Hashing to elliptic curves of $j$-invariant 1728

Koshelev Dmitrii

Versailles Laboratory of Mathematics, Versailles Saint-Quentin-en-Yvelines University
Algebra and Number Theory Laboratory, Institute for Information Transmission Problems
Department of Discrete Mathematics, Moscow Institute of Physics and Technology

Abstract. This article generalizes the simplified Shallue–van de Woestijne–Ulas (SWU) method of a deterministic finite field mapping $\mathbb{F}_q \to E(\mathbb{F}_q)$ to the case of any elliptic $\mathbb{F}_q$-curve $E$ of $j$-invariant 1728. More precisely, we obtain a rational $\mathbb{F}_q$-curve (and its explicit quite simple proper $\mathbb{F}_q$-parametrization) on the Kummer surface $K'$ associated with the direct product $E \times E'$, where $E'$ is the quadratic $\mathbb{F}_q$-twist of $E$.

The simplified SWU method consists in computing the direct image of the parametrization and a subsequent inverse image $(P, P')$ of the natural two-sheeted covering $E \times E' \to K'$. Denoting by $\sigma: E' \cong \to E$ the corresponding $\mathbb{F}_q$-isomorphism, it is easily seen that $P \in E(\mathbb{F}_q)$ or $\sigma(P') \in E(\mathbb{F}_q)$.

Key words: finite fields, pairing-based cryptography, elliptic curves of $j$-invariant 1728, Kummer surfaces, rational curves, Weil restriction, isogenies.

Introduction

Since its invention in the early 2000s, pairing-based cryptography (on an elliptic curve $E: y^2 = f(x)$ over an finite field $\mathbb{F}_q$ of characteristic $p$) has become more and more popular every year, for example in cryptocurrencies. One of the latest reviews of standards, commercial products and libraries for this type of cryptography is given in [42, §5].

Many pairing protocols (and some PAKE ones [13, §8.2.2]) use an efficiently computable mapping $h: \mathbb{F}_q \to E(\mathbb{F}_q)$ (by no means a group homomorphism) often called hashing or encoding. It should not be necessarily injective or surjective, but the bigger image $\text{Im}(h)$ is of course better. Reviews of this topic are represented in [13, Chapter 8], [33]. Certainly, we can just change (e.g. randomly) few bits of a given element $a \in \mathbb{F}_q$ such that $\sqrt{f(a)} \in \mathbb{F}_q$. Although the latter is true for about half $a \in \mathbb{F}_q$ (see, e.g., [13, §8.2.1]), this approach is nevertheless vulnerable to timing attacks [13, §8.2.2]. Another obvious method consists in the scalar multiplication $a \mapsto [a]P$ for some point $P \in E(\mathbb{F}_q)$. Despite its determinateness, it is also insecure [13 §8.1].

There are many safe (at least at first glance) constructions of the desired deterministic hashing such as Boneh–Franklin (bijective) hashing [7, §5.2] for supersingular curves of $j(E) = 0$, Icart hashing [23] for $q \equiv 2 \pmod{3}$, or Elligator 2 [5, §5] provided that $2 \mid \#E(\mathbb{F}_q)$ and $j(E) \neq 1728$. However the unique method valid for arbitrary $E$ and $\mathbb{F}_q$ was proposed in [37] (based on [31 Th. 14.1]) and improved in [33]. Now it is often called in honor of its authors: Shallue, van de Woestijne, and sometimes Ulas.

1Web page: https://www.researchgate.net/profile/Dmitri_Koshelev
Email: dishport@ya.ru
This work was supported by the grant RFBR № 19-31-90020/19
The SWU method consists in parametrizing a (possibly singular) rational $\mathbb{F}_q$-curve $C$ (see, e.g., [31] §4.1) lying on some Calabi–Yau $\mathbb{F}_q$-threefold $T$ (see, e.g., [40]). The latter is a minimal singularity resolution of some generalized Kummer threefold (studied in [11] §4.2, [10] §4, [12] §4.1.1), namely the geometric quotient of $E^3$ under some action of $(\mathbb{Z}/2)^2$. Looking at the definition, we obtain the affine model

$$T: y^2 = f(x_0)f(x_1)f(x_2) \subset \mathbb{A}^4_{(x_0,x_1,x_2,y)},$$

where $(x_i,y_i)$ are three general points of $E$ and $y := y_0y_1y_2$. Having a point $P \in C(\mathbb{F}_q)$, for at least one coordinate $a_i := x_i(P)$ the value $f(a_i)$ is a quadratic residue in $\mathbb{F}_q$. Therefore we get the points $(a_i, \pm \sqrt{f(a_i)}) \in E(\mathbb{F}_q)$.

According to [26] Th. 2] $T$ is not uniruled threefold [11] Ch. 4], but can be represented in the form $(K \times E)/(\mathbb{Z}/2)$ [41], where $K$ is the Kummer surface of $E^2$ (see, e.g., [6] §4). By virtue of the latter and the Bogomolov–Tschinkel theorem [6] Th. 1.1] the surface $K$ and hence threefold $T$ are covered over $\overline{\mathbb{F}_q}$ by rational curves. We stress that over the field $\mathbb{C}$ (unlike a prime characteristic) this would lead to a contradiction.

Also, for a quadratic non-residue $c \in \mathbb{F}_q$ (not necessarily from the image $f(\mathbb{F}_q)$) consider the surface

$$K': y^2 = f(x_0)f(x_1)c \subset \mathbb{A}^3_{(x_0,x_1,y)}.$$  

As you can see, this is the quadratic $\mathbb{F}_q$-twist of $K$, which in itself is the Kummer surface of $E \times E'$, where $E': y^2 = f(x)c$ is the quadratic $\mathbb{F}_q$-twist of $E$.

If in SWU method we take a rational $\mathbb{F}_q$-curve on $K'$ one obtains so-called simplified SWU method [8] §7]. In comparison with (classical) SWU method it allows to avoid 1 quadratic residuosity test in $\mathbb{F}_q$, which is a quite painful operation in cryptography with regard to timing attacks (for details see [13] §8.4.2]).

Nevertheless, despite Bogomolov–Tschinkel theorem finding a rational $\mathbb{F}_q$-curve $C$ on $K'$ (unlike $T$) is not a very simple task. For $j(E) \neq 0, 1728$ a desired curve (even for a larger class of Kummer surfaces) was first constructed in [29] (see also [32], [38] §2]). Interestingly, Articles [28] §1], [29] then use $C$ to prove some arithmetic results over the field $\mathbb{Q}$.

However in pairing-based cryptography ordinary elliptic curves of $j(E) = 0, 1728$ are only interesting [13] Ch. 4]. This is due to the existence of high-degree twists for them, leading to faster pairing computation [13] §3.3]. In [43] §4.3] for some curve $E$ with $j(E) = 0$ over the field $\mathbb{F}_p$ (resp. $\mathbb{F}_{p^2}$) it is proposed to use an ascending $\mathbb{F}_p$-isogeny (resp. $\mathbb{F}_{p^2}$-isogeny) $E \rightarrow E$ of degree 11 (resp. 3) from certain auxiliary elliptic curve $E$ with $j(E) \neq 0, 1728$. Unfortunately, this approach highly depends on $\mathbb{F}_q$, that is in some cases there is no a desired $\mathbb{F}_q$-isogeny of small degree, which could be rapidly computed.

In this work we resolve the problem of constructing a rational $\mathbb{F}_q$-curve $C \subset K'$ for all elliptic $\mathbb{F}_q$-curves $E_a: y^2 = x^3 - ax$ with $j = 1728$. The most famous example of such pairing-friendly curves are Kachisa–Schaefer–Scott (KSS) curves of embedding degree 16 [25] Exam. 4.2], which have become (according to [3], [4], [17]) a popular alternative for those of $j = 0$. We emphasize once again that before us (classical) SWU method, to our knowledge, was the only way to produce a hashing $h: \mathbb{F}_q \rightarrow E_a(\mathbb{F}_q)$ regardless of $\mathbb{F}_q$.

It is worth noting that to derive $C$ we actively use (among other things) the theory of Weil restriction (descent) [18] §8.1] for elliptic curves with respect to the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$. 

2
The cryptographic community knows this operation as an instrument of cryptanalysis \[9, §22.3\].

Interestingly, coefficients of our functions defining a proper parametrization of $C$ are almost entirely some powers of 2 and 3. This allows to compute the corresponding hashing $h: \mathbb{F}_q \to E_a(\mathbb{F}_q)$ very quickly. Finally, let us remark that at worst $h$ is 8:1 map (as the classical SWU one), that is for every point from $E_a(\mathbb{F}_q)$ its inverse image (under $h$) contains at most 8 elements.

The article is organized as follows. In paragraphs \[1] and \[2] we recall basic facts about the Weil restriction of elliptic curves (with respect to $\mathbb{F}_{q^2}/\mathbb{F}_q$) and the Kummer surface for the direct product of two elliptic curves respectively. Next, \[3] is dedicated to the new construction of a (singular) rational $\mathbb{F}_q$-curve on $K'$ for elliptic curves $E_a$ (of $j$-invariant 1728), providing explicit formulas for the hashing $h: \mathbb{F}_q \to E_a(\mathbb{F}_q)$. Finally, in \[4] we make some remarks and conclusions, including the computation of an algebraic complexity for $h$ and the estimation of cardinality for its image.

**Acknowledgements.** The author expresses his deep gratitude to his scientific advisor M. Tsfasman and thanks K. Loginov, K. Shramov for their help and useful comments.

**Contents**

- **Introduction** 1
- **1 The Weil restriction of an elliptic $\mathbb{F}_{q^2}$-curve** 3
- **2 Kummer surfaces** 5
- **3 Constructing a rational $\mathbb{F}_q$-curve on the Kummer surface** 8
  - 3.1 Its proper $\mathbb{F}_q$-parametrization 12
- **4 Remarks and conclusions** 13
- **References** 16

1 **The Weil restriction of an elliptic $\mathbb{F}_{q^2}$-curve**

In this paragraph we freely use some terms from the language of abelian varieties (for details see \[30\]). For a prime $p > 3$ and any its power $q$ consider the finite field extension $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{\gamma})$, where $\gamma \in \mathbb{F}_q$, $\sqrt{\gamma} \notin \mathbb{F}_q$. Besides, for $i \in \{0, 1\}$ consider two elliptic $\mathbb{F}_{q^2}$-curves $E_i$ given by the affine Weierstrass forms

$$E_i: y_i^2 = x_i^3 + a^i x_i + b^i \subset \mathbb{A}^2(x_i, y_i).$$

In other words, $E_i = E_i \sqcup \{P_\infty\} \subset \mathbb{P}^2$, where $P_\infty := (0 : 1 : 0)$. These curves are obviously isogenous by means of the Frobenius maps $\text{Fr}: E_0 \to E_1$, $\text{Fr}: E_1 \to E_0$ over $\mathbb{F}_q$. 

3
Consider the Weil restriction $R_i$ (resp. $\overline{R}_i$) of $E_i$ (resp. $\overline{E}_i$) with respect to $\mathbb{F}_{q^2}/\mathbb{F}_q$ (see, e.g., [18, §8.1]). We stress that $\overline{R}_i \neq R_i \cup \{P_\infty\}$ even over $\mathbb{F}_q$, however we will identify $E_i$ (resp. $R_i$) with $\overline{E}_i$ (resp. $\overline{R}_i$) for simplicity of the notation. Let $A := E_0 \times E_1$ and

\[ a := a_0 + a_1 \sqrt{\gamma}, \quad b := b_0 + b_1 \sqrt{\gamma}, \quad x_0 := u_0 + u_1 \sqrt{\gamma}, \quad y_0 := v_0 + v_1 \sqrt{\gamma}, \]

where $a_0, a_1, b_0, b_1 \in \mathbb{F}_q$. By definition $R_i(\mathbb{F}_q) = E_i(\mathbb{F}_{q^2})$ and

\[
R_i: \begin{cases}
    v_0^2 + \gamma v_1^2 = u_0^3 + 3u_0 u_1^2a_0 + (1)^i u_1 + b_0, \\
    2v_0v_1 = \gamma u_1^3 + 3u_0 u_1 + a_0 u_1 + (1)^i (a_1 u_1 + b_1)
\end{cases} \subset \mathbb{A}^4_{\mathbb{F}_{q^2}(u_0,v_0,u_1,v_1)}.
\]

Although $j$-invariants of the curves $E_0, E_1$ may be different, we always have the involution

\[ s: \mathbb{A}^4 \ni \mathbb{A}^4, \quad (u_0, v_0, u_1, v_1) \mapsto (u_0, v_0, -u_1, -v_1) \]

such that $s: R_0 \ni R_1$ and $s|_{R_0(\mathbb{F}_q)} = \text{Fr}|_{E_0(\mathbb{F}_{q^2})}$. Thus we will also identify $R_0$ with $R_1$, omitting the index. Besides, there is an $\mathbb{F}_{q^2}$-isomorphism

\[ \theta: \mathbb{A}^4_{\mathbb{F}_{q^2}(u_0,v_0,u_1,v_1)} \ni \mathbb{A}^4_{\mathbb{F}_{q^2}(x_0,y_0,x_1,y_1)}, \quad \text{s.t.} \quad \theta: R \ni A \]

given by the matrix

\[
\theta := \begin{pmatrix}
1 & 0 & \sqrt{\gamma} & 0 \\
0 & 1 & 0 & \sqrt{\gamma} \\
1 & 0 & -\sqrt{\gamma} & 0 \\
0 & 1 & 0 & -\sqrt{\gamma}
\end{pmatrix}, \quad \text{where} \quad \theta^{-1} = \frac{1}{2\sqrt{\gamma}} \begin{pmatrix}
\sqrt{\gamma} & 0 & \sqrt{\gamma} & 0 \\
0 & \sqrt{\gamma} & 0 & \sqrt{\gamma} \\
1 & 0 & -1 & 0 \\
0 & 1 & 0 & -1
\end{pmatrix}.
\]

Consider the permutation

\[ s' := \theta \circ s \circ \theta^{-1}: \mathbb{A}^4 \ni \mathbb{A}^4, \quad (x_0, y_0, x_1, y_1) \mapsto (x_1, y_1, x_0, y_0) \]

and the “twisted” Frobenius endomorphism

\[ \pi: \mathbb{A}^4 \rightarrow \mathbb{A}^4, \quad (x_0, y_0, x_1, y_1) \mapsto (x_0^q, y_0^q, x_1^q, y_1^q) \quad \text{s.t.} \quad \pi: A \rightarrow A. \]

It is easily checked that $\theta^{-1} \circ \pi \circ \theta$ is the (usual) Frobenius endomorphism. Thus $\pi$-invariant (hence $\mathbb{F}_{q^2}$-rational) curves $C \subset A$ and maps $\varphi: A \rightarrow \mathbb{A}^4_{\mathbb{F}_{q^2}(x_0,y_0,x_1,y_1)}$ correspond to $\mathbb{F}_q$-ones

\[ \theta^{-1}(C) \subset R, \quad \theta^{-1} \circ \varphi \circ \theta: R \rightarrow \mathbb{A}^4_{\mathbb{F}_{q^2}(u_0,v_0,u_1,v_1)}. \]

This means that

\[ C = s'(C^{(1)}), \quad \varphi = (\varphi_{x_0}, \varphi_{y_0}, \varphi_{x_0}^{(1)} \circ s', \varphi_{y_0}^{(1)} \circ s'), \]

where $C^{(1)}$ is the $\mathbb{F}_q$-conjugate curve to $C$ and $\varphi_{x_0}^{(1)}, \varphi_{y_0}^{(1)}$ are the $\mathbb{F}_q$-conjugate functions to some $\varphi_{x_0}, \varphi_{y_0} \in \mathbb{F}_{q^2}(A)$.  

4
It is also worth noting that on $A$ there are natural involutions $[-1]$ and $[-1]^i \times [-1]^{i+1}$ (for $i \in \{0, 1\}$), which are transformed to $R$ by $\theta$ as

$$(u_0, v_0, u_1, v_1) \mapsto (u_0, -v_0, u_1, -v_1),$$
$$(u_0, v_0, u_1, v_1) \mapsto \left(u_0, (-1)^i \sqrt{\gamma} v_1, u_1, (-1)^i (\sqrt{\gamma})^{-1} v_0\right)$$

respectively.

Hereafter we assume that $a, b \in \mathbb{F}_q$ (i.e., $E := E_0 = E_1$). In this case $s': E^2 \eqsim E^2$. Let $\Delta, \Delta' \subset E^2$ be the diagonal and antidiagonal respectively. Then

$$\theta^{-1}(\Delta) = R \cap \{u_1 = v_1 = 0\} = E, \quad \theta^{-1}(\Delta') = R \cap \{u_1 = v_0 = 0\} = E',$$

where the latter is the quadratic $\mathbb{F}_q$-twist of $E$:

$$E': \gamma y^2 = x^3 + ax + b, \quad \sigma : E' \eqsim E, \quad (x, y) \mapsto (x, \sqrt{\gamma} y).$$

Consider the exact sequences

$$0 \rightarrow E \hookrightarrow R \twoheadrightarrow E' \rightarrow 0, \quad 0 \rightarrow E' \hookrightarrow R \twoheadrightarrow E \rightarrow 0,$$

of $\mathbb{F}_q$-(homo)morphisms, where $\tau := [1] + s, \tau' := [1] - s$. Note that $\tau|_{R(\mathbb{F}_q)}$ is just the trace map on $E$ with respect to $\mathbb{F}_q^2/\mathbb{F}_q$. As a result, we obtain the $\mathbb{F}_q$-rational $(2, 2)$-isogeny

$$\chi := \tau \times \tau': R \rightarrow E \times E' \quad \text{with} \quad \ker(\chi) = E \cap E' = E[2] = E'[2].$$

Finally, the $(2, 2)$-isogenies

$$\psi := \chi \circ \theta^{-1} : E^2 \rightarrow E \times E', \quad \psi = \begin{pmatrix} 1 & 1 \\ \sigma^{-1} & -\sigma^{-1} \end{pmatrix}$$

and $\tilde{\chi} : E \times E' \rightarrow R$ (dual to $\chi$) have the kernels

$$\ker(\psi) = \Delta \cap \Delta' = \Delta[2] = \Delta'[2], \quad \ker(\tilde{\chi}) = \Gamma \cap \Gamma' = \Gamma[2] = \Gamma'[2],$$

where $\Gamma, \Gamma'$ are the graphs of $\sigma$ and $-\sigma = \text{Fr} \circ \sigma \circ \text{Fr}^{-1}$ respectively.

## 2 Kummer surfaces

In this paragraph we handle some concepts of two-dimensional algebraic geometry, which can be found, for example, in [19, Ch. V]. For $i \in \{0, 1\}$ consider any two elliptic $\mathbb{F}_q$-curves $E_i \subset \mathbb{P}^2$ given by the Weierstrass forms

$$E_i : y_i^2 = f_i(x_i) := x_i^3 + a_i x_i + b_i \subset \mathbb{A}_x^2(x_i, y_i)$$

and their direct product

$$A := E_0 \times E_1 \subset \mathbb{A}_x^4(x_0, y_0, x_1, y_1), \quad \overline{A} = \overline{E_0} \times \overline{E_1} \hookrightarrow \mathbb{P}_x^8,$$
where the second map is the Segre embedding. For \(j \in \{0, 1, 2\}\) let \(r_j\) (resp. \(s_j\)) are roots of \(f_0\) (resp. \(f_1\)) and \(P_{r_j} := (r_j, 0)\) (resp. \(P_{s_j} := (s_j, 0)\)) are order 2 points on \(E_0\) (resp. \(E_1\)). Also, let \(\infty := (1 : 0)\) and \(P_{\infty} := (0 : 1 : 0)\). Note that
\[
\overline{A} = A \cup E_0 \times \{P_0\} \cup \{P_\infty\} \times E_1.
\]

Hereafter we will identify \(E_0, E_1, \{P_0\} \times E_1\), and \(A, \overline{A}\).

By definition, the Kummer surface \(K_A\) of \(A\) (see, e.g., [6, §4]) is the minimal singularity resolution \(bl\) of the geometric quotient \(A/[-1]\), which is sometimes called (singular) Kummer surface. In other words, \(bl\) is blowing up 16 nodes, which form the image of \(A[2]\) to \(A/[-1]\). If \(E_0 \cong E_1\), then at least over \(\mathbb{F}_q\) the Kummer surface \(K_A\) is birationally isomorphic to a quartic in \(\mathbb{P}^3\) with 12 nodes. It is so-called desmic surface, which is related to the desmic system of three tetrahedrons (for more details see, e.g., [21, §B.5.2]).

There are also natural models
\[
A/[-1] : y^2 = f_0(x_0)f_1(x_1) \subset \mathbb{A}^3_{(x_0, x_1, y)},
\]
\[
K_A : y_0^2f_1(x_1) = y_1^2f_0(x_0) \subset \mathbb{A}^2_{(x_0, x_1)} \times \mathbb{P}^1_{(y_0 : y_1)}
\]
and the two-sheeted maps
\[
\rho : A \rightarrow A/[-1], \quad (x_0, y_0, x_1, y_1) \mapsto (x_0, x_1, y_0y_1),
\]
\[
\rho' : A \rightarrow K_A, \quad (x_0, y_0, x_1, y_1) \mapsto ((x_0, x_1), (y_0 : y_1)).
\]

Therefore blowing up and blowing down maps have the form
\[
bl = \rho \circ (\rho')^{-1} : K_A \rightarrow A/[-1], \quad ((x_0, x_1), (y_0 : y_1)) \mapsto (x_0, x_1, f_1(x_1) \frac{y_0}{y_1}) = (x_0, x_1, f_0(x_0) \frac{y_1}{y_0}),
\]
\[
bl^{-1} = \rho' \circ \rho^{-1} : A/[-1] \rightarrow K_A, \quad (x_0, x_1, y) \mapsto ((x_0, x_1), (y : f_1(x_1))) = (x_0, x_1, (f_0(x_0) : y))
\]
respectively. Further, the involutions \([1] \times [-1], [-1] \times [1]\) on \(A\) are induced to \(A/[-1]\) as \((x_0, x_1, y) \mapsto (x_0, x_1, -y)\). The quotient of \(A/[-1]\) under this new involution is \(\mathbb{P}^1 \times \mathbb{P}^1\) and the corresponding natural map is denoted by \(pr\). In simple words, it is the projection to the coordinates \(x_0, x_1\).

For \(r \in \{r_0, r_1, r_2, \infty\}, s \in \{s_0, s_1, s_2, \infty\}\) let
\[
L_r := \rho(P_r) \times E_1, \quad M_s := \rho(E_0 \times \{P_s\})
\]
and \(E_{r,s}\) be the exceptional \((-2)\)-curve on \(K_A\) corresponding to the point \(\rho(P_r, P_s)\). For \(r, s \neq \infty\) it is easily seen that
\[
L_r = \{x_0 = r, y = 0\}, \quad M_s = \{x_1 = s, y = 0\}, \quad E_{r,s} = \{x_0 = r, x_1 = s\}.
\]

Since \(Ram := \bigsqcup_{r,s} (L_r \cup M_s)\) is exactly the ramification locus of \(pr\), we will identify the lines \(L_r, pr(L_r)\) and \(M_s, pr(M_s)\). Note that
\[
\overline{A}/[-1] = A/[-1] \cup L_\infty \cup M_\infty, \quad \mathbb{P}^1 \times \mathbb{P}^1 = \mathbb{A}^2_{(x_0, x_1)} \cup L_\infty \cup M_\infty.
\]
It is well known that $K_A$ is a K3 surface \[22\], i.e., its canonical class and the first cohomology space $H^1(K_A, \mathcal{O}_{K_A})$ of the structure sheaf $\mathcal{O}_{K_A}$ are zero. According to \[39\], §2.8.4, \[22\] Ch. 17 we have:

$$\text{NS}(A) \simeq \mathbb{Z}[E_0, E_1] \oplus \text{Hom}(E_0, E_1) \quad \text{NS}(K_A) \simeq \text{Pic}(K_A) \simeq \text{NS}(A) \oplus \mathbb{Z}[[E_{r,s}]]^{Fr}$$

In particular, ranks of these free groups (i.e., Picard $\mathbb{F}_q$-numbers) satisfy the inequalities

$$2 \leq \rho(A) \leq 6, \quad 8 \leq \rho(K_A) \leq 22$$

If $\rho(A) = 2$, then the curves $E_0, E_1$ are not isogenous over $\mathbb{F}_q$. At the same time, from $\rho(A) = 6$ follows that $E_0, E_1$ are supersingular and the surface $K_A$ is geometrically unirational.

For an absolutely irreducible (possibly singular) $\mathbb{F}_q$-curve $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ (s.t. $C \not\subset \text{Ram}$) we denote by $r_C$ the count of branches $B$ \[20\], §4.3 on $C$ such that the intersection number $I_P(B, \text{Ram})$ is odd, where $P$ is the centre of $B$. In other words, denoting by $\nu: \mathbb{F}_q(C) \to \mathbb{Z}$ the discrete valuation \[32\] §1 corresponding to $B$, we get

$$I_P(B, \text{Ram}) = \begin{cases} 
\nu(f_0(x_0)f_1(x_1)) & \text{if } P \in \mathbb{A}^2_{(x_0, x_1)}, \\
\nu(1/(x_0x_1)) & \text{if } P \in L_\infty \cup M_\infty.
\end{cases}$$

**Theorem 1** (\[32\] Prop. 1.2.3). Suppose that $C$ is a rational curve. Let $D := \text{pr}^{-1}(C)$ and $k$ be one of the fields $\mathbb{F}_q, \mathbb{F}_q^2$.

1. If $r_C = 0$, then $D$ consists of two absolutely irreducible rational curves $D_0, D_1$ defined at most over $\mathbb{F}_q^2$. Moreover, $D$ is reducible over $k$ if and only if $y = \sqrt{f_0(x_0)f_1(x_1)} \in k(C)$. In this case $\text{pr}_D: D_0 \to C$, $\text{pr}_D: D_1 \to C$ are birational $k$-morphisms.

2. If $r_C > 0$, then $D$ is an absolutely irreducible (possibly singular) $\mathbb{F}_q$-curve of geometric genus $r_C/2 - 1$ (in particular, $2 \mid r_C$). Moreover, for $r_C > 2$ the curve $D$ is hyperelliptic.

**Theorem 2** (\[6\] Lem. 4.1, \[32\] §2.1).

1. A curve $D \subset A/[−1]$ is rational if and only if $H := \rho^{-1}(D) \subset A$ is a (possibly singular) hyperelliptic curve such that the hyperelliptic involution on $H$ is the restriction of $[−1]$.

2. Moreover, if the image $C := \text{pr}(D)$ is of bidegree $(1, 1)$ and $r_C = 2$, then geometric genus $g(H) = 2$ and $H$ also has a non-hyperelliptic involution $i$ such that $H/−i = E_0, H/−i = E_1$ (such hyperelliptic curves are studied in detail, e.g., in \[10\]).

Suppose that $E_0, E_1$ are $\mathbb{F}_q$-conjugate elliptic $\mathbb{F}_q$-curves as in §1 (hence we will use its notation). Let $K_R$ be the Kummer surface of the Weil restriction $R$ and


It can be checked that $Q$ is the Weil restriction of $\mathbb{P}^1$ with respect to $\mathbb{F}_q^2/\mathbb{F}_q$, which is also the unique (up to a change of variables) quadratic surface in $\mathbb{P}^3$ without $\mathbb{F}_q$-lines \[18\] Exer.
8.1.6.iii]. Looking at the transformation $\theta: R \Rightarrow A$, we see that in affine coordinates the natural two-sheeted maps have the form

$$\begin{align*}
\rho: R &\rightarrow R/[-1], \\
\rho &\downarrow \\
R/[-1] &\rightarrow A/[-1],
\end{align*}$$

and

$$\begin{align*}
pr: R/[-1] &\rightarrow Q, \\
pr &\downarrow \\
Q &\rightarrow \mathbb{P}^1 \times \mathbb{P}^1.
\end{align*}$$

Finally, denote by $\overline{\theta}$ isomorphisms over $\mathbb{F}_q^2$ that are the restrictions of $\theta$ to $R/[-1]$ and $Q$ respectively. Thus we obtain the commutative diagram

$$
\begin{array}{ccc}
R & \overset{\theta}{\Rightarrow} & A \\
\rho \downarrow & & \downarrow \rho \\
R/[-1] & \overset{\overline{\theta}}{\Rightarrow} & A/[-1] \\
pr \downarrow & & \downarrow pr \\
Q & \overset{\overline{\theta}}{\Rightarrow} & \mathbb{P}^1 \times \mathbb{P}^1 \\
\end{array}
$$

3 Constructing a rational $\mathbb{F}_q$-curve on the Kummer surface

We will often use notation and results from §1-2. Consider a finite field $\mathbb{F}_q$ of characteristic $p > 3$. We are interested in elliptic $\mathbb{F}_q$-curves $E_a$: $y^2 = f(x) := x^3 - ax$ of $j$-invariant 1728. According to [36, Exam. V.4.5] they are ordinary if and only if $p \equiv 1 \pmod{4}$, i.e., $\sqrt{-1} \in \mathbb{F}_q$. For definiteness we will suppose this condition, because for pairing-based cryptography supersingular curves are insecure at the moment.

Any two $\mathbb{F}_q$-curves of $j = 1728$ are isomorphic (at most over $\mathbb{F}_q^4$) by the map

$$E_a \cong E_{a'}, \quad (x, y) \mapsto (\sqrt[3]{a}x, \sqrt[3]{a}y),$$

where $\alpha := a'/a$. Therefore provided that $\sqrt{a} \notin \mathbb{F}_q$ (hence $\sqrt[3]{a} \notin \mathbb{F}_q^2$) the curves $E_{a_i}$ (for $i \in \mathbb{Z}/4$) are unique ones (up to $\mathbb{F}_q$-isomorphism) of $j = 1728$. For $E_1, E_a$ there are the quadratic $\mathbb{F}_q$-twists

$$E'_1: ay^2 = x^3 - x, \quad E'_a: ay^2 = x^3 - ax$$

and the corresponding $\mathbb{F}_q^2$-isomorphisms $\sigma: E'_1 \cong E_1$, $\sigma: E'_a \cong E_a$. It is obvious that

$$E'_1 \cong E_{a^2}, \quad E'_a \cong E_{a^3}, \quad (x, y) \mapsto (ax, a^2y).$$

The curves $E_{a^i}$ are pairwise non-isogenous over $\mathbb{F}_q$ [13 Prop. 2.5]. Hence, in particular, the Picard $\mathbb{F}_q$-numbers are equal to

$$\rho(K_{E_1 \times E'_1}) = 18, \quad \rho(K_{E_a \times E'_a}) = 12.$$

In this paragraph we focus on constructing a rational $\mathbb{F}_q$-curve only on the Kummer surface $K_{E_1 \times E'_1}$, because this is more difficult than analogous task for $K_{E_1 \times E'_1}$.
Obviously,

\[ E_a[2] = E'_a[2] = \{ P_0, P_{\pm}, P_{\infty} \}, \quad P_0 := (0,0), \quad P_{\pm} := (\pm \sqrt{a}, 0). \]

According to the Vélu formulas [15 §25.1.1] we obtain:

\[ E_a/P_0 \simeq_{E_i} E_a, \quad E_{\pm} := E_a/P_{\pm}, \quad y^2 = x^3 - 11ax \mp 14a\sqrt{a}, \]

where \( j(E_{\pm}) = 287496 \), and the corresponding vertical dual to each other 2-isogenies

\[ \widehat{\varphi}_{\pm}: E_a \to E_{\pm}, \quad \varphi_{\pm}: E_{\pm} \to E_a \]

have the form

\[ \widehat{\varphi}_{\pm} = \begin{cases} x := x + \frac{2a}{x \mp \sqrt{a}}, \\ y := \left(1 - \frac{2a}{(x \mp \sqrt{a})^2}\right)y, \end{cases} \quad \varphi_{\pm} = \begin{cases} x := \left(x + \frac{a}{x \pm 2\sqrt{a}}\right)/4, \\ y := \left(1 - \frac{a}{(x \pm 2\sqrt{a})^2}\right)y/8. \end{cases} \]

For compactness we will often use the value \( \alpha_{\pm} := 1 \pm 2\sqrt{2} \). Note that

\[ E_+[2] = \{ Q_0^{(0)}, Q_{\pm}^{(0)}, P_{\infty} \}, \quad E_-[2] = \{ Q_0^{(1)}, Q_{\pm}^{(1)}, P_{\infty} \}, \]

where

\[ Q_0^{(i)} := ((-1)^{(i+1)}2\sqrt{a}, 0), \quad Q_{\pm}^{(i)} := ((-1)^i\alpha_{\pm}\sqrt{a}, 0). \]

Clearly,

\[ \widehat{\varphi}_+(P_0) = \widehat{\varphi}_-(P_-) = Q_0^{(0)}, \quad \varphi_+(Q_{\pm}^{(0)}) = P_+, \]

\[ \widehat{\varphi}_-(P_0) = \widehat{\varphi}_+(P_+) = Q_0^{(1)}, \quad \varphi_-(Q_{\pm}^{(1)}) = P_- \]

and hence

\[ E_a = E_+/Q_0^{(0)} = E_-/Q_0^{(1)}. \]

Finally, letting

\[ A_{\pm} := E_+ \times E_- , \quad A_a := E_a \times E_a , \quad A'_a := E_a \times E'_a , \]

consider the dual to each other (2, 2)-isogenies

\[ \widehat{\varphi} := \widehat{\varphi}_+ \times \widehat{\varphi}_- : A_a \to A_{\pm}, \quad \varphi := \varphi_+ \times \varphi_- : A_{\pm} \to A_a, \]

which are \( \pi \)-invariant.

Next, let

\[ \varphi := \rho \circ \varphi \circ \rho^{-1} : A_{\pm}/[-1] \to A_a/[-1], \quad \overline{\psi} := \rho \circ \psi \circ \rho^{-1} : A_a/[-1] \to A'_a/[1], \]

\[ \overline{\varphi} := pr \circ \overline{\varphi} \circ pr^{-1} : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1 \times \mathbb{P}^1 , \quad \overline{\psi} := pr \circ \overline{\psi} : A_a/[1] \to \mathbb{P}^1 \times \mathbb{P}^1 , \]
where ψ is taken from §1. These maps form a commutative diagram represented in Figure 4. Note that ψ does not descend to any map \(\mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^1 \times \mathbb{P}^1\). Looking at the formulas of the isogeny \(\varphi\), we obtain:

\[
\begin{align*}
\varphi &= \left\{ 
\begin{array}{l}
x_0 := \left(x_0 + \frac{a}{x_0 + 2\sqrt{a}}\right)/4, \\
x_1 := \left(x_1 + \frac{a}{x_1 - 2\sqrt{a}}\right)/4, \\
y := \left(1 - \frac{a}{(x_0 + 2\sqrt{a})^2}\right)
\left(1 - \frac{a}{(x_1 - 2\sqrt{a})^2}\right)y/64.
\end{array}
\right.
\end{align*}
\]

At the same time, using the famous formulas of addition and subtraction on elliptic curves (see, e.g., [15, §9.1]) yields:

\[
\psi = \left\{ 
\begin{array}{l}
x_0 = \frac{x_0^2x_1 + x_0x_1^2 - a(x_0 + x_1) - 2y}{(x_0 - x_1)^2}, \\
x_1 = \frac{x_0^2x_1 + x_0x_1^2 - a(x_0 + x_1) + 2y}{(x_0 - x_1)^2}.
\end{array}
\right.
\]

Below we will often use the computer algebra system Magma to produce equations or formulas and check theoretical facts (see the corresponding code in [27]). Consider on \(\mathbb{A}^2_{(x_0,x_1)} \subset \mathbb{P}^1 \times \mathbb{P}^1\) the \(\pi\)-invariant conic

\[
C_1: 6x_0x_1 - 11\sqrt{a}x_0 + 11\sqrt{a}x_1 - 20a,
\]

which is unique bidegree \((1,1)\) curve (see Figure 1) passing through the points

\((−2\sqrt{a}, 2\sqrt{a}), (\alpha_+\sqrt{a}, −\alpha_-\sqrt{a}), (\alpha_-\sqrt{a}, −\alpha_+\sqrt{a})\).

Using Magma, one can compute the defining polynomial of \(C_2 := \varphi(C_1)\), namely

\[
C_2: 24x_0^2x_1 + 25\sqrt{a}x_0^2 - 24x_0x_1^2 - 62\sqrt{a}x_0x_1 - 40ax_0 + 25\sqrt{a}x_1^2 + 40ax_1 + 16\sqrt{a}.
\]

This is a \(\pi\)-invariant cubic (of bidegree \((2,2)\)) having the node \((\sqrt{a},−\sqrt{a})\) (see Figure 2). Note that \(r_{C_1} = r_{C_2} = 2\), hence by Theorem 1 the \(\pi\)-invariant curves

\[
D_1 := \text{pr}^{-1}(C_1) \subset A/[-1], \quad D_2 := \text{pr}^{-1}(C_2) = \varphi(D_1) \subset A_a/[-1]
\]

are rational. It turns out that the restriction \(\varphi: C_1 \rightarrow C_2\) (and hence \(\varphi: D_1 \rightarrow D_2\)) is invertible. Indeed,

\[
(\varphi)^{-1}: C_2 \longrightarrow C_1, \quad (\varphi)^{-1} = \left\{ 
\begin{array}{l}
x_0 := \frac{24x_0^2 - 24x_0x_1 - 49\sqrt{a}x_0 + 25\sqrt{a}x_1 + 26a}{6(x_0 - \sqrt{a})}, \\
x_1 := \frac{11\sqrt{a}x_0 + \sqrt{a}x_1 - 10a}{6(x_0 - \sqrt{a})}.
\end{array}
\right.
\]

Finally, denote by \(C_2^{(1)}\) (resp. \(D_2^{(1)} = \text{pr}^{-1}(C_2^{(1)})\)) the curve \(\mathbb{F}_q\)-conjugate to \(C_2\) (resp. \(D_2\).
Again, by means of Magma we get the image \( C_8 := \psi(D_2) = \psi(D_2^{(1)}) \) (see Figure 3) given by the symmetric \( \mathbb{F}_q \)-polynomial

\[
C_8: 5764801a^3s_1^6s_2^1 - 921984a^2s_1^6s_2^2 + 3471884416a^3s_1^6s_2^1s_3^2 + 6914880000a^4s_1^6 + 36864as_1^4s_2^4 - \\
6463336448a^2s_1^4s_2^3 + 216401113088a^3s_1^4s_2^3s_3^2 - 1634869760000a^4s_1^4s_2^2 + 207360000000a^5s_1^4 + \\
966524928as_1^2s_2^5 - 38111311616a^2s_1^2s_2^4s_3^4 - 941125009408a^3s_1^2s_2^4s_3^3 + 1018019840000a^4s_1^2s_2^2 + \\
1474560000000a^5s_1^2s_2^2 - 37748736s_2^7 + 1124073472as_2^6 - 56463720448a^2s_2^5 + \\
757642297344a^3s_2^4 - 1592005120000a^4s_2^3 + 2621440000000a^5s_2^2,
\]

where \( s_1 := x_0 + x_1, \ s_2 := x_0x_1 \) are the elementary symmetric polynomials. Note that \( \text{bideg}(C_8) = (8, 8) \). Since \( r_{C_8} = 0 \) it follows from Theorem 1 that the inverse image \( \text{pr}^{-1}(C_8) \) consists of two different rational curves \( D_8 := \psi(D_2) \) and \( D_8' := \psi(D_2^{(1)}) \) such that the restrictions \( \text{pr}: D_8 \to C_8, \text{pr}: D_8' \to C_8 \) are birational. Moreover, \( D_8, D_8' \) are defined over the field \( \mathbb{F}_q \), since \( D_2, D_2^{(1)} \) are \( \pi \)-invariant (for better comprehension see §1). Further, according to the Magma computation we obtain

**Lemma 1.**

1. The curve \( C_8 \subset \mathbb{P}^1 \times \mathbb{P}^1 \) has exactly 42 singular points, where \((0, 0), (\infty, \infty)\) are unique ones from the ramification locus \( \text{Ram} \).

2. The point \((0, 0)\) is a non-ordinary singularity of multiplicity 4 with two different tangents (each one of multiplicity 2).

3. The point \((\infty, \infty)\) is a node, whose tangents are the lines \( L_{\infty}, M_{\infty} \). Moreover, this point is an inflexion one with respect to each of the two local branches.

Figure 1: The curve \( C_1 \) \hspace{1cm} Figure 2: The curve \( C_2 \) \hspace{1cm} Figure 3: The curve \( C_8 \)

Dotted arrows denote the action of the endomorphism \( \pi \): blue ones if \( \sqrt{2} \in \mathbb{F}_q \), violet ones if \( \sqrt{2} / \in \mathbb{F}_q \), and red ones in both cases. Also, the green lines are two tangents to \( C_8 \) at \((0, 0)\).
Substituting the last formulas in the equation of $\varphi$,

$$A_{\pm} \xrightarrow{\varphi} A_a \xrightarrow{\psi} A_a' \quad \text{where} \quad i$$

Thus there are birational isomorphisms

$$H_1 \xrightarrow{\varphi} H_2 \xrightarrow{\psi} H_8$$

Further, Magma allows to compute the anticanonical map from $D_1$ to $D_8$

By Theorem 2 the inverse images

$$H_i := \rho^{-1}(D_i), \quad H^{(1)}_2 := \rho^{-1}(D^{(1)}_2), \quad H'_8 := \rho^{-1}(D'_8),$$

where $i \in \{1, 2, 8\}$, are hyperelliptic curves. Note that the maps

$$\varphi: H_1 \to H_2, \quad \psi: H_2 \to H_8, \quad \psi: H^{(1)}_2 \to H'_8$$

are birational and hence all these curves have geometric genus 2 and a non-hyperelliptic involution. We now have everything to represent Figure 5.

### 3.1 Its proper $\mathbb{F}_q$-parametrization

Now we are going to parametrize the curve $C_8$. Note that $C_1$ has the $\pi$-invariant point $(-5/3\sqrt{a}, 5/3\sqrt{a})$ and the projection from it gives:

$$pr_{C_1}: C_1 \sim \to \mathbb{A}^1_x, \quad x := \frac{3\sqrt{a}(x_0 + x_1)}{3(x_0 - x_1) + 10\sqrt{a}} \quad \text{s.t.} \quad pr_{C_1}^{-1}: \mathbb{A}^1_x \sim \to C_1,$$

Substituting the last formulas in the equation of $A_{\pm}/[-1]$, we obtain the $\mathbb{F}_q$-curve

$$D'_1: \frac{2^6 a^3 u^2 + 3^6 v^2 - 2^6 a^4}{3^6(a^2 - u^2)} \quad \subset \quad \mathbb{A}^2_{(u,v)}.$$}

Thus there are birational isomorphisms

$$\chi := pr_{C_1} \times \text{id}_y: D_1 \sim \to D'_1, \quad \chi^{-1} = pr_{C_1}^{-1} \times \text{id}_y: D'_1 \sim \to D_1.$$}

Further, Magma allows to compute the anticanonical map from $D'_1$ to the $\mathbb{F}_q$-conic

$$Q: \frac{2^6 a^3 u^2 + 3^6 v^2 - 2^6 a^4}{3^6(a^2 - u^2)} \quad \subset \quad \mathbb{A}^2_{(u,v)}$$

given by the $\mathbb{F}_q$-formulas

$$\varphi_{-K}: D'_1 \sim \to Q,$$

$$\varphi_{-K}^{-1}: Q \sim \to D'_1,$$

$$\begin{cases} u := x, \\ v := \frac{2^3 a^3(3^2 a - 2^3 x^2)x}{3^6(x^2 - a)y} \end{cases} \quad \text{s.t.} \quad \begin{cases} x := u, \\ y := \frac{(2^3 u^2 - 3^2 a)uv}{2^3(u^2 - a)^2} \end{cases}$$
Finally, the projection from the point \((2^3 a^2 / 3^3, 0) \in Q(\mathbb{F}_q)\) has the form

\[
pr_Q : Q \cong \mathbb{A}^1, \quad t := \frac{3^3 v - 2^4 a^2}{3^3 u} \quad \text{s.t.} \quad pr_Q^{-1} : \mathbb{A}^1 \cong Q, \quad \left\{ \begin{array}{l}
u := -\frac{2^4 3^3 a^2 t}{2^6 a^3 + 3^6 t^2}, \\
v := \frac{2^3 a^2 (2^6 a^3 - 3^6 t^2)}{3^3 (2^6 a^3 + 3^6 t^2)}.
\end{array} \right.
\]

Thus we obtain the \(\mathbb{F}_q\)-rational map

\[
par := \overline{\psi} \circ \varphi \circ \chi^{-1} \circ \varphi^{-1}_K \circ pr_Q^{-1} : \mathbb{A}^1 \cong C_8
\]
given by the functions

\[
par = \left\{ \begin{array}{l}
x_0 := \frac{(3^8 t^2 + 2^6 a^3)^2 g(t)}{2^{14} 3^2 a^4 (3^4 t^2 - 2^6 a^3) t^2}, \\
x_1 := \frac{(3^4 t^2 + 2^6 a^3)^2 g(t)}{2^8 3^6 a (3^4 t^2 - 2^6 a^3) t^2},
\end{array} \right. \quad \text{where} \quad g(t) := t^2 (3^{12} t^2 - 2^7 3^4 a^3) + 2^{12} a^6.
\]

It is easily seen that \(g(t)\) has no multiple roots and the functions are in the reduced form, that is the numerators and denominators have no common roots. By [34, Th. 4.21] we get

**Theorem 3.** The map \(par\) (or, equivalently, \(\overline{\psi}_{|_{D_2}}\)) is birational.

Another proof consists in applying the projection formula \([11, \S 1.2]\) with respect to \(\overline{\psi}\). Interestingly, according to [34, Cor. 6.14] the curve \(C_8\) is not polynomial, i.e., it cannot be parametrized by two polynomials (even over \(\mathbb{F}_q\)). Finally, the inverse map \(par^{-1} : C_8 \cong \mathbb{A}^1\) and the maps \(pr^{-1} \circ par : \mathbb{A}^1 \cong D_8, D_8'\) (or, equivalently, the functions \(\pm \sqrt{af(x_0)fg(x_1)} \in \mathbb{F}_q(t)\)) can be also computed, but we do not write out them here in the sake of compactness (as above, see the Magma code [27]).

### 4 Remarks and conclusions

Let us keep a notation of previous paragraphs. First of all, we would like to deal with the case \(\sqrt{a} \in \mathbb{F}_q\) (in fact, it is sufficient to take \(a = 1\)). Let \(E'_-, E'_a\) be the quadratic \(\mathbb{F}_q\)-twists of \(E'_-, E_a\) respectively (by the \(\mathbb{F}_q\)-isomorphism \(\sigma\)) and

\[
A'_\pm := E'_- \times E'_-, \quad A'_a := E'_a \times E'_a.
\]

By means of

\[
[1] \times \sigma : A'_\pm \Rightarrow A_\pm, \quad [1] \times \sigma : A'_a \Rightarrow A_a
\]

the morphisms \(\varphi, \overline{\varphi}\) are identically transformed to

\[
A'_\pm \to A'_a, \quad A'_\pm /[-1] \to A'_a /[-1]
\]

respectively, hence we save the notation. Finally, for \(i \in \{1, 2\}\) consider the \(\mathbb{F}_q\)-curves

\[
H'_i := ([1] \times \sigma^{-1})(H_i), \quad D'_i := \rho(H'_i) = pr^{-1}(C_i).
\]

13
Thus $D'_2 = \varphi(D'_1)$ is a desired rational $\mathbb{F}_q$-curve on the Kummer surface of $A'_a$ and we obtain the commutative diagrams

$$
\begin{array}{ccc}
A'_\pm & \xrightarrow{\varphi} & A'_a \\
\rho \downarrow & & \downarrow \rho \\
A'_\pm/[{-1}] & \xrightarrow{\varphi} & A'_a/[{-1}] \\
pr \downarrow & & \downarrow pr \\
\mathbb{P}^1 \times \mathbb{P}^1 & \xrightarrow{\varphi} & \mathbb{P}^1 \times \mathbb{P}^1 \\
\end{array}
\quad
H'_1 & \xrightarrow{\varphi} & H'_2 \\
\rho \downarrow & & \downarrow \rho \\
D'_1 & \xrightarrow{\varphi} & D'_2 \\
pr \downarrow & & \downarrow pr \\
C_1 & \xrightarrow{\varphi} & C_2
\end{array}
$$

Now we return to the more interesting case $\sqrt{a} \notin \mathbb{F}_q$. In particular, under the condition $q \equiv 5 \pmod{8}$ it is sufficient to take $a \in \{2, 8\}$, because it is known that the Legendre symbol

$$
\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = \begin{cases} 
1 & \text{if } p \equiv 1, 7 \pmod{8}, \\
-1 & \text{if } p \equiv 3, 5 \pmod{8},
\end{cases}
$$

and the simplified SWU method can be implemented quite efficiently.

Fortunately, for $q \equiv 1 \pmod{8}$ a square root in $\mathbb{F}_q$ can be computed by means of one exponentiation in $\mathbb{F}_q$ (see, e.g., [13, §5.1.7]), hence the simplified SWU method can be implemented quite efficiently.

It is time to clarify which sign of the square root $y = \sqrt{r}$ (for a quadratic residue $r \in \mathbb{F}_q^*$) should be chosen by default. Let $\mathbb{F}_q = \mathbb{F}_p(\gamma)$ and $y = \sum_{i=0}^{n-1} y_i \gamma^i \in \mathbb{F}_q^*$, where $0 \leq y_i < p$. If $i_0$ is the minimal index with $y_{i_0} \neq 0$, then we take $y$ such that the value from \{${y_{i_0}, p - y_{i_0}}$\} is even (or odd). Another way is to compare what the value is greater than $(p-1)/2$.

Let $U := \mathbb{P}^1 \setminus \text{par}^{-1}(\text{Ram})$ and

$$
h' : C_8(\mathbb{F}_q) \setminus \text{Ram} \to E_a(\mathbb{F}_q) \setminus E_a[2], \quad (x_0, x_1) \mapsto \begin{cases} 
(x_0, \sqrt{f(x_0)}) & \text{if } \sqrt{f(x_0)} \in \mathbb{F}_q, \\
(x_1, -\sqrt{f(x_1)}) & \text{if } \sqrt{f(x_1)} \in \mathbb{F}_q.
\end{cases}
$$

Thus the parametrization $\text{par} : \mathbb{P}^1 \to C_8$ from §3.1 induces the hashing

$$
h := h' \circ \text{par} : U(\mathbb{F}_q) \to E_a(\mathbb{F}_q).
$$

Of course, we could extend $h$ to all the field $\mathbb{F}_q$, but let us simplify the paragraph, not dealing with the exceptional cases. The defining polynomial of $C_8$ is symmetric, hence both points $\pm h(t)$ are in the image of $h$. More precisely, it can be checked that $h(2^h a^3/(3^i t)) = -h(t)$. Finally, since the curve $C_8$ is of bidegree $(8, 8)$, for any point $P \in E_a(\mathbb{F}_q)$ it follows that $|h^{-1}(P)| \leq 8$.

**Theorem 4.** We have the bounds

$$
\frac{q - 54}{8} \leq |\text{Im}(h)| \leq |E_a(\mathbb{F}_q)| - 2.
$$

**Proof.** By the adjunction formula [19, Exer. V.1.3.a] arithmetic genus $p_a = 49$ for the curve $C_8 \subset \mathbb{P}^1 \times \mathbb{P}^1$, because a canonical divisor $K_{\mathbb{P}^1 \times \mathbb{P}^1}$ is of bidegree $-(2, 2)$. Besides, for a point $P \in C_8(\mathbb{F}_q)$ consider the values

$$
\alpha_P := |\text{par}^{-1}(P)(\mathbb{F}_q)|, \quad \delta'_P := \begin{cases} 
0 & \text{if } \alpha_P = 0, \\
\alpha_P - 1, & \text{otherwise},
\end{cases}
$$

and we obtain
and $\delta_P$ [19, Exam. V.3.9.3]. Using [2, Lem. 2.2] and [19, Exam. V.3.9.(2-3)], we obtain the inequalities

$$|\text{par}(P_1(F_q))| = q + 1 - \sum_{P \in C_8(F_q)} \delta'_P \geq q + 1 - \sum_{P \in C_8(F_q)} \delta_P \geq q + 1 - p_a = q - 48.$$ 

Thus

$$\frac{q - 54}{8} \leq \left| \text{par}(\mathbb{P}^1(F_q)) \right| - \frac{\left| (C_8 \cap \text{Ram})(F_q) \right|}{8} \leq |\text{Im}(h)|$$

and the upper bound is trivial.

To be more precise the formula for $|E_a(F_q)|$ is given in [13, Prop. 2.5], [24, Th. 18.5]. The lower bound can be probably improved by the Chebotarev density theorem (in the function field case) as well as for another hashings (see [14, §3.2]).

We say that an arbitrary map has an algebraic (worst-case) complexity

$$n_S S + n_{M_c} M_c + n_M M + n_I I + n_{QRT} QRT + n_{SR} SR$$

if for all arguments it can be computed by means of (at most) $n_S$ squarings, $n_{M_c}$ multiplications by a constant $c \in \mathbb{F}_q$, $n_M$ general ones (with different non-constant multiples), $n_I$ inversions, $n_{QRT}$ quadratic residuosity tests, and $n_{SR}$ square roots, where all operations are in $\mathbb{F}_q$. Additions and subtractions in $\mathbb{F}_q$ are not considered, because they are very easy to compute. We also do not take account (in $n_{M_c}$) for multiplications by a constant $c \in \mathbb{F}_p$ such that $c \equiv 1 \pmod{3}$, because they are not more difficult than few additions. Implementation details of the operations mentioned see, for example, in [9, Ch. II], [13, §5.1].

**Lemma 2.** The hashing $h$ has an algebraic complexity

$$7S + 2M_c + 10M + 2I + QRT + SR.$$

**Proof.** It is easily checked that the functions $g(t), x_0(t), x_1(t)$ forming the parametrization $\text{par}$ have an algebraic complexity

$$S + M, \quad 2S + M_c + 3M + I, \quad 2S + M_c + 4M + I$$

respectively (the value $t^2$ is supposed to be known before calculating $x_0(t), x_1(t)$). In addition to $f(x_0)$ in the worst case (i.e., if $\sqrt{f(x_0)} \notin \mathbb{F}_q$) we must also compute $f(x_1)$. Each of these two substitutions is accomplished by $S + M$ operations. We emphasize once again that the quadratic residuosity test is unique. It remains to extract one square root $\sqrt{f(x_0)}$ or $\sqrt{f(x_1)}$. Thus we obtain the desired algebraic complexity for $h$. 

In pairing-based cryptography non-supersingular (i.e., for $p \equiv 1 \pmod{3}$) elliptic $\mathbb{F}_q$-curves $E_b: y^2 = x^3 - b$ of $j$-invariant 0 are only used in practice at the moment [42, Tab. 1]. Thus it is actual to generalize the simplified SWU method to them. More precisely, there is the following
Problem 1. Let $E_b$ be any elliptic $\mathbb{F}_q$-curve of $j = 0$ and $E'_b$ be its quadratic $\mathbb{F}_q$-twist. How to explicitly construct a rational $\mathbb{F}_q$-curve $D$ on the Kummer surface $K'_b$ of the direct product $E_b \times E'_b$ such that bidegree of the image $C := pr(D) \subset \mathbb{P}^1 \times \mathbb{P}^1$ does not depend on $\mathbb{F}_q$?

Unfortunately, the approach of this work does not allow to resolve this problem, because in the case $\sqrt[3]{b} \notin \mathbb{F}_q$ it seems that there is no a natural $\mathbb{F}_q^2$-isogeny from some elliptic curve of $j \neq 0$, that is an ascending $\mathbb{F}_q^2$-isogeny to $E_b$.

References


