# Hashing to elliptic curves of $j$-invariant 1728

Koshelev Dmitrii [1]

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 $h\colon \mathbb{F}_q \to E_a(\mathbb{F}_q)$ to the case of any elliptic $\mathbb{F}_q$-curve $E_a\colon y^2 = x^3 - ax$ of $j$-invariant 1728. In comparison with the (classical) SWU method the simplified SWU method allows to avoid one quadratic residuosity test in the field $\mathbb{F}_q$, which is a quite painful operation in cryptography with regard to timing attacks.

More precisely, in order to derive $h$ we obtain a rational $\mathbb{F}_q$-curve $C$ (and its explicit quite simple proper $\mathbb{F}_q$-parametrization) on the Kummer surface $K'$ associated with the direct product $E_a \times E_a'$, where $E_a'$ is the quadratic $\mathbb{F}_q$-twist of $E_a$. Our approach of finding $C$ is based on the fact that every curve $E_a$ has a vertical $\mathbb{F}_{q^2}$-isogeny of degree 2.

**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 $E\colon y^2 = f(x)$ 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 $h\colon \mathbb{F}_q \to E(\mathbb{F}_q)$ (by no means a group homomorphism) often called *hashing* or *encoding*. It should not be necessarily injective or surjective, but the bigger image $\mathrm{Im}(h)$ 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, Theorem 14.1]) and improved in [35]. Now it is often called in honor of its authors: *Shallue, van de Woestijne*, and sometimes *Ulas*.

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

The SWU method consists in parametrizing a (possibly singular) *rational* $\mathbb{F}_q$*-curve* $C$ (see, e.g., [34, §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 [1, §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

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

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 $\big(a_i, \pm\sqrt{f(a_i)}\big) \in E(\mathbb{F}_q)$.

According to [26, Theorem 2] the threefold $T$ is not uniruled [11, Chapter 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, Theorem 1.1] the surface $K$ and hence the 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

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

As one can see, this is the quadratic $\mathbb{F}_q$-twist of $K$, which in itself is the Kummer surface of $E\times E'$, where $E'\colon y^2 = f(x)c$ is the quadratic $\mathbb{F}_q$-twist of $E$. If in the SWU method we take a rational $\mathbb{F}_q$-curve on $K'$ one obtains the so-called *simplified SWU method* [8, §7].

Nevertheless, despite the 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 among elliptic curves only the ordinary ones with $j(E) = 0, 1728$ are interesting in pairing-based cryptography [13, Chapter 4]. This is due to the existence of high-degree twists for them, leading to faster pairing computations [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) $\mathcal{E} \to E$ of degree 11 (resp. 3) from a certain auxiliary elliptic curve $\mathcal{E}$ with $j(\mathcal{E}) \neq 0, 1728$. Unfortunately, this approach highly depends on $\mathbb{F}_q$, that is in some cases there is no 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 $E_a\colon y^2 = x^3 - ax$ with $j = 1728$. The most famous example of such pairing-friendly curves are Kachisa–Schaefer–Scott (KSS) curves of embedding degree 16 [25, Example 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 the (classical) SWU method, to our knowledge, was the only way to produce a hashing $h\colon \mathbb{F}_q \to E_a(\mathbb{F}_q)$ regardless of $\mathbb{F}_q$.

It is worth noting that to derive the curve $C$ we originally used (among other things) the theory of *Weil restriction* (*descent*) [18, §8.1] for elliptic curves with respect to the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$. The cryptographic community knows this operation as an instrument of cryptanalysis [9, §22.3]. However, in order to simplify the understanding of our construction we use an equivalent language, namely the "twisted" Frobenius endomorphism $\pi$ from §1.

Let us give a brief summary of our approach, commenting Figures 4 and 5, where the notation $D_8 \subset A'_a/[-1]$ is taken instead of $C \subset K'$. First, we use the direct product $\psi\colon E_a^2 \to E_a \times E'_a$ (from §1) of the trace and "twisted" trace maps with respect to $\mathbb{F}_{q^2}/\mathbb{F}_q$. Second, we take the direct product $\varphi$ (from §3) of the vertical $\mathbb{F}_{q^2}$-isogeny $\varphi_+\colon E_+ \to E_a$ of degree 2 and its $\mathbb{F}_q$-conjugate $\varphi_-\colon E_- \to E_a$, where $j(E_\pm) = 287496$. Further, it is considered the restrictions $\overline{\psi}$ and $\overline{\varphi}$ to the Kummer surfaces of $\psi$ and $\varphi$ respectively. By means of some technique we find in §3.1 the proper $\pi$-invariant parametrization $\omega$ of the curve $D_1$, which is the inverse image (under the projection $pr\colon E_+ \times E_-/[-1] \to \mathbb{P}^1 \times \mathbb{P}^1$ from §2) of a $\pi$-invariant curve $C_1$ of bidegree $(1,1)$. Thus we obtain the parametrization $par' := \overline{\psi} \circ \overline{\varphi} \circ \omega\colon \mathbb{A}^1 \simeq\dashrightarrow D_8$. It is proper according to Theorems 2.1 and 4. Finally, it is defined over $\mathbb{F}_q$ by virtue of Theorem 1 and the obvious fact that $\varphi$ is $\pi$-invariant.

Interestingly, coefficients of our functions defining $par'$ are almost entirely some powers of 2 and 3. This allows to compute the corresponding hashing $h\colon \mathbb{F}_q \to E_a(\mathbb{F}_q)$ 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 respectively about the Kummer surface for the direct product of two elliptic curves. Next, §3 is dedicated to the new construction of a (singular) rational $\mathbb{F}_q$-curve on $K'$ in the case of elliptic curves $E_a$, providing in §3.1 explicit formulas for its proper $\mathbb{F}_q$-parametrization. Finally, in §4 we make some remarks and conclusions, including the computation of an algebraic complexity for the hashing $h\colon \mathbb{F}_q \to E_a(\mathbb{F}_q)$ 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



# 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 $\overline{E_i}$ given by the affine Weierstrass forms

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

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

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 $\overline{R_i} \not\simeq R_i \cup \{P_\infty\}$ even over $\overline{\mathbb{F}_q}$, 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

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

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

$$R_i\colon \begin{cases} v_0^2 + \gamma v_1^2 = u_0^3 + 3\gamma u_0 u_1^2 + a_0 u_0 + (-1)^i a_1 \gamma u_1 + b_0, \\ 2v_0 v_1 = \gamma u_1^3 + 3u_0^2 u_1 + a_0 u_1 + (-1)^i (a_1 u_0 + b_1) \end{cases} \quad \subset \quad \mathbb{A}^4_{(u_0,v_0,u_1,v_1)}.$$

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

$$s\colon \mathbb{A}^4 \xrightarrow{\sim} \mathbb{A}^4, \qquad (u_0,v_0,u_1,v_1) \mapsto (u_0,v_0,-u_1,-v_1)$$

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

$$\theta\colon \mathbb{A}^4_{(u_0,v_0,u_1,v_1)} \xrightarrow{\sim} \mathbb{A}^4_{(x_0,y_0,x_1,y_1)} \qquad \text{s.t.} \qquad \theta\colon R \xrightarrow{\sim} A$$

given by the matrix

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

Consider the permutation

$$s' := \theta \circ s \circ \theta^{-1}\colon \mathbb{A}^4 \xrightarrow{\sim} \mathbb{A}^4, \qquad (x_0,y_0,x_1,y_1) \mapsto (x_1,y_1,x_0,y_0)$$

and the "twisted" Frobenius endomorphism

$$\pi\colon \mathbb{A}^4 \to \mathbb{A}^4, \qquad (x_0,y_0,x_1,y_1) \mapsto (x_1^q, y_1^q, x_0^q, y_0^q) \qquad \text{s.t.} \qquad \pi\colon A \to A.$$

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 $\varphi\colon A \dashrightarrow \mathbb{A}^4_{(x_0,y_0,x_1,y_1)}$ correspond to $\mathbb{F}_q$-ones

$$\theta^{-1}(C) \subset R, \qquad \theta^{-1} \circ \varphi \circ \theta\colon R \dashrightarrow \mathbb{A}^4_{(u_0,v_0,u_1,v_1)}.$$

This means that

$$C = s'\big(C^{(1)}\big), \qquad \varphi = \big(\varphi_{x_0}, \varphi_{y_0}, \varphi_{x_0}^{(1)} \circ s', \varphi_{y_0}^{(1)} \circ s'\big),$$

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 $\varphi_{x_0}, \varphi_{y_0} \in \mathbb{F}_{q^2}(A)$.

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

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

respectively.

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

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

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

$$E' \colon \gamma y^2 = x^3 + ax + b, \qquad\qquad \sigma \colon E' \xrightarrow{\sim} E, \qquad (x, y) \mapsto (x, \sqrt{\gamma}y).$$

Consider the exact sequences

$$0 \to E \hookrightarrow R \xrightarrow{\tau'} E' \to 0, \qquad 0 \to E' \hookrightarrow R \xrightarrow{\tau} E \to 0,$$

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

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

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

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

and $\widehat{\chi} \colon E \times E' \to R$ (dual to $\chi$) have the kernels

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

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

**Theorem 1.** *It is easily checked that* $(\mathrm{Fr} \times \mathrm{Fr}) \circ \psi = \psi \circ \pi$*. In particular, $\pi$-invariant points and curves on $E^2$ are transformed by means of $\psi$ to $\mathbb{F}_q$-ones on $E \times E'$.*

## 2 Kummer surfaces

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

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

and their direct product

$$A := E_0 \times E_1 \subset \mathbb{A}^4_{(x_0,y_0,x_1,y_1)}, \qquad \overline{A} = \overline{E_0} \times \overline{E_1} \hookrightarrow \mathbb{P}^8,$$

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

$$\overline{A} = A \ \sqcup \ \overline{E_0} \times \{P_\infty\} \ \cup \ \{P_\infty\} \times \overline{E_1}.$$

Hereafter we will identify $E_0$, $\overline{E_0}$, $\overline{E_0} \times \{P_\infty\}$ (resp. $E_1$, $\overline{E_1}$, $\{P_\infty\} \times \overline{E_1}$), 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 $E_0 \simeq E_1$, then at least over $\overline{\mathbb{F}_q}$ 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

$$\begin{aligned} A/[-1]\colon y^2 = f_0(x_0) f_1(x_1) \qquad &\subset \quad \mathbb{A}^3_{(x_0,x_1,y)}, \\ K_A\colon y_0^2 f_1(x_1) = y_1^2 f_0(x_0) \qquad &\subset \quad \mathbb{A}^2_{(x_0,x_1)} \times \mathbb{P}^1_{(y_0:y_1)} \end{aligned}$$

and the two-sheeted maps

$$\begin{aligned} \rho\colon A \to A/[-1], \qquad & (x_0,y_0,x_1,y_1) \mapsto (x_0,x_1,y_0y_1), \\ \rho'\colon A \dashrightarrow K_A, \qquad & (x_0,y_0,x_1,y_1) \mapsto \big((x_0,x_1),(y_0:y_1)\big). \end{aligned}$$

Therefore blowing up and blowing down maps have the form

$$\begin{aligned} bl = \rho \circ (\rho')^{-1}\colon K_A \to A/[-1], \qquad & \big((x_0,x_1),(y_0:y_1)\big) \mapsto \Big(x_0,x_1,f_1(x_1)\frac{y_0}{y_1}\Big) = \Big(x_0,x_1,f_0(x_0)\frac{y_1}{y_0}\Big), \\ bl^{-1} = \rho' \circ \rho^{-1}\colon A/[-1] \dashrightarrow K_A, \qquad & (x_0,x_1,y) \mapsto \Big((x_0,x_1),\big(y : f_1(x_1)\big)\Big) = \Big((x_0,x_1),\big(f_0(x_0):y\big)\Big) \end{aligned}$$

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

$$L_r := \rho(\{P_r\} \times E_1), \qquad M_s := \rho(E_0 \times \{P_s\})$$

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

$$L_r = \{x_0 = r, y = 0\}, \qquad M_s = \{x_1 = s, y = 0\}, \qquad E_{r,s} = \{x_0 = r, x_1 = s\}.$$

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

$$\overline{A}/[-1] = A/[-1] \sqcup L_\infty \cup M_\infty, \qquad \mathbb{P}^1 \times \mathbb{P}^1 = \mathbb{A}^2_{(x_0,x_1)} \sqcup L_\infty \cup M_\infty.$$

It is well known that $K_A$ is a K3 surface [22], i.e., its canonical class and the first cohomology space $\mathrm{H}^1(K_A, \mathcal{O}_{K_A})$ of the structure sheaf $\mathcal{O}_{K_A}$ are zero. According to [39, §2.8.4], [22, Chapter 17] we have:

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

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

$$2 \leqslant \rho(A) \leqslant 6, \qquad 8 \leqslant \rho(K_A) \leqslant 22$$

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. $C \not\subset Ram$) we denote by $r_C$ the count of branches $B$ [20, §4.3] on $C$ such that the intersection number $\mathrm{I}_P(B, Ram)$ is odd, where $P$ is the centre of $B$. It is known that branches on $C$ are in the natural bijective correspondence with points of the singularity resolution of $C$, i.e., with discrete valuations [32, §1] of the function field $\overline{\mathbb{F}_q}(C)$. In particular, denoting by $\nu$ the discrete valuation corresponding to $B$, we get

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

Thus in order to calculate the value $r_C$ we can choose any of the two given equivalent notions.

**Theorem 2** ([32, Proposition 1.2.3])**.** *Suppose that $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ is a rational $\mathbb{F}_q$-curve. Let $D := pr^{-1}(C)$ 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 $pr\colon D_0 \to C$, $pr\colon D_1 \to C$ 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 3** ([6, Lemma 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* $C := pr(D)$ *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* [16]*).*

Suppose that $E_0, E_1$ are $\mathbb{F}_q$-conjugate elliptic $\mathbb{F}_{q^2}$-curves as in §1 (hence we will use its notation). Let $K_R$ be the Kummer surface of the Weil restriction $R$ and

$$Q := K_R/\langle [1]\times[-1] \rangle \;=\; R/\langle [1]\times[-1], [-1]\times[1] \rangle.$$

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, Exercise 8.1.6.iii]. Looking at the transformation $\theta\colon R \xrightarrow{\sim} A$, we see that in affine coordinates the natural two-sheeted maps have the form

$$\rho\colon R \to R/[-1], \qquad (u_0, v_0, u_1, v_1) \mapsto (u_0, u_1, v_0^2 - \gamma v_1^2),$$
$$pr\colon R/[-1] \to Q, \qquad (u_0, u_1, v) \mapsto (u_0, u_1).$$

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

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

# 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 $E_a\colon y^2 = f(x) := x^3 - ax$ of $j$-invariant 1728. According to [36, Example V.4.5] they are ordinary if and only if $p \equiv 1 \pmod 4$, i.e., $\sqrt{-1} \in \mathbb{F}_p$. 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

$$E_a \xrightarrow{\sim} E_{a'}, \qquad (x, y) \mapsto (\sqrt{\alpha}x, \sqrt[4]{\alpha^3}y),$$

where $\alpha := a'/a$. From now on we assume that $\sqrt{a} \notin \mathbb{F}_q$ (hence $\sqrt[4]{a} \notin \mathbb{F}_{q^2}$). Therefore 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

$$E_1' \colon ay^2 = x^3 - x, \qquad E_a' \colon ay^2 = x^3 - ax$$

and the corresponding $\mathbb{F}_{q^2}$-isomorphisms $\sigma \colon E_1' \xrightarrow{\sim} E_1$, $\sigma \colon E_a' \xrightarrow{\sim} E_a$. It is obvious that

$$E_1' \xrightarrow{\sim} E_{a^2}, \qquad E_a' \xrightarrow{\sim} E_{a^3}, \qquad (x, y) \mapsto (ax, a^2 y).$$

The curves $E_{a^i}$ are pairwise non-isogenous over $\mathbb{F}_q$ [13, Proposition 2.5]. Hence, in particular, the Picard $\mathbb{F}_q$-numbers of the Kummer surfaces $K_{E_1 \times E_1'}$ and $K_{E_a \times E_a'}$ are equal to 18 and 12 respectively. In this paragraph we focus on constructing a rational $\mathbb{F}_q$-curve only on $K_{E_a \times E_a'}$, because this is more difficult than analogous task for $K_{E_1 \times E_1'}$.

Obviously,

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

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

$$E_a/\langle P_0 \rangle \simeq_{\mathbb{F}_q} E_a, \qquad E_\pm := E_a/\langle P_\pm \rangle \colon\ y^2 = x^3 - 11ax \mp 14a\sqrt{a},$$

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

$$\widehat{\varphi_\pm} \colon E_a \to E_\pm, \qquad \varphi_\pm \colon E_\pm \to E_a$$

have the form

$$\widehat{\varphi_\pm} = \begin{cases} x := x + \dfrac{2a}{x \mp \sqrt{a}}, \\ y := \Big(1 - \dfrac{2a}{(x \mp \sqrt{a})^2}\Big) y, \end{cases} \qquad \varphi_\pm = \begin{cases} x := \Big(x + \dfrac{a}{x \pm 2\sqrt{a}}\Big)/4, \\ y := \Big(1 - \dfrac{a}{(x \pm 2\sqrt{a})^2}\Big) y/8. \end{cases}$$

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

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

where

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

Clearly,

$$\widehat{\varphi_+}(P_0) = \widehat{\varphi_+}(P_-) = Q_0^{(0)}, \qquad \varphi_+\big(Q_\pm^{(0)}\big) = P_+,$$
$$\widehat{\varphi_-}(P_0) = \widehat{\varphi_-}(P_+) = Q_0^{(1)}, \qquad \varphi_-\big(Q_\pm^{(1)}\big) = P_-$$

and hence

$$E_a = E_+/\big\langle Q_0^{(0)} \big\rangle = E_-/\big\langle Q_0^{(1)} \big\rangle.$$

Finally, letting

$$A_{\pm} := E_+ \times E_-, \qquad A_a := E_a \times E_a, \qquad A'_a := E_a \times E'_a,$$

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

$$\widehat{\varphi} := \widehat{\varphi_+} \times \widehat{\varphi_-} \colon\ A_a \to A_{\pm}, \qquad \varphi := \varphi_+ \times \varphi_- \colon\ A_{\pm} \to A_a,$$

which are $\pi$-invariant.

Next, let

$$\overline{\varphi} := \rho \circ \varphi \circ \rho^{-1} \colon\ A_{\pm}/[-1] \to A_a/[-1], \qquad \overline{\psi} := \rho \circ \psi \circ \rho^{-1} \colon\ A_a/[-1] \to A'_a/[-1],$$
$$\overline{\overline{\varphi}} := pr \circ \overline{\varphi} \circ pr^{-1} \colon\ \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1 \times \mathbb{P}^1, \qquad \overline{\overline{\psi}} := pr \circ \overline{\psi} \colon\ A_a/[-1] \to \mathbb{P}^1 \times \mathbb{P}^1,$$

where $\psi$ is taken from §1. These maps form a commutative diagram represented in Figure 4. Note that $\overline{\psi}$ does not descend to any map $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1 \times \mathbb{P}^1$. Looking at the formulas of the isogeny $\varphi$, we obtain:

$$\overline{\varphi} = \begin{cases} x_0 := \Big(x_0 + \dfrac{a}{x_0 + 2\sqrt{a}}\Big)/4, \\ x_1 := \Big(x_1 + \dfrac{a}{x_1 - 2\sqrt{a}}\Big)/4, \\ y := \Big(1 - \dfrac{a}{(x_0 + 2\sqrt{a})^2}\Big)\Big(1 - \dfrac{a}{(x_1 - 2\sqrt{a})^2}\Big)y/64. \end{cases}$$

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

$$\overline{\overline{\psi}} = \begin{cases} x_0 = \dfrac{x_0^2 x_1 + x_0 x_1^2 - a(x_0 + x_1) - 2y}{(x_0 - x_1)^2}, \\ x_1 = \dfrac{x_0^2 x_1 + x_0 x_1^2 - a(x_0 + x_1) + 2y}{(x_0 - x_1)^2}. \end{cases}$$

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

$$C_1 \colon 6x_0x_1 - 11\sqrt{a}x_0 + 11\sqrt{a}x_1 - 20a,$$

which is the unique bidegree $(1,1)$ curve passing through the points

$$\big(-2\sqrt{a},\ 2\sqrt{a}\big), \qquad \big(\alpha_+\sqrt{a},\ -\alpha_-\sqrt{a}\big), \qquad \big(\alpha_-\sqrt{a},\ -\alpha_+\sqrt{a}\big)$$

(see Figure 1). This is one of the simplest $\pi$-invariant curves $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ having the value $r_C$ (from §2) equal to 2. Using Magma, one can compute the defining polynomial of $C_2 := \overline{\overline{\varphi}}(C_1)$, namely

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

This is a $\pi$-invariant cubic (of bidegree $(2,2)$) having the node $(\sqrt{a}, -\sqrt{a})$ (see Figure 2).

Since $r_{C_1} = r_{C_2} = 2$, by Theorem 2.2 the $\pi$-invariant curves

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

are rational. It turns out that the restriction $\overline{\overline{\varphi}}\colon C_1 \to C_2$ (and hence $\overline{\varphi}\colon D_1 \to D_2$) is invertible. Indeed,

$$(\overline{\overline{\varphi}})^{-1}\colon C_2 \dashrightarrow C_1, \qquad (\overline{\overline{\varphi}})^{-1} = \begin{cases} x_0 := \dfrac{24x_0^2 - 24x_0x_1 - 49\sqrt{a}x_0 + 25\sqrt{a}x_1 + 26a}{6(x_0 - \sqrt{a})}, \\ x_1 := \dfrac{11\sqrt{a}x_0 + \sqrt{a}x_1 - 10a}{6(x_0 - \sqrt{a})}. \end{cases}$$

Finally, denote by $C_2^{(1)}$ $\big($resp. $D_2^{(1)} = pr^{-1}\big(C_2^{(1)}\big)\big)$ the curve $\mathbb{F}_q$-conjugate to $C_2$ (resp. $D_2$).

Again, by means of Magma we get the image $C_8 := \overline{\overline{\psi}}(D_2) = \overline{\overline{\psi}}\big(D_2^{(1)}\big)$ (see Figure 3) given by the symmetric $\mathbb{F}_q$-polynomial

$$\begin{aligned} C_8\colon\ & 5764801a^3s_1^8 - 921984a^2s_1^6s_2^2 + 3471884416a^3s_1^6s_2 + 6914880000a^4s_1^6 + 36864as_1^4s_2^4 - \\ & 6463336448a^2s_1^4s_2^3 + 216401113088a^3s_1^4s_2^2 - 1634869760000a^4s_1^4s_2 + 2073600000000a^5s_1^4 + \\ & 966524928as_1^2s_2^5 - 3811311616a^2s_1^2s_2^4 - 941125009408a^3s_1^2s_2^3 + 10180198400000a^4s_1^2s_2^2 - \\ & 14745600000000a^5s_1^2s_2 - 37748736s_2^7 + 1124073472as_2^6 - 56463720448a^2s_2^5 + \\ & 757642297344a^3s_2^4 - 15920005120000a^4s_2^3 + 26214400000000a^5s_2^2, \end{aligned}$$

where $s_1 := x_0 + x_1$, $s_2 := x_0x_1$ are the elementary symmetric polynomials. Note that $\mathrm{bideg}(C_8) = (8,8)$. Since $r_{C_8} = 0$ it follows from Theorem 2.1 that the inverse image $pr^{-1}(C_8)$ consists of two different rational curves $D_8 := \overline{\psi}(D_2)$ and $D_8' := \overline{\psi}\big(D_2^{(1)}\big)$ such that the restrictions $pr\colon D_8 \to C_8$, $pr\colon D_8' \to C_8$ are birational. Moreover, $D_8, D_8'$ are defined over the field $\mathbb{F}_q$, since $D_2, D_2^{(1)}$ are $\pi$-invariant. This is an immediate corollary from Theorem 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 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.*

By Theorem 3 the inverse images

$$H_i := \rho^{-1}(D_i), \qquad H_2^{(1)} := \rho^{-1}\big(D_2^{(1)}\big), \qquad H_8' := \rho^{-1}(D_8'),$$

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

$$\varphi\colon H_1 \to H_2, \qquad \psi\colon H_2 \to H_8, \qquad \psi\colon H_2^{(1)} \to H_8'$$

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

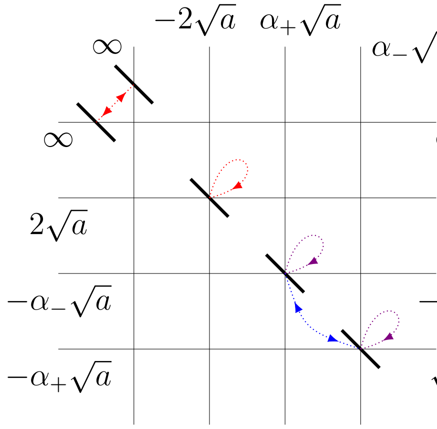


Figure 1: The curve $C_1$

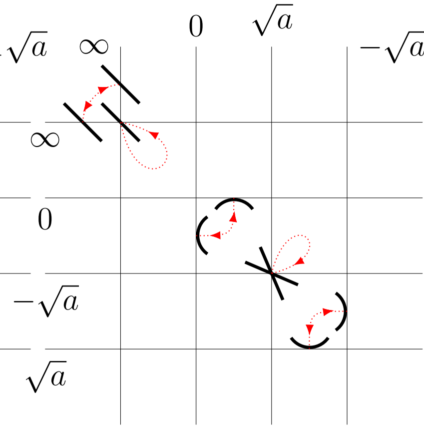


Figure 2: The curve $C_2$

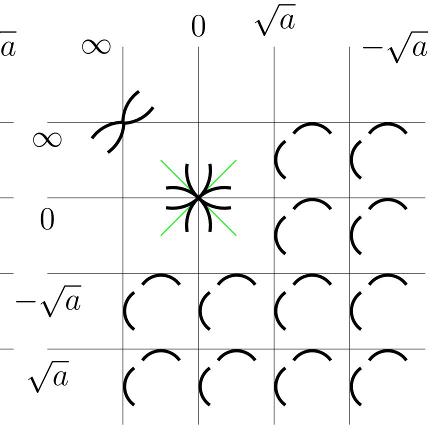


Figure 3: The curve $C_8$

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

$$\begin{array}{ccccc}
A_\pm & \xrightarrow{\varphi} & A_a & \xrightarrow{\psi} & A'_a \\
\rho\downarrow & & \rho\downarrow & & \downarrow\rho \\
A_\pm/[-1] & \xrightarrow{\overline{\varphi}} & A_a/[-1] & \xrightarrow{\overline{\psi}} & A'_a/[-1] \\
pr\downarrow & & pr\downarrow & \overset{\overline{\overline{\psi}}}{\searrow} & \downarrow pr \\
\mathbb{P}^1\times\mathbb{P}^1 & \xrightarrow{\overline{\overline{\varphi}}} & \mathbb{P}^1\times\mathbb{P}^1 & & \mathbb{P}^1\times\mathbb{P}^1
\end{array}$$

Figure 4

$$\begin{array}{ccccc}
H_1 & \xrightarrow{\varphi} & H_2 & \xrightarrow{\psi} & H_8 \\
\rho\downarrow & & \rho\downarrow & & \downarrow\rho \\
D_1 & \xrightarrow{\overline{\varphi}} & D_2 & \xrightarrow{\overline{\psi}} & D_8 \\
pr\downarrow & & pr\downarrow & \overset{\overline{\overline{\psi}}}{\searrow} & \downarrow pr \\
C_1 & \xrightarrow{\overline{\overline{\varphi}}} & C_2 & & C_8
\end{array}$$

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:

$$pr_{C_1}\colon C_1 \xrightarrow{\sim} \mathbb{A}^1_x, \quad x := \frac{3\sqrt{a}(x_0+x_1)}{3(x_0-x_1)+10\sqrt{a}} \qquad \text{s.t.} \qquad pr_{C_1}^{-1}\colon \mathbb{A}^1_x \xrightarrow{\sim} C_1, \quad \begin{cases} x_0 := \dfrac{-5\sqrt{a}x+6a}{3(x-\sqrt{a})}, \\ x_1 := \dfrac{5\sqrt{a}x+6a}{3(x+\sqrt{a})}. \end{cases}$$

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

$$D'_1\colon 3^6x^6y^2 + 2^6a^3x^6 - 3^7ax^4y^2 - 2^4 3^2a^4x^4 + 3^7a^2x^2y^2 + 3^4a^5x^2 - 3^6a^3y^2 \quad \subset \quad \mathbb{A}^2_{(x,y)}.$$

Thus there are birational isomorphisms

$$\chi := pr_{C_1}\times \mathrm{id}_y\colon D_1 \xrightarrow{\sim} D'_1, \qquad \chi^{-1} = pr_{C_1}^{-1}\times\mathrm{id}_y\colon D'_1 \xrightarrow{\sim} D_1.$$

Further, Magma allows to compute the anticanonical map from $D_1'$ to the $\mathbb{F}_q$-conic

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

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

$$\varphi_{-K}\colon D_1' \simeq\dashrightarrow Q, \quad \begin{cases} u := x, \\ v := \dfrac{2^3a^3(3^2a - 2^3x^2)x}{3^6(x^2-a)y} \end{cases} \quad \text{s.t.} \quad \varphi_{-K}^{-1}\colon Q \simeq\dashrightarrow D_1', \quad \begin{cases} x := u, \\ y := \dfrac{(2^3u^2 - 3^2a)uv}{2^3(u^2-a)^2}. \end{cases}$$

Finally, the projection from the point $(2^3a^2/3^3, 0) \in Q(\mathbb{F}_q)$ has the form

$$pr_Q\colon Q \simeq\dashrightarrow \mathbb{A}^1_t, \quad t := \frac{3^3v - 2^3a^2}{3^3u} \quad \text{s.t.} \quad pr_Q^{-1}\colon \mathbb{A}^1_t \simeq\dashrightarrow Q, \quad \begin{cases} u := \dfrac{-2^43^3a^2t}{2^6a^3 + 3^6t^2}, \\ v := \dfrac{2^3a^2(2^6a^3 - 3^6t^2)}{3^3(2^6a^3+3^6t^2)}. \end{cases}$$

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

$$par := \overline{\overline{\psi}} \circ \overline{\varphi} \circ \omega\colon \ \mathbb{A}^1_t \simeq\dashrightarrow C_8, \qquad \text{where} \qquad \omega := \chi^{-1} \circ \varphi_{-K}^{-1} \circ pr_Q^{-1}\colon \ \mathbb{A}^1_t \simeq\dashrightarrow D_1,$$

given by the functions

$$par = \begin{cases} x_0 := \dfrac{(3^8t^2 + 2^6a^3)^2 g(t)}{2^{14}3^2a^4(3^7t^2 - 2^6a^3)^2 t}, \\ x_1 := \dfrac{(3^4t^2 + 2^6a^3)^2 g(t)}{2^83^6a(3^5t^2 - 2^6a^3)^2t^3}, \end{cases} \qquad \text{where} \qquad g(t) := t^2(3^{12}t^2 - 2^73^47a^3) + 2^{12}a^6.$$

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, Theorem 4.21] we get

**Theorem 4.** *The map par (or, equivalently, $\overline{\overline{\psi}}|_{D_2}$) is birational.*

Another proof consists in applying the projection formula [11, §1.2] with respect to $\overline{\overline{\psi}}$. Interestingly, according to [34, Corollary 6.14] the curve $C_8$ is not polynomial, i.e., it cannot be parametrized by two polynomials (even over $\overline{\mathbb{F}_q}$). Finally, the inverse map $par^{-1}\colon C_8 \simeq\dashrightarrow \mathbb{A}^1_t$ and the maps $par' := pr^{-1} \circ par\colon \mathbb{A}^1_t \simeq\dashrightarrow D_8, D_8'$ (or, equivalently, the functions $\pm\sqrt{af(x_0)f(x_1)} \in \mathbb{F}_q(t)$) 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 $\mathbb{F}_{q^2}$-isomorphism $\sigma$) and

$$A_\pm' := E_+ \times E_-', \qquad A_a' := E_a \times E_a'.$$

By means of

$$[1]\times\sigma\colon A'_{\pm} \xrightarrow{\sim} A_{\pm}, \qquad [1]\times\sigma\colon A'_a \xrightarrow{\sim} A_a$$

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

$$A'_{\pm} \to A'_a, \qquad A'_{\pm}/[-1] \to A'_a/[-1]$$

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

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

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

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

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

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

Fortunately, for $q \not\equiv 1 \pmod 8$ 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 $0 \leqslant y_i < p$. 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 when the value is greater than $(p-1)/2$.

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

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

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

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

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 $h\big(2^6a^3/(3^6t)\big) = -h(t)$. Finally, since the curve $C_8$ is of bidegree $(8,8)$, for any point $P \in E_a(\mathbb{F}_q)$ it follows that $|h^{-1}(P)| \leqslant 8$.

**Theorem 5.** *We have the bounds*

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

*Proof.* By the adjunction formula [19, Exercise 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

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

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

$$\left|par\big(\mathbb{P}^1(\mathbb{F}_q)\big)\right| \ = \ q+1-\sum_{P\in C_8(\mathbb{F}_q)} \delta'_P \ \geqslant \ q+1-\sum_{P\in C_8(\mathbb{F}_q)} \delta_P \ \geqslant \ q+1-p_a \ = \ q-48.$$

Thus

$$\frac{q-54}{8} \leqslant \frac{\left|par\big(\mathbb{P}^1(\mathbb{F}_q)\big)\right| - \left|(C_8 \cap Ram)(\mathbb{F}_q)\right|}{8} \leqslant |\mathrm{Im}(h)|$$

and the upper bound is trivial. □

To be more precise the formula for $|E_a(\mathbb{F}_q)|$ is given in [13, Proposition 2.5], [24, Theorem 18.5]. The lower bound can be probably improved by the Chebotarev density theorem (in the function field case) as well as this is done for some other 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 $c \pmod p \leqslant 7$, because they are not more difficult than few additions. Implementation details of the operations mentioned see, for example, in [9, Chapter 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 *par* have an algebraic complexity

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

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 $E_b\colon y^2 = x^3 - b$ of $j$-invariant 0 are only used in practice at the moment [42, Table 1]. Thus it is tempting 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 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


[1] Andreatta M., Wiśniewski J. *On the Kummer construction.* // Revista Matemática Complutense, 2010. Vol. 23(1). P. 191–215.

[2] Aubry Y., Perret M. *A Weil theorem for singular curves.* // Arithmetic, Geometry and Coding Theory (AGCT-4), 1993. P. 1–7.

[3] Barbulescu R., El Mrabet N., Ghammam L. *A taxonomy of pairings, their security, their complexity.* // IACR Cryptology ePrint Archive, 2019.

[4] Barbulescu R., Duquesne S. *Updating key size estimations for pairings.* // Journal of Cryptology, 2018. P. 1–39.

[5] Bernstein D., Hamburg M., Krasnova A., Lange T. *Elligator: Elliptic-curve points indistinguishable from uniform random strings.* // Conference on Computer & Commun. Security, 2013. P. 967–980.

[6] Bogomolov F., Tschinkel Y. *Rational curves and points on K3 surfaces.* // American Journal of Mathematics, 2005. Vol. 127(4). P. 825–835.

[7] Boneh D., Franklin M. *Identity-based encryption from the Weil pairing.* // SIAM Journal on Computing, 2003. Vol. 32(3). P. 586–615.

[8] Brier E., Coron J.-S., Icart T., Madore D., Randriam H., Tibouchi M. *Efficient indifferentiable hashing into ordinary elliptic curves.* // 30th Annual Cryptology Conference, 2010. P. 237–254.

[9] Cohen H., Frey G., Avanzi R., Doche C., Lange T., Nguyen K., Vercauteren F. *Handbook of elliptic and hyperelliptic curve cryptography.* — Boca Raton.: Chapman & Hall, 2006.

[10] Cynk S., Schütt M. *Generalised Kummer constructions and Weil restrictions.* // Journal of Number Theory, 2009. Vol. 129(8). P. 1965–1975.

[11] Debarre O. *Higher-dimensional algebraic geometry.* — Berlin.: Springer-Verlag, 2001.

[12] Donten M. *On Kummer 3-folds.* // Revista Matemática Complutense, 2011. Vol. 24(2). P. 465–492.

[13] El Mrabet N., Joye M. *Guide to pairing-based cryptography.* — New York.: Chapman and Hall, 2016.

[14] Fouque P.-A., Tibouchi M. *Estimating the size of the image of deterministic hash functions to elliptic curves.* // 1st Inter. Conference on Crypto. and Information Security in Latin America, 2010. P. 81–91.

[15] Galbraith S. *Mathematics of public key cryptography.* — New York.: Cambridge University Press, 2012.

[16] Gaudry P., Schost É. *On the invariants of the quotients of the Jacobian of a curve of genus* 2. // 14th Inter. Symp. on Applied Algebra, Algebraic Algorithms, and Error-Correct. Codes, 2001. P. 373–386.

[17] Ghammam L., Fouotsa E. *Adequate elliptic curves for computing the product of n pairings.* // International Workshop on the Arithmetic of Finite Fields, 2016. P. 36–53.

[18] Gorchinskiy S., Shramov C. *Unramified Brauer group and its applications.* — Providence.: American Mathematical Society, 2018.

[19] Hartshorne R. Algebraic geometry. — Berlin.: Springer, 1977.

[20] Hirschfeld J., Korchmáros G., Torres F. *Algebraic curves over a finite field.* — Princeton.: Princeton University Press, 2008.

[21] Hunt B. *The geometry of some special arithmetic quotients.* — Berlin.: Springer-Verlag, 1996.

[22] Huybrechts D. *Lectures on K3 surfaces.* — Cambridge.: Cambridge University Press, 2016.

[23] Icart T. *How to hash into elliptic curves.* // 29th Annual International Cryptology Conference, 2009. P. 303–316.

[24] Ireland K., Rosen M. *A classical introduction to modern number theory.* — New York.: Springer-Verlag, 1990.

[25] Kachisa E., Schaefer E., Scott M. *Constructing Brezing–Weng pairing-friendly elliptic curves using elements in the cyclotomic field.* // 2nd Internat. Conf. on Pairing-Based Crypto., 2008. P. 126–135.

[26] Kollár J., Larsen M. *Quotients of Calabi–Yau varieties.* // Algebra, arithmetic, and geometry. — Birkhäuser Boston, 2009. P. 179–211.

[27] Koshelev D. *Magma code.* https://github.com/dishport/Hashing-to-elliptic-curves-of-j-invariant-1728.

[28] Kuwata M., Wang L. *Topology of rational points on isotrivial elliptic surfaces.* // International Mathematics Research Notices, 1993. Vol. 1993(4). P. 113–123.

[29] Mestre J.-F. *Rang de courbes elliptiques d'invariant donné.* // Comptes Rendus de l'Académie des Sciences - Series I - Mathematics, 1992. Vol. 314(12). P. 919–922.

[30] Milne J. *Abelian varieties.* // Arithmetic Geometry, 1986. P. 103–150.

[31] Mordell L. *Diophantine equations.* — London.: Academic Press, 1969.

[32] 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. — Birkhäuser Basel, 2001. P. 313–334.

[33] Scott S., Sullivan N., Wood C. *Hashing to elliptic curves.* // Internet-Draft, IETF Secretariat, 2018.

[34] Sendra J., Winkler F., Pérez-Díaz S. *Rational algebraic curves: A computer algebra approach.* — Berlin.: Springer-Verlag, 2008.

[35] Shallue A., van de Woestijne C. *Construction of rational points on elliptic curves over finite fields.* // 7th International Algorithmic Number Theory Symposium, 2006. P. 510–524.

[36] Silverman J. *The arithmetic of elliptic curves.* — New York.: Springer-Verlag, 2009.

[37] Skałba M. *Points on elliptic curves over finite fields.* // Acta Arithmetica, 2005. Vol. 117. P. 293–301.

[38] Ulas M. *Rational points on certain hyperelliptic curves over finite fields.* // Bulletin of the Polish Academy of Sciences. Mathematics, 2007. Vol. 55(2). P. 97–104.

[39] Ulmer D. *Elliptic curves over function fields.* // Arithmetic of L-functions, 2011. P. 211–280.

[40] Van der Geer G., Katsura T. *On the height of Calabi–Yau varieties in positive characteristic.* // Documenta Mathematica, 2003. Vol. 8(1). P. 97–113.

[41] Voisin C. *Miroir set involutions sur les surfaces K3.* // Astérisque, 1993. Vol. 218. P. 273–323.

[42] Yonezawa S., Chikara S., Kobayashi T., Saito T. *Pairing-friendly curves.* // Internet-Draft, IETF Secretariat, 2019.

[43] Wahby R., Boneh D. *Fast and simple constant-time hashing to the BLS12-381 elliptic curve.* // IACR Cryptology ePrint Archive, 2019.