frac{x^3}{(x^2-3a)^2}, \qquad X_1 = \frac{2^8ax_1^2+3^2}{2^5 3x_1}.$$

In order to determine them we make use of the standard Magma function "Decomposition". Unfortunately, it does not work over the function field in a, hence before we substitute in a a large prime and after we check the correctness for general a.

In addition to 0, the remaining 4 roots of the polynomial f (where $H\colon y^2 = f(x)$) are equal to

$$r_\pm := \frac{(\pm i + 2\sqrt{2})\sqrt{a}}{3}, \qquad r'_\pm := \frac{(\pm i - 2\sqrt{2})\sqrt{a}}{3}.$$

It is readily checked that

$$x_0(0) = x_1(0) = 0, \qquad x_0(r_\pm) = x_0(r'_\pm) = \frac{\mp 3i\sqrt{a}}{2^4a^2}, \qquad x_1(r_\pm) = x_1(r'_\pm) = \frac{\pm 3i\sqrt{a}}{2^4a}.$$

Consider the polynomials

$$g_k(x) := x\big(x - x_k(r_+)\big)\big(x - x_k(r_-)\big) = x^3 + \frac{3^2}{2^8a^{3-2k}}x.$$

It turns out that in the function field $\mathbb{F}_q(H)$ there are the square roots of $f_k(x) := 6g_k\big(x_k(x)\big)$, namely

$$\sqrt{f_0(x)} = \frac{3^2x^2+a}{2^4a^2(3x^2-a)^3}\cdot y, \qquad \sqrt{f_1(x)} = \frac{x^3+3^2ax}{2^4a(x^2-3a)^3}\cdot y.$$

As a consequence, $E\colon y^2 = 6g_0(x)$, $E'\colon y^2 = 6g_1(x)$ and the corresponding covers are nothing but

$$\overline{\varphi}\colon H \to E \qquad (x,y) \mapsto \big(x_0(x), \sqrt{f_0(x)}\big), \qquad \overline{\varphi}'\colon H \to E' \qquad (x,y) \mapsto \big(x_1(x), \sqrt{f_1(x)}\big).$$

Composing these covers with the $\mathbb{F}_q$-isomorphisms

$$\eta\colon E \xrightarrow{\sim} E_a \qquad (x,y) \mapsto \left(\frac{2^4ia^2}{3}\cdot x,\ \frac{2^5(i-1)a^3}{3^2}\cdot y\right),$$

$$\eta'\colon E' \xrightarrow{\sim} E_a^a \qquad (x,y) \mapsto \left(\frac{2^4ia}{3}\cdot x,\ \frac{2^5(i-1)a}{3^2}\cdot y\right),$$

we obtain the desired $\mathbb{F}_q$-covers $\varphi\colon H \to E_a$, $\varphi'\colon H \to E_a^a$. This is a computational exercise to show that $\widetilde{\varphi} = [i]\circ e \circ \varphi$ and $\widetilde{\varphi}' = [i]\circ e\circ\varphi'$ as stated above.

It remains to prove the optimality of φ, φ'. The only possible non-trivial decomposition of φ (up to an $\mathbb{F}_q$-isomorphism) has the form $\varphi = e\circ\varphi_2$ for some quadratic $\mathbb{F}_q$-cover $\varphi_2\colon H \to E_a$. For φ_2 there is the quadratic complementary $\mathbb{F}_q$-cover φ_2' whose the construction is explained, e.g., in [15, §2]. It is easy to make sure that φ_2' maps to E_a'. Taking into account §2.1, we come to a contradiction. The same reasoning is equally correct for φ'. Another argument consists of the fact that Magma returned the complete decompositions of X_0, X_1. □

3 Covers $\varphi\colon H \to E_b$, $\varphi'\colon H \to E_b'$

Throughout all this section we deal with curves $E_b\colon y^2 = x^3 + b$ over a finite field $\mathbb{F}_q$ such that $q \equiv 1 \pmod 3$, i.e., $\omega := \sqrt[3]{1} \in \mathbb{F}_q$, $\omega \neq 1$ or, equivalently, $\sqrt{-3} \in \mathbb{F}_q$. The formulas of covers represented below are immediately verified in Magma [25].

3.1 Degree $n = 2$

This case is well studied in the literature, but we shortly discuss it for the sake of completeness. There is on E_b the order 6 automorphism $[-\omega]\colon (x, y) \mapsto (\omega x, -y)$, which is known to generate $\mathrm{Aut}(E_b)$. Regardless of a quadratic non-residue c, obviously,

$$E_b[2] = E_b^c[2] = \{P_k\}_{k=0}^2 \cup \{\mathcal{O}\}, \qquad \text{where} \qquad P_k := \big(-\omega^k \sqrt[3]{b}, 0\big).$$

Also, note that $[-\omega](P_k) = P_{k+1}$.

If $\sqrt[3]{b} \in \mathbb{F}_q$, that is $E_b[2] \subset E_b(\mathbb{F}_q)$, then we have the $\mathbb{F}_q$-(anti)-isometry

$$\tau\colon E_b[2] \xrightarrow{\sim} E_b^c[2] \qquad P_0 \mapsto P_1, \qquad P_1 \mapsto P_0, \qquad P_2 \mapsto P_2.$$

This isometry is irreducible according to [17, Proposition 3], because it is not the restriction of an element from $\mathrm{Aut}(E_b)$. Using the given proposition also in the opposite case, we obtain

Lemma 4. *There is an irreducible $\mathbb{F}_q$-(anti)-isometry $E_b[2] \simeq E_b'[2]$ if and only if $\sqrt[3]{b} \in \mathbb{F}_q$.*

Moreover, after simplifying the formulas of [17, Proposition 4] applied to τ, we get the quadratic $\mathbb{F}_q$-covers

$$\varphi\colon H \to E_b \qquad (x, y) \mapsto \left(\frac{\sqrt[3]{b}}{cx^2}, \ \frac{y}{c^2x^3}\right),$$

$$\varphi'\colon H \to E_b^c \qquad (x, y) \mapsto \left(c\sqrt[3]{b}x^2, \ \frac{y}{c}\right)$$

by the genus 2 curve

$$H\colon y^2 = bc(c^3x^6 + 1).$$

3.2 Degree $n = 5$

The degrees $3, 4$, and > 5 are discussed in §3.3. Due to §3.1 hereafter one can suppose that $\sqrt[3]{b} \notin \mathbb{F}_q$, although we do not use this. In addition to the Legendre symbol $\left(\frac{x}{q}\right) = x^{(q-1)/2}$ for $x \in \mathbb{F}_q^*$, we will need the k-th power residue one $\left(\frac{x}{q}\right)_k := x^{(q-1)/k}$, where $k \in \{3, 6\}$.

Lemma 5. *There is an irreducible $\mathbb{F}_q$-anti-isometry $E_b[5] \simeq E_b'[5]$ if and only if $\sqrt{5} \notin \mathbb{F}_q$ and $\sqrt[3]{b/10} \in \mathbb{F}_q$.*

Proof. As is known (e.g., from [16, Proposition X.5.4]), among all curves of $j = 0$ the quadratic twist $E_{b'}$ of E_b (for $b' \in \mathbb{F}_q^*$) is uniquely characterized by the equality $\left(\frac{b'/b}{q}\right)_6 = -1$. Consequently, by virtue of [30, §13] the curves E_b, E_b' are reversely 5-congruent if and only if exists a point $(\lambda : \mu) \in \mathbb{P}^1(\mathbb{F}_q)$ such that $\mathbf{c}_4(\lambda, \mu) = 0$ and $\left(\frac{\mathbf{c}_6(\lambda,\mu)/c_6}{q}\right)_6 = -1$, where $c_6 := -b/54$. Here $\mathbf{c}_4$, $\mathbf{c}_6$ are the *dual Hesse polynomials* for $n = 5$ from [30, §9].

It is readily checked that for $c_4 = 0$ we have the decomposition

$$\mathbf{c}_4(x, y) = -2^2 5 c_6^{13} xy \cdot Q_0(x^3, y^3) Q_1(x^3, y^3) Q_2(x^3, y^3),$$

where

$$Q_0 := x^2 - 2^6 5 c_6 xy - 2^6 5 c_6^2 y^2, \quad Q_1 := x^2 - 5 c_6 xy + 2^3 5 c_6^2 y^2, \quad Q_2 := x^2 + 2^3 5 c_6 xy + 2^9 5 c_6^2 y^2.$$

First, $\mathbf{c}_6(0, 1) = 2^{30} 5^5 c_6^{29}$ and $\mathbf{c}_6(1, 0) = c_6^{19}$. Therefore

$$\left(\frac{\mathbf{c}_6(0,1)/c_6}{q}\right)_6 = \left(\frac{c_6^4/5}{q}\right)_6, \qquad \left(\frac{\mathbf{c}_6(1,0)/c_6}{q}\right)_6 = 1$$

and hence

$$\left(\frac{\mathbf{c}_6(0,1)/c_6}{q}\right) = \left(\frac{5}{q}\right), \qquad \left(\frac{\mathbf{c}_6(0,1)/c_6}{q}\right)_3 = \left(\frac{c_6/5}{q}\right)_3 = \left(\frac{b/10}{q}\right)_3.$$

Second, the discriminants of the quadratic forms are equal to

$$D(Q_0) = 2^8 3^4 5 c_6^2, \qquad D(Q_1) = -3^3 5 c_6^2, \qquad D(Q_2) = -2^6 3^3 5 c_6^2.$$

As a result, for $y = 1$ their roots are

$$x_{0,\pm} = 2^3(2^2 5 \pm 3^2\sqrt{5})c_6, \qquad x_{1,\pm} = \frac{(5 \pm 3\sqrt{-3}\sqrt{5})c_6}{2}, \qquad x_{2,\pm} = 2^2(-5 \pm 3\sqrt{-3}\sqrt{5})c_6.$$

It is easily shown that

$$\mathbf{c}_6\left(\sqrt[3]{x_{0,\pm}}, 1\right) = -2^{30} 3^{15} 5^5 \alpha_0^2 c_6^{29}, \quad \mathbf{c}_6\left(\sqrt[3]{x_{1,\pm}}, 1\right) = -3^{15} 5^5 \alpha_1^2 c_6^{29}, \quad \mathbf{c}_6\left(\sqrt[3]{x_{2,\pm}}, 1\right) = -2^{30} 3^{15} 5^5 c_6^{29}$$

for some $\alpha_0, \alpha_1 \in \mathbb{F}_q(\sqrt{5})$. No matter the index k, the element $\mathbf{c}_6\left(\sqrt[3]{x_{k,\pm}}, 1\right)/c_6$ is a quadratic residue in $\mathbb{F}_q$ whenever 5 is so. However only in this case $x_{k,\pm} \in \mathbb{F}_q$. Finally, the lemma is proved according to the equivalence 2 ⇔ 3 of Theorem 1. □

Based on this lemma we find the optimal $\mathbb{F}_q$-covers

$$\varphi\colon H \to E_{10} \qquad (x, y) \mapsto \left(\frac{5^2(x^3 - 2^3)}{x^2(2x^3 - 5^2)}, \frac{2^2x^6 - 5{\cdot}11x^3 + 2^4 5^2}{x^3(2x^3 - 5^2)^2}{\cdot}y\right),$$

$$\varphi'\colon H \to E_{10}^5 \qquad (x, y) \mapsto \left(\frac{x^2(2^3x^3 - 5^3)}{5^2(x^3 - 2{\cdot}5)}, \frac{2^4x^6 - 5^2 11x^3 + 2^2 5^4}{5^4(x^3 - 2{\cdot}5)^2}{\cdot}y\right)$$

by the genus 2 curve

$$H\colon y^2 = 5(2x^6 - 3^2 5x^3 + 2{\cdot}5^3).$$

The implication 3 ⇒ 4 of Theorem 1 allowed us to derive these formulas in the same way as in §2.3. In order to save space let us not repeat the intermediate computations. Nevertheless, it is necessary to emphasize that, in contrast to §2.3, in the current situation

$j(E_\pm) \notin \mathbb{F}_q$ and the definition field $\mathbb{F}_q(E_\pm[2]) = \mathbb{F}_{q^6}$ (see details in [22, §1]). So as an irreducible anti-isometry $\tau\colon E_+[2] \xrightarrow{\sim} E_-[2]$ we should take χ from [29, §1]. Besides, the endomorphism $e = [2]$ (up to $\mathrm{Aut}(E_{10})$), because $\deg(\widetilde{\varphi}) = \deg(\widetilde{\varphi}') = 20$ and curves of $j = 0$ do not possess cyclic endomoprhisms of degree 4.

For $B := b/10$ we have the $\mathbb{F}_q$-isomorphisms

$$E_{10} \xrightarrow{\sim} E_b, \qquad E_{10}^5 \xrightarrow{\sim} E_b^5 \qquad (x, y) \mapsto \left(\sqrt[3]{B}\cdot x, \sqrt{B}\cdot y\right)$$

if $\sqrt{B} \in \mathbb{F}_q$ and

$$E_{10} \xrightarrow{\sim} E_b^5 \qquad (x, y) \mapsto \left(\sqrt[3]{B}\cdot x, \sqrt{B/5}\cdot y\right), \qquad\qquad E_{10}^5 \xrightarrow{\sim} E_b \qquad (x, y) \mapsto \left(\sqrt[3]{B}\cdot x, \sqrt{5B}\cdot y\right)$$

otherwise. Correctly composing these isomorphisms with φ, φ', we obtain $\mathbb{F}_q$-covers $H \to E_b$, $H \to E_b^5$ of degree 5 for any b.

3.3 Other degrees n

According to Lemma 1 the condition $n \mid 2t$ is necessary for the existence of an n-congruence between the curves E_b, E_b'. Since q and $\#E_b(\mathbb{F}_q)$ are odd by our assumptions, the trace $t = q + 1 - \#E_b(\mathbb{F}_q)$ is so. Conversely, by virtue of Theorem 1 there is an irreducible $\mathbb{F}_q$-anti-isometry $E_b[\ell] \simeq E_b'[\ell]$ for any prime divisor $\ell \mid t$. Therefore it is enough to consider primes $n = \ell$, because we are interested in n as small as possible. Recall that the discriminant of the Frobenius characteristic polynomial on E_b (and E_b') equals $t^2 - 4q = -3f^2$ for some $f \in \mathbb{N}$ (details see in [2, §4.2.1]). Since $3 \nmid q$ in this article, the case $\ell = 3$ does not arise.

It remains to treat $\ell \geqslant 7$. Unfortunately, for such numbers the *modular curves* $X^-_{E_b}(\ell)$ (from [30, §13], [31, §1.1]) are no longer rational. So we can not provide (similarly to §2.2, §3.2) necessary and sufficient conditions under which E_b, E_b' are reversely ℓ-congruent. Instead, the theory developed in [31, §2.3-2.4] is perhaps useful to extract some information. Besides, we did not find in today's real-world cryptography $\mathbb{F}_q$-curves E_b with a greater trace divisor and without an efficient encoding. Thus we decided to stop at $\ell = 5$.

Formally, all our Magma computations are over fields of characteristic 0 so that the derived formulas of the covers φ, φ' are valid independently of $\mathbb{F}_q$ (except for maybe a finite number of degenerate cases). However the *strong Frey–Mazur conjecture* [28, §1] predicts that at least over the field $\mathbb{Q}$ there is no ℓ-congruent pair E_b, E_b^c no matter $b, c \in \mathbb{Q}$, $\ell > 13$. Hence one may try to construct φ, φ' to some curves E_b, E_b^c only for $\ell \in \{7, 11, 13\}$.

4 Encodings $h\colon \mathbb{P}^1(\mathbb{F}_q) \xrightarrow{\sim} H(\mathbb{F}_q)$ and $\varphi \circ h\colon \mathbb{P}^1(\mathbb{F}_q) \to E(\mathbb{F}_q)$

Note that all genus 2 curves previously encountered in this article are given in the affine $\mathbb{F}_q$-form

$$H\colon y^2 = f(x) := f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + df_4x^2 + d^2f_5x + d^3f_6$$

for some $d \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^2$. Its precise values are contained in Table 1. As usual, H has the smooth completion in the weighted projective plane $\mathbb{P}(1, 2, 1)$ with respect to variables X, Y, Z such that $x = X/Z$, $y = Y/Z^3$. At infinity H contains the points $\mathcal{O}_\pm := (1 : \pm\sqrt{f_6} : 0)$. In compliance with [1, Definition 10.1.11] the equation of H is a ramified model if $f_6 = 0$, a split model if $\sqrt{f_6} \in \mathbb{F}_q^*$, and an inert one otherwise.

§	2.1	2.2	2.3	3.1	3.2
d	$1/c$	a	a	$1/c$	5

Table 1: The values of $d \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^2$

It is readily checked that there are on H the involutions

$$\pm\alpha\colon H \xrightarrow{\sim} H \qquad (X:Y:Z) \mapsto \big(dZ : \pm d\sqrt{d}{\cdot}Y : X\big)$$

or in the affine coordinates:

$$\pm\alpha\colon H \xrightarrow{\sim} H \qquad (x,y) \mapsto \Big(\frac{d}{x},\ \pm\frac{d\sqrt{d}}{x^3}{\cdot}y\Big).$$

In particular, $P_\pm := \big(0, \pm d\sqrt{df_6}\big) \overset{\alpha}{\longleftrightarrow} \mathcal{O}_\pm$. In the case $f_6 = 0$ the points $P_+ = P_-$, $\mathcal{O}_+ = \mathcal{O}_-$ are moreover Weierstrass points on H. Also, it is worth mentioning that the quotients $H/(\pm\alpha)$ are $\mathbb{F}_q$-conjugate elliptic curves. By the way, over algebraically closed fields genus 2 curves with non-hyperelliptic involutions were actively studied, for example, in [32].

Consider any partition $\mathbb{F}_q^* = Y \sqcup -Y$ (e.g., as in [21, §4]) and the modulus analogue

$$\mathbb{F}_q \to Y \sqcup \{0\} \qquad |y| := \begin{cases} y & \text{if} \quad y \in Y \sqcup \{0\}, \\ -y & \text{otherwise.} \end{cases}$$

The involution α enables to construct the encoding

$$h\colon \mathbb{F}_q^* \to H(\mathbb{F}_q) \qquad h(x) := \begin{cases} \big(x,\ \big|\sqrt{f(x)}\big|\big) & \text{if} \quad \sqrt{f(x)} \in \mathbb{F}_q, \\ \left(\dfrac{d}{x},\ -\left|\dfrac{d\sqrt{df(x)}}{x^3}\right|\right) & \text{otherwise, i.e.,}\ \sqrt{df(x)} \in \mathbb{F}_q \end{cases}$$

extended to $\mathbb{P}^1(\mathbb{F}_q)$ as follows:

$$\big(h(0), h(\infty)\big) := \begin{cases} (P_+, \mathcal{O}_+) & \text{if} \quad f_6 = 0, \\ (\mathcal{O}_+, \mathcal{O}_-) & \text{if} \quad \sqrt{f_6} \in \mathbb{F}_q^*, \\ (P_+, P_-) & \text{otherwise, i.e.,}\ \sqrt{df_6} \in \mathbb{F}_q^*. \end{cases}$$

Lemma 6. *The encoding $h\colon \mathbb{P}^1(\mathbb{F}_q) \to H(\mathbb{F}_q)$ is bijective and hence $\#H(\mathbb{F}_q) = q+1$.*

Proof. Obviously, $h(0) \neq h(\infty)$ and $h(\{0,\infty\})$ coincides with the set of all $\mathbb{F}_q$-points among $P_\pm, \mathcal{O}_\pm$ regardless of the model of H. Since $h(\mathbb{F}_q^*) \cap \{P_\pm, \mathcal{O}_\pm\} = \emptyset$, it remains to prove the lemma for h restricted to $\mathbb{F}_q^*$. Further, the first condition in the definition of h also processes non-zero $\mathbb{F}_q$-roots of the polynomial f (if any). Consequently, h gives the bijection between them and Weierstrass $\mathbb{F}_q$-points on H different from P_+, $\mathcal{O}_+$.

Assume that $h(x_0) = h(x_1)$ for some $x_0, x_1 \in \mathbb{F}_q^*$ outside the set of roots of f. If in addition $f(x_0)f(x_1) \in (\mathbb{F}_q^*)^2$, then clearly $x_0 = x_1$. In the opposite case $x_1 = d/x_0$, from the modulus definition it follows the contradiction $f(x_0) = f(x_1) = 0$. Thus the injectivity is proved. To show the surjectivity we need the property $f(d/x)f(x) \notin (\mathbb{F}_q^*)^2$, which stems from the equality $f(d/x) = d^3 f(x)/x^6$ for $x \in \mathbb{F}_q^*$. Then given a point $P = (x, y)$ from $H(\mathbb{F}_q) \setminus \{P_\pm, \mathcal{O}_\pm\}$ it is easily checked that $h^{-1}(P) = x$ if $|y| = y$ and $h^{-1}(P) = d/x$ otherwise. $\square$

As before, denote by $\varphi\colon H \to E$ any $\mathbb{F}_q$-cover of small degree to an elliptic curve E. By analogy with the Kummer surfaces approach [22, §2] and with the case $d = -1$ [29, §2], [8, Algorithm 1] we have the following remark. We decided to omit its detailed consideration, because it would not contain the scientific novelty.

Remark 1. *Whenever* $q \not\equiv 1 \pmod 8$ *a slight modification of the encoding* h *(and hence of* $\varphi \circ h$*) is implemented in constant time of one exponentiation in* $\mathbb{F}_q$.

Finally, by virtue of Lemma 6 and [4, Theorem 7] we obtain

Corollary 1. *The encoding* h *is* 2*-well-distributed (the same is true for* $\varphi \circ h$ *if the cover* φ *is optimal). More formally, let* $\psi_1 := \varphi$, $\psi_2 := \mathrm{id}$*, and* J *be the Jacobian of* H*. Then*

$$\left| \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_k\big((\psi_k \circ h)(x)\big) \right| \leqslant 2\sqrt{q}$$

for any non-trivial characters $\chi_1\colon E(\mathbb{F}_q) \to \mathbb{C}^*$ *and* $\chi_2\colon J(\mathbb{F}_q) \to \mathbb{C}^*$.

Acknowledgements. The author is grateful to Tom Fisher and Yuri Zarhin for answering some of his questions.

References

[1] Galbraith S., *Mathematics of Public Key Cryptography*, Cambridge University Press, New York, 2012.

[2] El Mrabet N., Joye M., *Guide to Pairing-Based Cryptography*, Cryptography and Network Security Series, Chapman and Hall/CRC, New York, 2017.

[3] Faz-Hernandez A. et al., *Hashing to elliptic curves*, https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve, 2021.

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

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

[6] Wahby R., Boneh D., "Fast and simple constant-time hashing to the BLS12-381 elliptic curve", *IACR Transactions on Cryptographic Hardware and Embedded Systems*, **2019**:4, 154–179.

[7] Sakemi Y. et al., *Pairing-friendly curves*, https://datatracker.ietf.org/doc/draft-irtf-cfrg-pairing-friendly-curves, 2021.

[8] Fouque P.-A., Tibouchi M., "Deterministic encoding and hashing to odd hyperelliptic curves", Pairing-Based Cryptography — Pairing 2010, LNCS, **6487**, eds. Joye M., Miyaji A., Otsuka A., Springer, Berlin, Heidelberg, 2010, 265–277.

[9] Fried M., "Global construction of general exceptional covers, with motivation for applications to encoding", Finite Fields: Theory, Applications, and Algorithms, Contemporary Mathematics, **168**, eds. Mullen G., Shiue P., American Mathematical Society, Providence, 1994, 69–100.

[10] Bucur A. et al., "Statistics for traces of cyclic trigonal curves over finite fields", *International Mathematics Research Notices*, **2010**:5 (2010), 932–967.

[11] Icart T., "How to hash into elliptic curves", Advances in Cryptology — CRYPTO 2009, LNCS, **5677**, eds. Halevi S., Springer, Berlin, Heidelberg, 2009, 303–316.

[12] Couveignes J., Kammerer J., "The geometry of flex tangents to a cubic curve and its parameterizations", *Journal of Symbolic Computation*, **47**:3, 266–281.

[13] Fouque P.-A., Joux A., Tibouchi M., "Injective encodings to elliptic curves", Australasian Conference on Information Security and Privacy, LNCS, **7959**, eds. Boyd C., Simpson L., Springer, Berlin, Heidelberg, 2013, 203–218.

[14] Kani E., "The number of curves of genus two with elliptic differentials", *Journal fur die Reine und Angewandte Mathematik*, **485** (1997), 93–122.

[15] Bruin N., Doerksen K., "The arithmetic of genus two curves with $(4,4)$-split Jacobians", *Canadian Journal of Mathematics*, **63**:5, 992–1024.

[16] Silverman J., *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, **106**, Springer, New York, 2009.

[17] Howe E., Leprévost F., Poonen B., "Large torsion subgroups of split Jacobians of curves of genus two or three", *Forum Mathematicum*, **12**:3 (2000), 315–364.

[18] ISO/IEC, *Cryptographic Techniques Based on Elliptic Curves — Part 5: Elliptic Curve Generation (ISO/IEC 15946-5)*, https://www.iso.org/standard/69726.html, 2017.

[19] Trusted Computing Group, *TCG Algorithm Registry*, https://trustedcomputinggroup.org/resource/tcg-algorithm-registry, 2020.

[20] FIDO Alliance, *FIDO ECDAA Algorithm*, https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-ecdaa-algorithm-v2.0-id-20180227.html, 2018.

[21] Koshelev D., "Hashing to elliptic curves of j-invariant 1728", Cryptography and Communications, 2021.

[22] Koshelev D., "Hashing to elliptic curves of $j = 0$ and quadratic imaginary orders of class number 2", https://eprint.iacr.org/2020/969, *Discrete Mathematics and Applications*, 2021.

[23] Satgé P., "Une construction de courbes k-rationnelles sur les surfaces de kummer d'un produit de courbes de genre 1", Rational Points on Algebraic Varieties, Progress in Mathematics, **199**, eds. Peyre E., Tschinkel Y., Birkhäuser, Basel, 2001, 313–334.

[24] Howe E., Nart E., Ritzenthaler C., "Jacobians in isogeny classes of abelian surfaces over finite fields", *Annales de l'Institut Fourier*, **59**:1 (2009), 239–289.

[25] Koshelev D., *Magma code*, https://github.com/dishport/Optimal-encodings-to-elliptic-curves-of-j-invariants-0-1728, 2021.

[26] Fisher T., "On families of 9-congruent elliptic curves", *Acta Arithmetica*, **171**:4 (2015), 371–387.

[27] Bröker R. et al., "Genus-2 curves and Jacobians with a given number of points", *LMS Journal of Computation and Mathematics*, **18**:1 (2015), 170–197.

[28] Fisher T., *On pairs of* 17*-congruent elliptic curves*, https://arxiv.org/abs/2106.02033, 2021.

[29] Koshelev D., *Faster indifferentiable hashing to elliptic* $\mathbb{F}_{q^2}$*-curves*, https://eprint.iacr.org/2021/678, 2021.

[30] Fisher T., "The Hessian of a genus one curve", *Proceedings of the London Mathematical Society*, **104**:3 (2012), 613–648.

[31] Cremona J., Freitas N., "Global methods for the symplectic type of congruences between elliptic curves", *Revista Matemática Iberoamericana*, 2021.

[32] Shaska T., Völklein H., "Elliptic subfields and automorphisms of genus 2 function fields", Algebra, Arithmetic and Geometry with Applications, 2004, 703–723.