A new elliptic curve point compression method based on $\mathbb{F}_p$-rationality of some generalized Kummer surfaces

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. In the article we propose a new compression method (to $2\log_2(p) + 3$ bits) for the $\mathbb{F}_{p^2}$-points of an elliptic curve $E_b\colon y^2 = x^3 + b$ (for $b \in \mathbb{F}_{p^2}^*$) of j-invariant 0. It is based on $\mathbb{F}_p$-rationality of some generalized Kummer surface GK_b. This is the geometric quotient of the Weil restriction $R_b := \mathrm{R}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_b)$ under the order 3 automorphism restricted from E_b. More precisely, we apply the theory of conic bundles (i.e., conics over the function field $\mathbb{F}_p(t)$) to obtain explicit and quite simple formulas of a birational $\mathbb{F}_p$-isomorphism between GK_b and $\mathbb{A}^2$. Our point compression method consists in computation of these formulas. To recover (in the decompression stage) the original point from $E_b(\mathbb{F}_{p^2}) = R_b(\mathbb{F}_p)$ we find an inverse image of the natural map $R_b \to GK_b$ of degree 3, i.e., we extract a cubic $\mathbb{F}_p$-root. For $p \not\equiv 1 \pmod{27}$ this is just a single exponentiation in $\mathbb{F}_p$, hence the new method seems to be much faster than the classical one with x-coordinate, which requires two exponentiations in $\mathbb{F}_p$.

Key words: pairing-based cryptography, elliptic curves of $j = 0$, point compression, Weil restriction, generalized Kummer surfaces, rationality problems, conic bundles, cubic roots, singular cubic surfaces.

Introduction

Nowadays, no doubt, elliptic cryptography is widely used in practice [6]. In many of its protocols one needs a *compression method* for points of an elliptic curve E over a finite field $\mathbb{F}_q$ of characteristic p. This is done for quick transmission of the information over a communication channel or for its compact storage in a memory. There exists a classical method, which considers an $\mathbb{F}_q$-point on $E \subset \mathbb{A}^2_{(x,y)}$ as the x (or y [16]) coordinate with 1 (resp. 2) bits to uniquely recover the another coordinate by solving a quadratic (resp. cubic) equation over $\mathbb{F}_q$. See variations of this method for $p = 2$ in [18], [52].

Consider an ordinary (i.e., non-supersingular) elliptic curve $E_b\colon y^2 = x^3 + b$ for $b \in \mathbb{F}_q^*$ (of j-invariant 0). Despite the insignificant acceleration [17] of Pollard rho method, these curves $\big($for $q = p \equiv 1 \pmod 3\big)$ have become very popular in elliptic cryptography. This is confirmed by the standards WAP WTLS [47, table 8], SEC 2 [50, §2] and different technologies such as cryptocurrencies (e.g., the curve Secp256k1 used in Bitcoin). The main reason for this is the existence of the order 3 automorphism $[\omega]\colon (x, y) \mapsto (x\sqrt[3]{1}, y)$ defined over $\mathbb{F}_p$. Therefore for a faster scalar multiplication on a curve E_b we can apply the so-called *GLV decomposition*

[1]Web page: https://www.researchgate.net/profile/Dima_Koshelev
Email: dishport@yandex.ru

This work was supported by a public grant as part of the FMJH project

[26]. At the same time, in [28] it is suggested to also consider curves E_b over $\mathbb{F}_{p^2}$, because for such fields we can apply the *GLS decomposition* [25] (an improvement of GLV one). It is worth noting, however, that the GLS decomposition is also applied to elliptic curves with $j \neq 0$. The most famous example is the curve Four$\mathbb{Q}$ [13] proposed by Microsoft. See [43, §8] for a comparison of the efficiency of the GLV-GLS approaches implemented for several curves, including some with $j = 0$.

Because of many interesting applications such as *identity-based cryptography* [53] or short signature schemes and breakthroughs in pairing computation [12] *pairing-based cryptography* [19] is becoming a more and more popular alternative to classical elliptic cryptography. Indeed, see standards of the organizations IEEE [30], ISO/IEC [33], [34], FIDO [42], W3C [58] and products of the companies ZECC [7], Intel [8], Ethereum Foundation [20] (more information is represented in [59]).

As usual in cryptography, an elliptic curve $E/\mathbb{F}_p$ is assumed to have a subgroup $G \subset E(\mathbb{F}_p)$ of large prime order $\ell \neq p$. The *embedding degree* of E (with respect to ℓ) is, by definition, the extension degree $k := [\mathbb{F}_p(\mu_\ell) : \mathbb{F}_p]$. Further, let E' be a twist for E of degree $d \mid k$ and $G' \subset E'(\mathbb{F}_{p^{\frac{k}{d}}})$ be the subgroup of order ℓ. In practice, pairings (of type 2 [12, §2.3.2]) are mainly taken in the form

$$G \times G' \to \mu_n \subset \mathbb{F}_{p^k}^* \quad [22, §7.3],$$

where k is the minimally possible number such that the discrete logarithm problem in $\mathbb{F}_{p^k}^*$ is hard, but d is, conversely, the maximally possible one. It is a classical fact that $d \leqslant 6$ and this bound is only attained by the elliptic curves E_b. Therefore they are considered to be the most pairing-friendly. Among those, the *Barreto–Naehrig* (BN) curves [5], [45, §2] and *Barreto–Lynn–Scott* (BLS12) curves [4] of embedding degree $k = 12$ (and only they as far as the author knows) are used in practice at the moment. Barreto–Naehrig curves also have $k = 12$, that is $k/d = 2$.

Thus it will be useful to find a compression method for $\mathbb{F}_{p^2}$-points of the curves $E_b/\mathbb{F}_{p^2}$, whose decompression stage is much faster than extracting a square $\mathbb{F}_{p^2}$-root. It is easily seen that the latter can be accomplished by extracting 2 square $\mathbb{F}_p$-roots (for details see [1]). Despite the known fact that for $p \not\equiv 1 \pmod 8$ a square $\mathbb{F}_p$-root is computed by a single exponentiation in $\mathbb{F}_p$, it is still a quite laborious operation. This article proposes a novel point compression method requiring (in the decompression stage) to extract only a single cubic $\mathbb{F}_p$-root. For $p \not\equiv 1 \pmod{27}$ this can also be done by one exponentiation in $\mathbb{F}_p$ (see [10, prop. 1]), hence our method seems to be about twice as quick as the classical one with the x (a fortiori, y) coordinate.

Our approach is based on an $\mathbb{F}_p$-rationality proof of the *generalized Kummer surface* $GK_b := R_b/[\omega]_2$ of the *Weil restriction* (*descent*) $R_b := \mathrm{R}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_b)$ [23, §3.2] with respect to the order 3 automorphism $[\omega]_2 := \mathrm{R}_{\mathbb{F}_{p^2}/\mathbb{F}_p}([\omega])$. More precisely, we apply the theory of *conic bundles* [31], [32] $\big($i.e., conics over the function field $\mathbb{F}_p(t)\big)$ to obtain explicit as well as quite simple formulas of a birational $\mathbb{F}_p$-isomorphism between GK_b and $\mathbb{A}^2$. The new compression method consists in computation of these formulas. To recover the original point from $E_b(\mathbb{F}_{p^2}) = R_b(\mathbb{F}_p)\big)$ we need to find an inverse image of the natural map $\varrho\colon R_b \to GK_b$ of degree 3, i.e., to solve a cubic equation over $\mathbb{F}_p$. The advantage of curves E_b is that the pull-back map ϱ^* is actually a *Kummer extension*, i.e., the field $\mathbb{F}_p(R_b)$ is generated by a cubic root of some rational function from $\mathbb{F}_p(GK_b)$.

A similar result has been obtained early in the author's master's thesis [41] for point compression of some two Jacobians J_b [2] over the fields $\mathbb{F}_{2^e}$, where $b \in \mathbb{F}_2$ and $2, 3 \nmid e$. These are the unique (up to an $\mathbb{F}_{2^e}$-isogeny) supersingular simple abelian surfaces that have the maximally possible embedding degree $k = 12$. We proved $\mathbb{F}_2$-rationality of (usual) Kummer surfaces $K := J_b/[-1]$ and even obtained explicit formulas of an $\mathbb{F}_2$-birational isomorphism between K and $\mathbb{A}^2$, also using the theory of conic bundles, but in a different way. Based on this knowledge, in the current article we formulate a conjecture about $\mathbb{F}_q$-rationality of geometrically rational generalized Kummer surfaces defined over a finite field $\mathbb{F}_q$.

This article is organized as follows. In §1 we recall or prove some mathematical facts, which are necessary for our main results. More precisely, §1.1 is dedicated to the theory of cubic polynomials (§1.1.1) and cubic $\mathbb{F}_p$-surfaces S_h with two $\mathbb{F}_p$-nodes (§1.1.2). Further, in §1.2 we review some facts about curves E_b and their Weil restrictions R_b (§1.2.1). In §1.3 we consider generalized Kummer surfaces, in particular GK_b (§1.3.1). Further, §1.4 discusses the theory of conic bundles, in particular an example of such a bundle on S_h (§1.4.1) and some propositions about blowing down components of degenerate fibers (§1.4.2). In §2 we prove $\mathbb{F}_p$-rationality of the surfaces GK_b, which leads to a new point compression method. We instantiate this method in §2.1 for a special case (including commercially used curve BLS12-381 [7]) and calculate its algebraic complexity. Finally, §3 discusses further questions regarding possible generalizations of this work.

Acknowledgements. The author expresses his deep gratitude to his scientific advisor M. Tsfasman and thanks A. Trepalin, K. Loginov, K. Shramov, L. de Feo, N. El Mrabet, and S. Gashkov for their help and useful comments. Also, special thanks to D. Fiorilli for his help in writing this text.

Contents

1 Mathematical preliminaries and auxiliary results

1.1 Cubics

1.1.1 Cubic polynomials

In this paragraph we recall some known facts about cubic polynomials. Many of these can be found, for example, in [35]. Consider a polynomial $x^3 + \alpha x^2 + \beta x + \gamma$ over a field k of characteristic $p \neq 2, 3$. After the variable change $x := y - \alpha/3$, we obtain the polynomial

$$f(y) := y^3 + cy + d, \qquad \text{where} \qquad c := \beta - \frac{\alpha^2}{3}, \qquad d := \gamma - \frac{\alpha\beta}{3} + \frac{2\alpha^3}{27}.$$

Let $G \hookrightarrow S_3$ be the Galois group of the splitting field of f over k. Further, for $a \in k$ we denote by $\left(\frac{a}{k}\right)$ the Legendre symbol, however in the case of a finite field $k = \mathbb{F}_q$ we also use the notation $\left(\frac{a}{q}\right)$.

Lemma 1. *The discriminant of f is equal to $\Delta = -4c^3 - 27d^2$ and*

$$\left(\frac{\Delta}{k}\right) = \begin{cases} 0 & \text{if} \quad f \text{ has a multiple root,} \\ 1 & \text{if} \quad G = 1 \text{ or } G \simeq \mathbb{Z}/3, \\ -1 & \text{if} \quad G \simeq \mathbb{Z}/2 \text{ or } G \simeq S_3. \end{cases}$$

Theorem 1 (Cardano formula)**.** *The roots of f are equal to $R_+ + R_-$, where*

$$R_\pm := \sqrt[3]{-\frac{d}{2} \pm \sqrt{D}}, \qquad D := -\frac{\Delta}{108} = \frac{c^3}{27} + \frac{d^2}{4}, \qquad R_+R_- = -\frac{c}{3}.$$

One can see that for general c, d finding roots of f (by this formula) consists in extracting 1 square root and 2 cubic ones.

Throughout the article we denote by ζ_3 a fixed primitive 3-th root of unity, which is equal to $(-1 + \sqrt{-3})/2$. However for $p = 0$ we prefer the symbol ω.

Lemma 2. *Assume that $\zeta_3 \in k^*$, i.e., $\left(\frac{-3}{k}\right) = 1$. Then a cubic extension of k is cyclic iff it is Kummer, i.e., it has the form $k(\sqrt[3]{a})$ for some $a \in k^*$ such that $a \notin (k^*)^3$.*

For $k = \mathbb{F}_p$ the condition $\zeta_3 \in \mathbb{F}_p^*$ is also equivalent to $p \equiv 1 \pmod 3$.

To formulate the next theorem we need to recall a definition of the Lucas sequence $v_n = v_n(a, b)$ for $a, b \in k$ and $n \in \mathbb{N}$:

$$v_0 := 2, \qquad v_1 := b, \qquad v_n := bv_{n-1} - av_{n-2}.$$

Theorem 2 ([16, thm 2])**.**
Assume that $k = \mathbb{F}_p$, $c, d \neq 0$, and $\left(\frac{\Delta}{p}\right) = -1$. Then the unique $\mathbb{F}_p$-root of f is equal to

$$-\frac{(3c)^{-\left(\frac{p}{3}\right)} v_n(C, D)}{3}, \qquad \textit{where} \qquad C := -27c^3, \qquad D := -27d, \qquad n := \frac{p + 2\left(\frac{p}{3}\right)}{3}.$$

Lemma 3 ([16, rem. 2])**.** *For* $a \in \mathbb{F}_p^*$ *we obtain:*

$$a \notin (\mathbb{F}_p^*)^3 \qquad \textit{if and only if} \qquad p \equiv 1 \pmod 3 \quad \textit{and} \quad a^{\frac{p-1}{3}} \neq 1.$$

Moreover, if $a \in (\mathbb{F}_p^*)^3$*, then*

$$\sqrt[3]{a} = \begin{cases} a^{\frac{2p-1}{3}} & \text{if} \quad p \equiv 2 \pmod 3, \\ \text{[10, prop. 1]} & \text{if} \quad p \equiv 1 \pmod 9 \text{ and } p \not\equiv 1 \pmod{27}, \\ a^{-\frac{p-4}{9}} & \text{if} \quad p \equiv 4 \pmod 9, \\ a^{\frac{p+2}{9}} & \text{if} \quad p \equiv 7 \pmod 9). \end{cases}$$

Algorithms of exponentiation in $\mathbb{F}_p$ and extracting cubic $\mathbb{F}_p$-roots in the case $p \equiv 1 \pmod{27}$ can be found, for example, in [54, §3.4] and [10] respectively. At the same time, for extracting square $\mathbb{F}_p$-roots see [54, §12.5.1].

1.1.2 Cubic $\mathbb{F}_p$-surfaces S_h with two $\mathbb{F}_p$-nodes

In this paragraph we study some singular cubic surfaces with 16 lines, which occur in §1.4.1, §2. The general theory of singular cubic ones (over a non-closed field) can be found, for example, in [11, part I].

Lemma 4. *Let* p *(>3) be a prime. For* $h = h_1 t + h_0 \in \mathbb{F}_p[t]$ $(h_1 \neq 0)$ *consider a cubic surface*

$$S_h := x^2 y - (t^2 + y^2) y - (h_1 t + h_0 y) z^2 \quad \subset \quad \mathbb{P}^3_{(x:y:z:t)}.$$

It has only two singular points $P_\pm := (\pm 1 : 0 : 0 : 1)$ *and they are nodes (i.e., of type* A_1*). In particular, the surface* S_h *is* $\mathbb{F}_p$*-rational.*

Proof. The partial derivatives of S_h are equal to

$$\frac{\partial S_h}{\partial x} = 2xy, \qquad \frac{\partial S_h}{\partial y} = x^2 - (t^2 + 3y^2) - h_0 z^2, \qquad \frac{\partial S_h}{\partial z} = -2(h_1 t + h_0 y) z, \qquad \frac{\partial S_h}{\partial t} = -2ty - h_1 z^2.$$

Besides, after the translation

$$\tau_{P_\pm} \colon (x : y : z : t) \mapsto (\pm x - t : y : z : t), \qquad \tau_{P_\pm}^{-1} \colon (x : y : z : t) \mapsto \big(\pm(x + t) : y : z : t\big)$$

the tangent cone of

$$S_{h,O} := \tau_{P_\pm}(S_h) \;=\; x^2 y + 2xty - y^3 - (h_1 t + h_0 y) z^2$$

at the origin $O = \tau_{P_\pm}(P_\pm)$ of $\mathbb{A}^3_{(x,y,z)}$ has the form

$$\mathrm{T}_O(S_{h,O}) = 2xy - h_1 z^2.$$

Therefore the points $P_\pm$ are nodes and the projection from one of them is the birational $\mathbb{F}_p$-isomorphism $pr \colon S_h \overset{\simeq}{\dashrightarrow} \mathbb{A}^2$. $\square$

Let $N_h := h_0^2 + h_1^2$ and note that

$$S_{h,O} \cap \mathrm{T}_O(S_{h,O}) = L_{P_+,P_-} \cup M_O,$$

where

$$L_{P_+,P_-} := \mathbb{V}(y,z), \qquad M_O := \begin{cases} h_1 x = \big(h_0 \pm \sqrt{N_h}\big) y, \\ h_1 z = \pm\sqrt{2h_1 xy}. \end{cases}$$

Here M_O is the union of 4 lines, i.e., the signs $\pm$ are taken independently. Consider the projection from O and its inverse map:

$$pr_O \colon S_{h,O} \overset{\simeq}{\dashrightarrow} \mathbb{A}^2_{(u,v)}, \qquad (x:y:z:t) \mapsto \Big(\frac{x}{y}, \frac{z}{y}\Big),$$

$$pr_O^{-1} \colon \mathbb{A}^2_{(u,v)} \overset{\simeq}{\dashrightarrow} S_{h,O}, \qquad (u,v) \mapsto (uY : Y : vY : T),$$

where

$$Y := h_1 v^2 - 2u, \qquad T := u^2 - h_0 v^2 - 1.$$

Note that pr_O, pr_O^{-1} are isomorphisms on the open subsets

$$U_O := S_{h,O} \setminus \big(\mathrm{T}_O(S_{h,O}) \cup L_\infty\big), \qquad V := \mathbb{A}^2_{(u,v)} \setminus \mathbb{V}(Y),$$

where $L_\infty := \mathbb{V}(y,t)$. Thus the maps

$$pr = pr_O \circ \tau_{P_\pm} \colon S_h \overset{\simeq}{\dashrightarrow} \mathbb{A}^2, \qquad pr^{-1} = \tau_{P_\pm}^{-1} \circ pr_O^{-1} \colon \mathbb{A}^2 \overset{\simeq}{\dashrightarrow} S_h$$

are those on the open subsets V and

$$U := \tau_{P_\pm}^{-1}(U_O) = S_h \setminus \big(\mathrm{T}_{P_\pm}(S_h) \cup L_\infty\big),$$

where

$$\mathrm{T}_{P_\pm}(S_h) = \tau_{P_\pm}^{-1}(S'_h) \;=\; \pm 2(x+t)y - h_1 z^2.$$

Thus we proved

Lemma 5. *If $\big(\frac{N_h}{p}\big) = -1$, then $pr \colon U(\mathbb{F}_p) \xrightarrow{\sim} V(\mathbb{F}_p)$, where*

$$U(\mathbb{F}_p) = S_h(\mathbb{F}_p) \setminus \mathbb{V}(y), \qquad V(\mathbb{F}_p) = \mathbb{A}^2(\mathbb{F}_p) \setminus \mathbb{V}(Y).$$

We are also interested in the involution

$$[-1] \colon S_h \xrightarrow{\sim} S_h, \qquad (x:y:z:t) \mapsto (x:y:-z:t),$$

the meaning of which is explained in Remark 2. Let $P \in S_h \setminus \mathrm{T}_\infty(S_h)$ be a point outside the tangent plane

$$\mathrm{T}_\infty(S_h) = h_1 t + h_0 y \qquad \text{at} \qquad \infty := (0:0:1:0) \in S_h.$$

In geometric terms the point $[-1](P)$ is the third intersection one of the surface S_h and the line $L_{\infty,P}$ passing through ∞ and P (see also [44, prop. II.12.13]). In other words,

$$S_h \cdot L_{\infty,P} = \infty + P + [-1](P).$$

1.2 Elliptic curves E_b (of j-invariant 0)

Consider a finite field $\mathbb{F}_q$, where $q = p^e$, $e \in \mathbb{N}$, and p (>3) is a prime. In this paragraph we review elliptic curves $\overline{E_b} \subset \mathbb{P}^2$ (of $j = 0$) given by the affine model

$$E_b\colon y^2 = x^3 + b \quad \subset \quad \mathbb{A}^2_{(x,y)}$$

for $b \in \mathbb{F}_q^*$. In other words, $\overline{E_b} = E_b \cup \{\mathcal{O}\}$, where $\mathcal{O} := (0 : 1 : 0)$. Unless otherwise specified we will identify E_b and $\overline{E_b}$ for the sake of simplicity. Curves E_b are discussed, for example, in [28]. They have the order 3 automorphism

$$[\omega]\colon E_b \xrightarrow{\sim} E_b, \qquad (x, y) \mapsto (\zeta_3 x, y)$$

with fixed point set

$$\mathrm{Fix}([\omega]) = \big\{\mathcal{O}, (0, \pm\sqrt{b})\big\}.$$

Let us recall some well known results.

Theorem 3 ([55, exam. V.4.4]). *A curve E_b is ordinary if and only if $p \equiv 1 \pmod 3$.*

Hereafter we will assume this condition, because results of the article have immediate applications only for discrete logarithm cryptography, where supersingular elliptic curves are weak.

Theorem 4 ([45, prop. 1.50], [45, exam. 1.112]).

1. *Curves E_b are isomorphic to each other at most over $\mathbb{F}_{q^6}$ by the map*

   $$\varphi_{b,b'}\colon E_b \xrightarrow{\sim} E_{b'}, \qquad (x, y) \mapsto (\sqrt[3]{\beta}x, \sqrt{\beta}y),$$

   where $\beta := b'/b$. Besides, for $\alpha \in \mathbb{F}_q$ such that $\alpha \notin (\mathbb{F}_q^*)^2$, $\alpha \notin (\mathbb{F}_q^*)^3$ the curves E_{α^i} ($i \in \mathbb{Z}/6$) are unique ones of $j = 0$ (up to an $\mathbb{F}_q$-isomorphism).

2. *The endomorphism ring of curves E_b (and only of them) is that of Eisenstein integers:*

   $$\mathrm{End}(E_b) \simeq \mathbb{Z}[\omega] \ \subset \ \mathbb{Q}(\sqrt{-3}),$$

   where $\omega = \sqrt[3]{1} \in \mathbb{C}^*$ corresponds to the automorphism $[\omega]$. In particular,

   $$\mathrm{Aut}(E_b) \simeq \langle -\omega \rangle \simeq \mathbb{Z}/6.$$

Let us recall some things about the ring of Eisenstein integers. First, there is the unique decomposition $p = \pi\overline{\pi}$ such that $\pi = n + m\omega$ is a prime in $\mathbb{Z}[\omega]$ and $\pi \equiv 2 \pmod 3$. Besides, for a number $a \in \mathbb{Z}[\omega] \setminus (\pi)$ its 6-th power residue symbol $\left(\frac{a}{\pi}\right)_6$ is, by definition, the 6-th root of unity that is congruent to $a^{\frac{p-1}{6}}$ modulo π. We will denote by t_q (by f_q) trace (respectively conductor) of the Frobenius map $\pi_q = \pi^e$ on $E_b/\mathbb{F}_q$. In other words, f_q is conductor of the order $\mathbb{Z}[\pi_q] \subset \mathbb{Z}[\omega]$. In particular,

$$t_q^2 - 4q = -3f_q^2 \qquad \text{and hence} \qquad \pi_q, \overline{\pi_q} = \frac{t_q \pm f_q\sqrt{-3}}{2},$$

where $\overline{\pi_q} = \overline{\pi}^e$ is the Verschiebung map on $E_b/\mathbb{F}_q$. Finally, let

$$n_b := |E_b(\mathbb{F}_q)| = q + 1 - t_q.$$

Theorem 5 ([28, thm 2], [45, prop. 1.57])**.**

1. *For $q = p$ we obtain:*

$$t_p = -\overline{\left(\frac{4b}{\pi}\right)_6}\pi - \left(\frac{4b}{\pi}\right)_6\overline{\pi} \quad \in \quad \Big\{\pm(n+m),\ \pm(2n-m),\ \pm(n-2m)\Big\}.$$

2. *If $E_{b'}$ is a twist of E_b of degree d, then its trace is equal to*

$$t'_q = \begin{cases} -t_q & \text{if} \quad d = 2, \\ \dfrac{\pm 3f_q - t_q}{2} & \text{if} \quad d = 3, \\ \dfrac{\pm 3f_q + t_q}{2} & \text{if} \quad d = 6. \end{cases}$$

Moreover, for any curve E_b all cases occur.

Consequently, applying both parts of this theorem, we can immediately compute the trace t_q (and then the order n_b) of any curve $E_b/\mathbb{F}_q$.

Theorem 6 ([27, thm 9])**.** *Let α be as in Theorem 4. If $2, 3 \nmid n_b$, then*

$$E_b(\mathbb{F}_{q^6}) \simeq \bigoplus_{i \in \mathbb{Z}/6} E_{\alpha^i}(\mathbb{F}_q).$$

Moreover, if $\mathbb{F}_q(E_b[\ell]) = \mathbb{F}_{q^6}$ for some prime $\ell \mid n_b$, then E_b has the unique sextic twist $E_{b'}/\mathbb{F}_q$ such that $\ell \mid n_{b'}$. In other words,

$$E_b[\ell] = E_b(\mathbb{F}_q)[\ell] \times \varphi_{b,b'}^{-1}(G), \qquad \textit{where} \qquad G := E_{b'}(\mathbb{F}_q)[\ell].$$

1.2.1 The Weil restriction of $E_b/\mathbb{F}_{p^2}$

For simplicity suppose $p \equiv 3 \pmod 4$, i.e., $i := \sqrt{-1} \notin \mathbb{F}_p$. Also, let $b := b_0 + b_1 i$ and $N_b := b_0^2 + b_1^2$ for some $b_0, b_1 \in \mathbb{F}_p$. Then the Weil restriction [23, §3.2] of $E_b \subset \mathbb{A}^2_{(x,y)}$ (with respect to the extension $\mathbb{F}_{p^2}/\mathbb{F}_p$) is equal to

$$R_b := \begin{cases} y_0^2 - y_1^2 = x_0^3 - 3x_0x_1^2 + b_0, \\ 2y_0y_1 = -x_1^3 + 3x_0^2x_1 + b_1 \end{cases} \subset \quad \mathbb{A}^4_{(x_0,x_1,y_0,y_1)}.$$

Further, we denote by $\overline{R_b} \hookrightarrow \mathbb{P}^8$ the Weil restriction of $\overline{E_b} \subset \mathbb{P}^2$, recalling that $\overline{R_b} \simeq \overline{E_b} \times \overline{E_{b^p}}$ over $\mathbb{F}_{p^2}$. Also consider the restriction of $[\omega]$, i.e., the order 3 automorphism

$$[\omega]_2\colon R_b \xrightarrow{\sim} R_b, \qquad (x_0, x_1, y_0, y_1) \mapsto (\zeta_3 x_0, \zeta_3 x_1, y_0, y_1).$$

If $b_1 \neq 0$, then its fixed point set

$$\mathrm{Fix}([\omega]_2) = \Big\{(0, 0, y_0, y_1) \ \big|\ 2y_0y_1 = b_1,\ 2y_0^2 = b_0 \pm \sqrt{N_b}\Big\}.$$

Over $\overline{\mathbb{F}_p}$ it obviously consists of exactly 4 points, and besides, $\mathrm{Fix}([\omega]_2)(\mathbb{F}_p) = \emptyset$ if and only if $\left(\frac{b}{p^2}\right) = -1$. At the same time, the continuation $[\omega]_2\colon \overline{R_b} \xrightarrow{\sim} \overline{R_b}$ has exactly 9 fixed $\overline{\mathbb{F}_p}$-points. The similar analysis can be carried out for the involution

$$[-1]\colon R_b \xrightarrow{\sim} R_b, \qquad (x_0, x_1, y_0, y_1) \mapsto (x_0, x_1, -y_0, -y_1).$$

1.3 Generalized Kummer surfaces

Let A be an abelian surface over a perfect field k of characteristic p and σ be its automorphism as a group variety. The quotient A/σ (or its minimal resolution of singularities) is called *generalized Kummer surface*. The theory of geometric quotients is well represented in [48]. For $\sigma = [-1]$ this is just *Kummer surface* K_A. Besides, we will denote by $\varrho\colon A \to A/\sigma$ the quotient morphism (of degree $\mathrm{ord}(\sigma)$).

Let us recall some rationality properties of generalized Kummer surfaces.

Theorem 7 ([37, thm A], [38, thm 1.3])**.** *For $k = \overline{k}$ we obtain:*

1. *If $p > 2$, $p \not\equiv 1 \pmod{12}$, then A is supersingular $\Leftrightarrow$ K_A is a Zariski surface* [61];
2. *If $p = 2$, then A is supersingular $\Leftrightarrow$ K_A is a rational surface.*

Theorem 8 ([24, table 6], [60, §2])**.** *For $k = \mathbb{C}$ there are only two abelian surfaces having σ of a prime order such that the generalized Kummer surface is rational. These are:*

1. *The direct square E_1^2 with $\sigma = ([\omega], [\omega])$ of order 3;*
2. *The Jacobian J_1 of the genus 2 curve given by the affine model $y^2 = x^5 + 1$ with σ (of order 5) induced from the curve automorphism $(x, y) \mapsto (x\sqrt[5]{1}, y)$.*

In fact, J_1 is the unique simple abelian surface A having σ with the rational quotient A/σ even if we omit the prime condition on $\mathrm{ord}(\sigma)$.

Theorem 9 ([36, thm 2.11])**.** *Assume that $k = \overline{k}$, $\dim\big(\mathrm{Fix}(\sigma)\big) = 0$, and at least one of singularities on A/σ is not a node. Then A/σ is a rational surface.*

Recently, a sort of classification for automorphism groups of abelian surfaces over a finite field $\mathbb{F}_q$ appeared in [29]. Nevertheless, almost nothing is known about $\mathbb{F}_q$-rationality of generalized Kummer surfaces unlike their $\overline{\mathbb{F}_q}$-unirationality in some cases (see [36]). This article can be considered the first step in this direction.

1.3.1 The generalized Kummer surfaces GK_b

We keep the notation of §1.2.1. Consider the generalized Kummer surface $\overline{GK_b} := \overline{R_b}/[\omega]_2$ and its open subset $GK_b := R_b/[\omega]_2$. Besides, we will need the polynomials

$$\alpha(t) := 3t^2 - 1, \qquad \beta(t) := t(t^2 - 3), \qquad f(t) \ := \ -b_0\alpha(t) + b_1\beta(t) \ = \ b_1t^3 - 3b_0t^2 - 3b_1t + b_0.$$

Note that the discriminant of f/b_1 is equal to $\Delta = 2^2 3^3 N_b^2/b_1^4$ and hence $\left(\frac{\Delta}{p}\right) = -1$. By Lemma 1 there is the decomposition $f = \lambda\gamma$ into linear λ and $\mathbb{F}_p$-irreducible quadratic γ polynomials over $\mathbb{F}_q$. For uniqueness we suppose γ to be reduced. This decomposition (or, equivalently, the unique $\mathbb{F}_p$-root of f) can be found, for example, by means of Theorem 2.

Theorem 10. *There is the affine model*

$$GK_b = \alpha(t)(y_0^2 - y_1^2) - 2\beta(t)y_0y_1 + f(t) \quad \subset \quad \mathbb{A}^3_{(t,y_0,y_1)}$$

for which the corresponding quotient map has the form

$$\varrho\colon R_b \dashrightarrow GK_b, \qquad (x_0, x_1, y_0, y_1) \mapsto \Big(\frac{x_0}{x_1}, y_0, y_1\Big).$$

Proof. It is well known that $\mathbb{F}_p(GK_b) = \mathbb{F}_p(R_b)^{[\omega]_2}$, that is rational functions on GK_b are $[\omega]_2$-invariant ones on R_b. Also, consider the field

$$F := \mathbb{F}_p(t, y_0, y_1) \subset \mathbb{F}_p(GK_b), \qquad \text{where} \qquad t := \frac{x_0}{x_1}.$$

Note that $F(x_1) = \mathbb{F}_p(R_b)$, because $x_0 = tx_1$. Since $x_1^3 = (2y_0y_1 - b_1)/\alpha(t)$, the extension degree $[\mathbb{F}_p(R_b) : F] \leqslant 3$. At the same time, $[\mathbb{F}_p(R_b) : \mathbb{F}_p(GK_b)] = 3$ according to the Artin theorem from the Galois theory. Thus $F = \mathbb{F}_p(GK_b)$. Finally, looking at the equations of R_b and the equalities

$$\frac{y_0^2 - y_1^2 - b_0}{2y_0y_1 - b_1} = \frac{x_0^3 - 3x_0x_1^2}{-x_1^3 + 3x_0^2x_1} = \frac{(x_0^3 - 3x_0x_1^2)/x_1^3}{(-x_1^3 + 3x_0^2x_1)/x_1^3} = \frac{\beta(t)}{\alpha(t)},$$

we obtain the aforementioned equation for GK_b. There are no another dependencies between the coordinates t, y_0, y_1, because GK_b is a surface. □

It is known [56, exam. 8.10] that the image of $\mathrm{Fix}([\omega]_2) \subset \overline{R_b}$ under ϱ is the singular locus of $\overline{GK_b}$ and all its 9 singularities are cyclic quotient ones of type $\frac{1}{3}(1,1)$. Later it will be more practical to consider the closure GK_b in $\mathbb{A}^1_t \times \mathbb{P}^2_{(y_0:y_1:y_2)}$, keeping the same notation. In this case the quotient map takes the form

$$\varrho\colon R_b \dashrightarrow GK_b, \qquad (x_0, x_1, y_0, y_1) \mapsto \Big(\frac{x_0}{x_1}, (y_0 : y_1 : 1)\Big).$$

An inverse image of ϱ is represented, for example, as

$$\big(t, (y_0 : y_1 : y_2)\big) \mapsto \big(tX_1, X_1, Y_0, Y_1\big),$$

where

$$X_1 := \sqrt[3]{\frac{2Y_0Y_1 - b_1}{\alpha(t)}}, \qquad Y_0 := \frac{y_0}{y_2}, \qquad Y_1 := \frac{y_1}{y_2}.$$

In other words, these formulas give the map ϱ^{-1} from GK_b to the set-theoretic quotient of R_b by $[\omega]_2$.

1.4 Conic bundles (conics over the function field)

In this paragraph we will recall some facts about conic bundles. For a deeper look, see [31], [32]. Let $(x_0 : x_1)$ be homogenous coordinates of $\mathbb{P}^1$ and $t := x_0/x_1$. As usual, we denote a point $(t_0 : 1)$ just by t_0 and the point $(1 : 0)$ by ∞.

Consider a projective irreducible (possibly singular) surface S over a finite field $\mathbb{F}_q$ of characteristic $p > 2$. We call a non-constant $\mathbb{F}_p$-morphism $\pi\colon S \to \mathbb{P}^1$ *conic bundle* if for general $t_0 \in \mathbb{P}^1$ the fibre $\pi^{-1}(t_0)$ is a non-degenerate conic. The latter means an irreducible (or, equivalently, non-singular) algebraic curve $\big($over $\mathbb{F}_q(t_0)\big)$ of degree 2. As usually, a $\mathbb{F}_q$-section of π is a $\mathbb{F}_q$-morphism $\sigma\colon \mathbb{P}^1 \to S$ such that $\pi \circ \sigma = \mathrm{id}$.

It is clear that π corresponds to its general fibre F_π, which is a non-degenerate conic over the univariate function field $\mathbb{F}_q(t)$. And besides, $\mathbb{F}_q$-sections of π correspond to $\mathbb{F}_q(t)$-points on F_π. For one another conic bundle $\pi'\colon S' \to \mathbb{P}^1$ any birational $\mathbb{F}_q$-isomorphism $\varphi\colon S \overset{\sim}{\dashrightarrow} S'$

(such that $\pi = \pi' \circ \varphi$) corresponds to an $\mathbb{F}_q(t)$-isomorphism (i.e., a transformation in $\mathbb{P}^2$) of their general fibers $\varphi_{\pi,\pi'}\colon F_\pi \xrightarrow{\sim} F_{\pi'}$, and vice versa. If the general fibre F_π is *isotropic*, i.e., it has $\mathbb{F}_q(t)$-point, then S is obviously an $\mathbb{F}_q$-rational surface. Inverse is not true (see, for example, Theorem 14).

Suppose S to be a non-singular surface. A conic bundle π is called *relatively* $\mathbb{F}_q$*-minimal* if S has no $\mathbb{F}_q$-orbits of pairwise disjoint exceptional (-1)-curves in fibers of π. In other words, the surface S can not be contracted over $\mathbb{F}_q$ with respect to π. A conic bundle may have several relatively $\mathbb{F}_q$-minimal models, however the Frobenius action on each of them is the same.

Theorem 11 (Iskovskih)**.** *Suppose $\pi\colon S \to \mathbb{P}^1$ to be a relatively $\mathbb{F}_q$-minimal conic bundle. Then we obtain:*

1. *The number of degenerate fibres of π (over $\overline{\mathbb{F}_q}$) is equal to $8 - K^2$, where K is a canonical divisor of S;*

2. *The surface S is $\mathbb{F}_q$-rational if and only if $K^2 \geqslant 5$, i.e., there is no more than 3 degenerate fibers.*

3. *If $K^2 \in \{5, 6\}$, then S is a del Pezzo surface. Moreover, S is unique among all relatively $\mathbb{F}_q$-minimal conic bundles of degree K^2.*

It is well known that every surface having conic bundle can be reduced by means of some birational $\mathbb{F}_q$-isomorphism to the form

$$S = F(x_0, x_1)y_0^2 + G(x_0, x_1)y_1^2 + H(x_0, x_1)y_2^2 \quad \subset \quad \mathbb{P}^1_{(x_0:x_1)} \times \mathbb{P}^2_{(y_0:y_1:y_2)},$$

where F, G, H are non-zero homogenous $\mathbb{F}_q$-polynomials of the same degree. The conic bundle itself is transformed into the projection $\pi\colon S \to \mathbb{P}^1_{(x_0:x_1)}$. The product $\Delta := FGH$ is called *discriminant* of π. After a simple check we obtain

Lemma 6. *For $t_0 \in \mathbb{P}^1$ the following is true:*

1. *The fibre of π over t_0 is degenerate $\Leftrightarrow \Delta(t_0) = 0$;*

2. *The fibre of π over t_0 contains a singular point on $S \Leftrightarrow t_0$ is a multiple root of Δ;*

3. *Singular curves on S may only be double fibers of π.*

Further, it is clear that the surface S has the non-singular $\mathbb{F}_q$-model

$$S_{f,g,h} := f(t)y_0^2 + g(t)y_1^2 + h(t)y_2^2 \quad \subset \quad \mathbb{A}^1_t \times \mathbb{P}^2_{(y_0:y_1:y_2)},$$

where f, g, h are non-zero (possibly $\mathbb{F}_q$-reducible) square-free polynomials having no common roots in pairs. We will also call the projection $S_{f,g,h} \to \mathbb{A}^1_t$ (induced from π) a conic bundle despite the fact that $S_{f,g,h}$ is not a projective surface. Thus its general fibre can be written as

$$Q_{\alpha,\beta} := y_0^2 + \alpha(t)y_1^2 + \beta(t)y_2^2, \qquad \text{where} \qquad \alpha(t) := \frac{g(t)}{f(t)}, \qquad \beta(t) := \frac{h(t)}{f(t)}.$$

Lemma 7 ([49, thm 3.7]). *The conic bundle $S_{f,g,h} \to \mathbb{A}^1_t$ has an $\mathbb{F}_q$-section if and only if the following identities on the Legendre symbols are satisfied:*

$$\left(\frac{-fg}{h}\right) = \left(\frac{-fh}{g}\right) = \left(\frac{-gh}{f}\right) = 1.$$

A quite efficient algorithm for finding an $\mathbb{F}_q$-section of a conic bundle can be found, for example, in [57].

We recall that for functions $\alpha, \beta \in \mathbb{F}_q(t)^*$ their (*quadratic*) *Hilbert symbol at* $t_0 \in \mathbb{P}^1$ is the Legendre one

$$(\alpha, \beta)_{t_0} := \left(\frac{e(\alpha, \beta)}{\mathbb{F}_q(t_0)}\right), \qquad \text{where} \qquad e(\alpha, \beta) := (-1)^{ab}\frac{\alpha^b}{\beta^a}(t_0) \ \in \ \mathbb{F}_q(t_0)^*$$

and a, b are orders at t_0 of α, β respectively. The following theorem is very useful despite the fact that it is not constructive.

Theorem 12 ([31, exam. 3.7]). *Fix two more functions $\alpha', \beta' \in \mathbb{F}_q(t)^*$. Then the conics $Q_{\alpha,\beta}$, $Q_{\alpha',\beta'}$ are $\mathbb{F}_q(t)$-isomorphic if and only if for all $t_0 \in \mathbb{P}^1$ we have that $(\alpha, \beta)_{t_0} = (\alpha', \beta')_{t_0}$.*

1.4.1 A conic bundle on S_h

We save the notation of §1.1.2. In §2 we will encounter the projection $\pi\colon S_h \to \mathbb{P}^1_{(y:t)}$ from the line L_∞, which is a conic bundle. The surfaces S_h and

$$S'_h := x^2 - (t^2+1)y^2 - (h_1 t + h_0)z^2 \quad \subset \quad \mathbb{A}^1_t \times \mathbb{P}^2_{(x:y:z)}$$

are obviously equal for $y \neq 0$ on both ones. Moreover, after inducing the maps $\pi, pr, [-1]$ on S'_h they respectively become the projection $\pi'\colon S'_h \to \mathbb{A}^1_t$,

$$pr'\colon S'_h \overset{\sim}{\dashrightarrow} \mathbb{A}^2_{(u,v)}, \qquad \big(t, (x:y:z)\big) \mapsto \left(\pm\frac{x}{y} - t, \frac{z}{y}\right),$$

and

$$[-1]\colon S'_h \overset{\sim}{\to} S'_h, \qquad \big(t, (x:y:z)\big) \mapsto \big(t, (x:y:-z)\big).$$

Besides,

$$(pr')^{-1}\colon \mathbb{A}^2_{(u,v)} \overset{\sim}{\dashrightarrow} S'_h, \qquad (u,v) \mapsto \left(\frac{T}{Y}, \big(\pm(uY+T) : Y : vY\big)\right),$$

where

$$Y := h_1 v^2 - 2u, \qquad T := u^2 - h_0 v^2 - 1.$$

For compactness we will sometimes use the notation $g(t) := t^2 + 1$.

Lemma 8. *Suppose $p \equiv 3 \pmod 4$. Then the conic bundle π' has an $\mathbb{F}_p$-section $\Leftrightarrow \left(\frac{N_h}{p}\right) = 1$.*

Proof. According to Lemma 7 there is an $\mathbb{F}_p$-section for π' if and only if

$$\left(\frac{g}{h}\right) = \left(\frac{h}{g}\right) = \left(\frac{-gh}{1}\right) = 1.$$

The last equality is obviously true. Also, note that

$$\left(\frac{g}{h}\right) = \left(\frac{g(h_0/h_1)}{p}\right) = \left(\frac{N_h}{p}\right).$$

Finally, the second equality is, by definition, the existence of an $\mathbb{F}_p$-polynomial $r(t) = r_1 t + r_0$ such that $g \mid h - r^2$. The remainder of dividing $h - r^2$ by g is equal to

$$(h_1 - 2r_0 r_1)t + (h_0 - r_0^2 + r_1^2),$$

hence we obtain the equation system

$$\begin{cases} r_0 = \dfrac{h_1}{2r_1}, \\ 4r_1^4 + 4h_0 r_1^2 - h_1^2 = 0. \end{cases}$$

Therefore $r_1^2 = R_\pm$, where

$$R_\pm := \frac{-h_0 \pm \sqrt{N_h}}{2}, \qquad R_+ R_- = -\frac{h_1^2}{4}.$$

If $\left(\frac{N_h}{p}\right) = 1$, then the above system is solvable. Indeed, $R_\pm \in \mathbb{F}_p$ and exactly one of these elements is a quadratic residue in $\mathbb{F}_p$. $\square$

Provided $\left(\frac{N_h}{p}\right) = -1$ we see that $pr' \colon U(\mathbb{F}_p) \rightsquigarrow V(\mathbb{F}_p)$ by analogy with Lemma 5. For the next theorem consider the lines

$$L_\pm := h_1 x \pm y\sqrt{N_h}, \qquad M_\pm := x - z\sqrt{h(\pm i)}, \qquad M_\pm^{(1)} = x + z\sqrt{h(\pm i)}.$$

Theorem 13. *If* $\left(\frac{N_h}{p}\right) = -1$, *then:*

1. *The degenerate fibers of* π' *over* $t \neq \infty$ *are represented in Figure* 1;
2. *The fibre of* π' *over* ∞ *is the double one with the unique surface singular point* $(1:0:0)$, *which is of type* A_3;
3. *The relatively* $\mathbb{F}_p$*-minimal model of* S'_h *is a del Pezzo surface of degree* 5.

Proof. The first fact is immediately checked. To prove the second one we write out the surface S'_h (locally over $\overline{\mathbb{F}_p}$) as

$$s^2 - (1+s^2)y^2 - (1 + \frac{h_0}{h_1}s)sz^2 \quad \subset \quad \mathbb{A}^3_{(y,z,s)}.$$

To obtain the surface $\mathbb{V}(s^2 + y^2 + z^4)$ it remains to apply the analytical change of variables

$$(y,z,s) \mapsto \left(Ay, Bz, s + \frac{(Bz)^2}{2}\right),$$

where

$$A = \sqrt{-(1+s^2)}, \quad B = \sqrt{-(1 + \frac{h_0}{h_1}s)} \quad \in \quad \overline{\mathbb{F}_p}[[s]].$$

Finally, the third fact follows from the Iskovskih theorem 11 and $\mathbb{F}_p$-rationality of S_h (see Lemma 4). $\square$

Hereafter we will identify (S_h, π, pr) and (S'_h, π', pr'), saving for simplicity only the first notation.

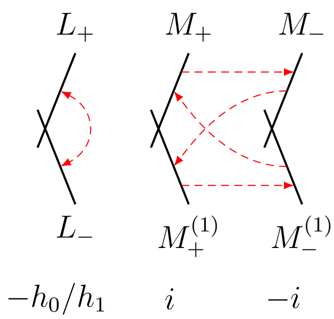

Figure 1: The Frobenius action on degenerate fibers of the conic bundle $\pi'\colon S'_h \to \mathbb{A}^1_t$

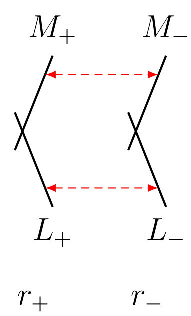

Figure 2: Pairs of $\mathbb{F}_p$-conjugate lines lying in two $\mathbb{F}_p$-conjugate degenerate fibers

1.4.2 Blowing down components of degenerate fibres

According to [31, §3] we have explicit formulas for contracting one of $\mathbb{F}_p$-lines of a degenerate $\mathbb{F}_p$-fibre. We will also need to explicitly contract one of the pairs of $\mathbb{F}_p$-conjugate lines $L_\pm$ (or $M_\pm$) lying in two $\mathbb{F}_p$-conjugate degenerate fibers over roots $r_\pm$ of some $\mathbb{F}_p$-irreducible quadratic polynomial. This is done in Lemma 9 in a particular case, which is sufficient for our purposes. For better comprehension of the described situation see Figure 2.

For any polynomial $h \in \mathbb{F}_p[t]$ consider the surface

$$S_h := x^2 - (t^2+1)y^2 - h(t)z^2 \quad \subset \quad \mathbb{A}^1_t \times \mathbb{P}^2_{(x:y:z)}.$$

As usual, the projection $\pi\colon S_h \to \mathbb{A}^1_t$ is a conic bundle.

Lemma 9. *Let $q(t) := t^2 + ct + d \in \mathbb{F}_p[t]$ with roots $r_\pm$ and discriminant $D = c^2 - 4d$ such that $\left(\frac{D}{p}\right) = -1$. Also, let $h \in \mathbb{F}_p[t]$ and $s_\pm := r_\pm^2 + 1$ provided that $q \mid h$ and $\left(\frac{s_\pm}{p^2}\right) = 1$. Then for some $u \in \mathbb{F}_p^*$ there is a birational $\mathbb{F}_p$-isomorphism (respecting the conic bundles)*

$$\varphi_q\colon S_h \overset{\sim}{\dashrightarrow} S_{u\frac{h}{q}} \qquad \textit{such that} \qquad \varphi_q\colon S_h(\mathbb{F}_p) \rightsquigarrow S_{u\frac{h}{q}}(\mathbb{F}_p).$$

Proof. We propose to start the searching a desired transformation in the form

$$\psi_q := \begin{cases} x_2 := (b_0 + b_1 t)x - y, \\ y_2 := -x + (a_0 + a_1 t)y, \\ z_2 := a_1 b_1 q(t) z, \end{cases} \qquad \psi_q^{-1} = \begin{cases} x := (a_0 + a_1 t)x_2 + y_2, \\ y := x_2 + (b_0 + b_1 t)y_2, \\ z := z_2, \end{cases} \qquad \det(\psi_q^{-1}) = a_1 b_1 q(t),$$

where $a_0, b_0 \in \mathbb{F}_p$, $a_1, b_1 \in \mathbb{F}_p^*$. After substitution ψ_q^{-1} into S_h and division by $q(t)$ the coefficients of the monomials x_2^2, x_2y_2, y_2^2 we obtain (up to a non-zero constant) the remainders

$$\begin{aligned}
&(a_0^2 - a_1^2 d + d - 1)x_2^2, && (2a_0a_1 - a_1^2 c + c)x_2^2 t, \\
&(a_0 + b_0 d - b_0 - b_1 cd)x_2y_2, && \big(a_1 + b_0 c - b_1(c^2 - d + 1)\big)x_2y_2t, \\
&\big(db_0^2 - b_0^2 - 2cdb_0b_1 + d(c^2 - d + 1)b_1^2 + 1\big)y_2^2, && \big(cb_0^2 - 2(c^2 - d + 1)b_0b_1 + c(c^2 - 2d + 1)b_1^2\big)y_2^2 t
\end{aligned}$$

and the non-zero quotients ux_2^2, $v(t)x_2y_2$, $w(t)y_2^2$, where

$$\begin{aligned}
&u := a_1^2 - 1,\\
&v(t) := 2(-b_1t + b_1c - b_0),\\
&w(t) := -b_1^2t^2 + b_1(-2b_0 + b_1c)t - b_0^2 + 2b_0b_1c - b_1^2(c^2 - d + 1).
\end{aligned}$$

Consider the trace and norm:

$$T := \mathrm{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(s_\pm) = c^2 - 2d + 2, \qquad N := \mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(s_\pm) = c^2 + d^2 - 2d + 1.$$

Because of $\left(\frac{s_\pm}{p^2}\right) = 1$ we get $\left(\frac{N}{p}\right) = 1$. Also, it is easily checked that $T^2 - c^2D = 4N$. The system of reminders has two $\mathbb{F}_p$-solutions:

$$a_0 := c\frac{(d+1)Nb_1^2 + 1 - d}{2Nb_1}, \qquad a_1 := \frac{TNb_1^2 - c^2}{2Nb_1}, \qquad b_0 := c\frac{Nb_1^2 + 1}{2Nb_1}, \qquad b_1 := \pm\sqrt{\beta},$$

where β is exactly one (due to $\left(\frac{D}{p}\right) = -1$) of the roots

$$\frac{T \pm 2\sqrt{N}}{ND} \in \mathbb{F}_{p^*} \qquad \text{of} \qquad DN^2X^2 - 2TNX + c^2 \in \mathbb{F}_p[X]$$

such that $\left(\frac{\beta}{p}\right) = 1$. Therefore

$$\psi_q \colon S_h \xrightarrow{\sim} S', \qquad \text{where} \qquad S' := ux_2^2 + v(t)x_2y_2 + w(t)y_2^2 - \frac{h(t)}{q(t)}z_2^2.$$

Note that $u, a_1 \neq 0$. Thus after the $\mathbb{F}_p$-transformation $\chi_q \colon S' \xrightarrow{\sim} S_{u\frac{h}{q}}$ given by

$$\chi_q := \begin{cases} x_3 := ux_2 + \dfrac{v(t)}{2}y_2,\\ y_3 := a_1b_1y_2,\\ z_3 := z_2, \end{cases} \qquad \chi_q^{-1} = \begin{cases} x_2 := \dfrac{a_1b_1}{u}x_3 - \dfrac{v(t)}{2u}y_3,\\ y_2 := y_3,\\ z_2 := a_1b_1z_3, \end{cases} \qquad \det(\chi_q) = ua_1b_1$$

we obtain the desired surface $S_{u\frac{h}{q}}$, i.e., $\varphi_q := \chi_q \circ \psi_q$ satisfies the theorem conditions. $\square$

Under the conditions of this lemma as the lines of Figure 2 we can take

$$L_\pm = x - \sqrt{s_\pm}y, \qquad M_\pm = x + \sqrt{s_\pm}y.$$

In the following corollary $L_+ = L_-$ (resp. $M_+ = M_-$).

Corollary 1. *If $c = 0$ and $d \neq 1$ in the previous lemma, then the condition $\left(\frac{s_\pm}{p^2}\right) = 1$ is fulfilled. Thus, letting $\delta := \sqrt{d(d-1)}$, we obtain:*

$$u = -\frac{1}{d}, \qquad v(t) = \mp\frac{2t}{\delta}, \qquad w(t) = -\frac{t^2 - d + 1}{\delta^2}$$

(in particular, $\left(\frac{u}{p}\right) = -1$) and (up to multiplication by elements of $\mathbb{F}_p^*$)

$$\psi_q = \begin{cases} x_2 := \pm\dfrac{t}{\delta}x - y, \\ y_2 := -x \mp \dfrac{(d-1)t}{\delta}y, \\ z_2 := -\dfrac{q(t)}{d}z, \end{cases} \qquad \psi_q^{-1} = \begin{cases} x := \mp\dfrac{(d-1)t}{\delta}x_2 + y_2, \\ y := x_2 \pm \dfrac{t}{\delta}y_2, \\ z := z_2, \end{cases}$$

$$\chi_q = \begin{cases} x_3 := x_2 \pm \dfrac{dt}{\delta}y_2, \\ y_3 := y_2, \\ z_3 := -dz_2, \end{cases} \qquad \chi_q^{-1} = \begin{cases} x_2 := x_3 \mp \dfrac{dt}{\delta}y_3, \\ y_2 := y_3, \\ z_2 := -\dfrac{1}{d}z_3. \end{cases}$$

Proof. It is immediately checked that

$$s_+ = s_- = 1-d, \qquad D = -4d, \qquad T = -2(d-1), \qquad N = (d-1)^2, \qquad \beta = \frac{1}{\delta^2}$$

and all other values are as stated. □

2 New point compression method

We will freely use notation of previous paragraphs. As early, p be a prime such that $p \equiv 1 \pmod 3$, $p \equiv 3 \pmod 4$. Consider the following ordinary elliptic $\mathbb{F}_{p^2}$-curve, its Weil restriction (with respect to $\mathbb{F}_{p^2}/\mathbb{F}_p$), and the generalized Kummer $\mathbb{F}_p$-surface respectively:

$$E_b \subset \mathbb{A}^2_{(x:y)}, \qquad R_b \subset \mathbb{A}^4_{(x_0,x_1,y_0,y_1)}, \qquad GK_b \subset \mathbb{A}^1_t \times \mathbb{P}^2_{(y_0:y_1:y_2)}.$$

Note that the projection $\pi\colon GK_b \to \mathbb{A}^1_t$ is a conic bundle. In this paragraph we prove $\mathbb{F}_p$-rationality of GK_b, which leads to the creation of our compression method for $\mathbb{F}_{p^2}$-points of E_b. We also discuss some technical details of its implementation.

Remark 1. *If $\sqrt{b} = a_0 + a_1 i$ for some $a_0, a_1 \in \mathbb{F}_p$, then the general fibre of π contains the point $(a_0 : a_1 : 1)$ and the projection from it obviously gives a birational $\mathbb{F}_p$-isomorphism between GK_b and $\mathbb{A}^2$. In fact, this case does not happen in pairing-based cryptography, otherwise by Theorem 4 the curve E_b would not be a sextic $\mathbb{F}_{p^2}$-twist for any initial $\mathbb{F}_p$-curve $E_{b'}$. Thus we can always assume that $\left(\frac{b}{p^2}\right) = -1$, in particular $b_0, b_1 \neq 0$.*

First, we reduce GK_b to a diagonal form by the map $\sigma\colon GK_b \dashrightarrow S_{\alpha f}$ given by

$$\sigma := \begin{cases} x := \beta(t)y_0 + \alpha(t)y_1, \\ y := g(t)y_0, \\ z := y_2, \end{cases} \qquad \sigma^{-1} = \begin{cases} y_0 := \alpha(t)y, \\ y_1 := g(t)x - \beta(t)y, \\ y_2 := \alpha(t)g(t)z, \end{cases} \qquad \det(\sigma) = \alpha(t)g(t).$$

In particular, σ respects the conic bundle π and $\sigma\colon GK_b(\mathbb{F}_p) \simeq S_{\alpha f}(\mathbb{F}_p)$. Next we successively apply Corollary 1 and Lemma 9 to contract pairs of $\mathbb{F}_p$-conjugate lines lying in the fibres of π over roots of the $\mathbb{F}_p$-irreducible polynomials α, γ respectively. More precisely, this is done by means of the maps

$$\varphi_{\alpha/3}\colon S_{\alpha f} \dashrightarrow S_{9f}, \qquad \varphi_\gamma\colon S_{9f} \dashrightarrow S_h,$$

where $h(t) = 9u\lambda(t)$ for some $u \in \mathbb{F}_p^*$. The cubic surface S_h is $\mathbb{F}_p$-rational by the projection pr from any of its two nodes (see Lemma 4). Thus we obtain the maps

$$\theta := \varphi_\gamma \circ \varphi_{\alpha/3} \circ \sigma \colon GK_b \xrightarrow{\simeq} S_h, \qquad \tau := pr \circ \theta \colon GK_b \xrightarrow{\simeq} \mathbb{A}^2,$$
$$\theta_\varrho := \theta \circ \varrho \colon R_b \dashrightarrow S_h, \qquad \tau_\varrho := \tau \circ \varrho \colon R_b \dashrightarrow \mathbb{A}^2.$$

By analogy with ϱ^{-1} we also have the map θ_ϱ^{-1} (resp. τ_ϱ^{-1}) from S_h (resp. $\mathbb{A}^2$) to the set-theoretic quotient of R_b by $[\omega]_2$.

Remark 2. *It is immediately checked that by θ_ϱ the involution $[-1]\colon R_b \xrightarrow{\sim} R_b$ is induced to the cubic surface S_h as the involution $[-1]$ from §1.1.2, §1.4.1. Similarly, on S_h there is the double map $[2]$. It would be very interesting to also understand its geometric picture.*

According to Lemma 8 we can assume that $\left(\frac{N_h}{p}\right) = -1$, otherwise the conic bundle π on S_h (or, equivalently, on GK_b) has an $\mathbb{F}_p$-section. Thus taking into account Lemma 5 we sum up the main result of this article in

Theorem 14. *For a prime p such that $p \equiv 1 \pmod 3$, $p \equiv 3 \pmod 4$ the generalized Kummer surface GK_b is $\mathbb{F}_p$-rational. More precisely, assume that the conic bundle π on GK_b has no an $\mathbb{F}_p$-section, in particular $\left(\frac{b}{p^2}\right) = -1$. Then we have the birational $\mathbb{F}_p$-isomorphism*

$$\tau\colon GK_b \xrightarrow{\simeq} \mathbb{A}^2 \qquad \textit{such that} \qquad \tau\colon GK_b(\mathbb{F}_p) \hookrightarrow \mathbb{A}^2(\mathbb{F}_p).$$

Another constructive proof of the $\mathbb{F}_p$-rationality could consist in applying the theory of adjoints [49, §5]. However, in our opinion, the approach using conic bundles is more simple and elegant.

The map ϱ is not defined for $x_1 = 0$. We extend it to this case as follows. Let

$$R_{b,\infty} := R_b \cap \mathbb{V}(x_1) = \begin{cases} 2y_0y_1 = b_1, \\ y_0^2 - y_1^2 = x_0^3 + b_0. \end{cases} \quad \subset \quad \mathbb{A}^3_{(x_0,y_0,y_1)},$$

$$Q_b := 4y_0^2(y_0^2 - x_0^3 - b_0) - b_1^2 \quad \subset \quad \mathbb{A}^2_{(x_0,y_0)}.$$

Then the projection $\varrho_\infty \colon R_{b,\infty} \xrightarrow{\simeq} Q_b$ to (x_0, y_0) is a birational $\mathbb{F}_p$-isomorphism with the inverse one

$$\varrho_\infty^{-1} \colon Q_b \xrightarrow{\simeq} R_{b,\infty}, \qquad \varrho_\infty^{-1} \colon (x_0, y_0) \mapsto \Big(x_0, y_0, \frac{b_1}{2y_0}\Big).$$

It is obvious that ϱ_∞ is an isomorphism if $y_0 \neq 0$ both on $R_{b,\infty}$ and Q_b. In particular, this is fulfilled for $b_1 \neq 0$.

Similarly, the map pr is not defined for $y = 0$. Let

$$S_{h,\infty} := x^2 - (h_1t + h_0)z^2 \quad \subset \quad \mathbb{A}^3_{(t,x,z)}.$$

Then the projection $pr_\infty \colon S_{h,\infty} \xrightarrow{\simeq} \mathbb{A}^2_{(x,z)}$ is a birational $\mathbb{F}_p$-isomorphism with the inverse one

$$pr_\infty^{-1} \colon \mathbb{A}^2_{(x,z)} \xrightarrow{\simeq} S_{h,\infty}, \qquad (x, z) \mapsto \Big(x, z, \frac{x^2 - h_0z^2}{h_1z^2}\Big).$$

As a result we obtain the compression map

$$\mathrm{com}_b\colon \overline{E_b}(\mathbb{F}_{p^2}) \hookrightarrow \mathbb{F}_p^2 \times \mathbb{F}_2^3, \qquad \mathrm{com}_b(P) := \begin{cases} \big(\varrho_\infty(P), (0,0,0)\big) & \text{if} \quad x_1(P) = 0, \\ \big((0,0), (0,0,1)\big) & \text{if} \quad P = \mathcal{O}, \\ \big((pr_\infty \circ \theta_\varrho)(P), (v,0)\big) & \text{if} \quad y\big(\theta_\varrho(P)\big) = 0, \\ \big(\tau_\varrho(P), (v,1)\big) & \text{otherwise}, \end{cases}$$

where $v \in \{(0,1),(1,0),(1,1)\}$ is the position number of $x_1(P) \in \mathbb{F}_p^*$ in the representative set $\{\zeta_3^i x_1(P) \pmod{p}\}_{i=0}^2$ ordered with respect to the usual numerical order. Therefore the corresponding decompression map has the form

$$\mathrm{com}_b^{-1}\colon \mathrm{Im}(\mathrm{com}_b) \rightsquigarrow \overline{E_b}(\mathbb{F}_{p^2}), \qquad \mathrm{com}_b^{-1}\big(Q, w\big) = \begin{cases} \varrho_\infty^{-1}(Q) & \text{if} \quad w = (0,0,0), \\ \mathcal{O} & \text{if} \quad w = (0,0,1), \\ (\theta_\varrho^{-1} \circ pr_\infty^{-1})(Q) & \text{if} \quad w = (v,0), \\ \tau_\varrho^{-1}(Q) & \text{if} \quad w = (v,1), \end{cases}$$

where in the two last cases the image of com_b^{-1} is uniquely defined by the value v.

2.1 Usage of the method for some curves (including BLS12-381)

In this paragraph we instantiate the new point compression method in the case $b_0 = b_1$. In particular, this condition is fulfilled for the curve BLS12-381 [7], which is one the most popular pairing-friendly curves today according to [59, table 1]. For this curve

$$p \equiv 10 \pmod{27}, \qquad p \equiv 3 \pmod{4}, \qquad \log_2(p) = 381, \qquad b = 4(1+i).$$

The former allows to extract a cubic $\mathbb{F}_p$-root by means of 1 exponentiation in $\mathbb{F}_p$ (see Lemma 3). More generally, for $b_0 = b_1$ we obtain:

$$N_b = 2b_1^2, \qquad \lambda(t) = b_1(t+1), \qquad \gamma(t) = t^2 - 4t + 1, \qquad r_\pm = 2 \pm \sqrt{-3}i, \qquad s_\pm = 4r_\pm.$$

In particular, $\left(\frac{s_\pm}{p^2}\right) = 1$, because the norm $\mathrm{N}(r_\pm) = 1$. As usually, we will suppose that $\left(\frac{b}{p^2}\right) = -1$ (i.e., $\left(\frac{2}{p}\right) = -1$), hence according to the known formula $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ [54, thm 12.1.iv] we have $p \equiv 3 \pmod{8}$.

We say that an arbitrary map has (on the average) an algebraic complexity

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

if (for most arguments) it can be computed by means of n_S squarings, n_{M_c} multiplications by a constant, n_M general ones (with different non-constant multiples), n_I inversions and n_{CR} cubic roots, where all operations are in $\mathbb{F}_p$. Additions and subtractions in $\mathbb{F}_p$ 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 $c \pmod{p} \leqslant 6$, because they are not more difficult than few additions. Implementation details of the most operations mentioned see, for example, in [54].

Next we specify the maps $\varphi_{\alpha/3}$ and φ_γ, multiplying them by some elements of $\mathbb{F}_p^*$ to reduce their algebraic complexity.

Corollary 2. *For $q = \alpha/3$ the value $\delta = 2/3$ and hence Corollary 1 takes the form:*

$$u = 3, \qquad v(t) = \mp 3t, \qquad w(t) = -3\Big(\frac{3}{4}t^2 + 1\Big)$$

and

$$\psi_q = \begin{cases} x_2 := \pm 3tx - 2y, \\ y_2 := -2x \pm 4ty, \\ z_2 := 2\alpha(t)z, \end{cases} \qquad \psi_q^{-1} = \begin{cases} x := \pm 4tx_2 + 2y_2, \\ y := 2x_2 \pm 3ty_2, \\ z := 2z_2, \end{cases}$$

$$\chi_q = \begin{cases} x_3 := 6x_2 \mp 3ty_2, \\ y_3 := 6y_2, \\ z_3 := 2z_2, \end{cases} \qquad \chi_q^{-1} = \begin{cases} x_2 := 2x_3 \pm ty_3, \\ y_2 := 2y_3, \\ z_2 := 6z_3. \end{cases}$$

Corollary 3. *For $q = \gamma$ Lemma 9 takes the form:*

$$u = -\frac{1}{3}, \qquad v(t) = \mp\frac{t-1}{\sqrt{6}}, \qquad w(t) = -\frac{t^2 - 6t + 1}{24}$$

and

$$\psi_q = \begin{cases} x_2 := \pm\frac{\sqrt{6}}{2}(5-t)x + 6y, \\ y_2 := 6x \pm 2\sqrt{6}(1+t)y, \\ z_2 := q(t)z, \end{cases} \qquad \psi_q^{-1} = \begin{cases} x := \mp\frac{2}{\sqrt{6}}(1+t)x_2 + y_2, \\ y := x_2 \mp \frac{1}{2\sqrt{6}}(5-t)y_2, \\ z := z_2, \end{cases}$$

$$\chi_q = \begin{cases} x_3 := 2x_2 \mp \frac{\sqrt{6}}{2}(1-t)y_2, \\ y_3 := y_2, \\ z_3 := -6z_2, \end{cases} \qquad \chi_q^{-1} = \begin{cases} x_2 := -3x_3 \mp \frac{3\sqrt{6}}{2}(1-t)y_3, \\ y_2 := -6y_3, \\ z_2 := z_3. \end{cases}$$

It is easily seen that after applying φ_γ we obtain the surface S_h with $h(t) = -3b_1(t+1)$. To make sure in correctness of the above formulas see our code [40] in the language of the computer algebra system Magma.

Lemma 10. *The maps com_b, com_b^{-1} respectively have an algebraic complexity*

$$3S + 5M_c + 14M + 2I \qquad \text{and} \qquad 4S + 6M_c + 18M + 3I + CR.$$

Proof. It is easily checked that the basic maps forming com_b, com_b^{-1} have an algebraic complexity as in Table 1. Therefore we know that of the maps τ_ϱ, τ_ϱ^{-1}. Exactly these functions are computed for most arguments. It remains to note that for finding $v \in \mathbb{F}_2^2$ (during computation of com_b) it is necessary to accomplish two multiplications by the constants ζ_3, ζ_3^2. And vice versa, this is also done to recover the initial value of x_1-coordinate (during computation of com_b^{-1}). □

map	ϱ_∞	pr_∞	ϱ	σ	$\varphi_{\alpha/3}$	φ_γ	pr	ϱ_∞^{-1}
alg. complexity	0	0	I	$S+4M$	$S+4M$	$S+3M_c+4M$	$2M+I$	M_c+I

pr_∞^{-1}	ϱ^{-1}	σ^{-1}	$\varphi_{\alpha/3}^{-1}$	φ_γ^{-1}	pr^{-1}
$2S+M_c+M+I$	$S+4M+2I+CR$	$S+6M$	$3M$	$3M_c+3M$	$2S+M_c+2M+I$

Table 1: An algebraic complexity of the maps

3 Further questions

We end the article by some comments about possible generalizations of our point compression method. First of all, in addition to Theorem 14 the author has already proved in [41] a similar one about $\mathbb{F}_2$-rationality of the (usual) Kummer surface of some two supersingular Jacobians [2] of dimension 2. Thus we are feel free to formulate

Conjecture 1. *Let A be an abelian surface over a finite field $\mathbb{F}_q$ and σ be its $\mathbb{F}_q$-automorphism. If the generalized Kummer surface A/σ is geometrically rational, then it is also $\mathbb{F}_q$-rational.*

We do not see any problems to extend the new point compression method to the Weil restriction $\mathrm{R}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(E_b)$ for any finite field $\mathbb{F}_q$ such that $q \equiv 1 \pmod 3$ and $p > 3$. Besides, our approach could be immediately applied to $A_{b,b'} := E_b \times E_{b'}$. Nevertheless, in this article we focused on the surface R_b, because compression of its points seemed to us more difficult and important for practice. Finally, according to Theorem 8 the Jacobian of a hyperelliptic curve $y^2 = x^5 + b$ (for $b \in \mathbb{F}_q^*$, $q \equiv 1 \pmod 5$, and $p > 5$) seems to also have the $\mathbb{F}_q$-rational generalized Kummer surface.

The task of point compression for $A_{b,b'}$ (so-called *double point compression*) is also reasonable. It has already been discussed (in a slightly different way) in [39] for the direct square E^2 of any elliptic curve $E/\mathbb{F}_q$. In that article authors do not try to compress points as compact as possible. Instead of this they find an $\mathbb{F}_q$-model of E^2 in $\mathbb{A}^3$ and the corresponding birational $\mathbb{F}_q$-isomorphism. The advantage of their approach is speed, because it should not solve equations at the decompression stage.

Double point compression also occurs [3] in supersingular isogeny-based cryptography [14]. The main difference from classical one is the need to compress points of a *superspecial* abelian surface E^2 for any supersingular elliptic curve $E/\mathbb{F}_{p^2}$ of trace $2p$ (or $-2p$). Therefore our approach does not spread immediately to this case.

Up to now we have focused only on the rationality problem of a generalized Kummer surface. However there is also another possible method to compress points of a superspecial abelian surface $E^2/\mathbb{F}_{p^2}$. According to Theorem 7 its Kummer surface K is a so-called Zariski surface [61] for $p \not\equiv 1, 2 \pmod{12}$. This means the existence of a purely inseparable map $K \dashrightarrow \mathbb{A}^2$ (or, equivalently, $\mathbb{A}^2 \dashrightarrow K$) of degree p. We stress that computation of such a map (and its inverse image) is very fast and usually even trivial. But, unfortunately, the known proof of the mentioned theorem is valid only over $\overline{\mathbb{F}_p}$ and it is absolutely not constructive.

It is very natural to think about compression for points of m-dimensional abelian varieties, where $m > 2$. *Multiple point compression*, i.e., that for a direct power E^m of an elliptic curve

$E/\mathbb{F}_q$ is discussed in [21] by analogy with double one. At the same time, by the Weil descent attack [15], [23, §3.2] it may be dangerous to consider elliptic curves over $\mathbb{F}_{p^m}$ for classical elliptic cryptography. However, in pairing-based one optimal embedding degree k will exceed 12 in the near future. Therefore we will have to use twists (of degree d) defined over $\mathbb{F}_{p^m}$, where $m = k/d$.

According to [22, §8.2] for most $k > 12$ the curves E_b are still the most pairing-friendly, because there are methods to generate such curves with a quite large prime $\mathbb{F}_p$-subgroup. Unfortunately, for $m > 2$ the generalized Kummer variety corresponding to the order 3 automorphism $[\omega]_m := \mathrm{R}_{\mathbb{F}_{p^m}/\mathbb{F}_p}([\omega])$ on the Weil restriction $R_{b,m} := \mathrm{R}_{\mathbb{F}_{p^m}/\mathbb{F}_p}(E_b)$ is no longer rational [56, lemma 8.11] even over $\overline{\mathbb{F}_p}$. Nevertheless, for $m = 3$ (resp. $m \in \{4, 5\}$) geometrical rationality is proved [46, thm 1.4.(1)] (conjectured [9, ques. 1.3, 1.4]) for the quotient of $R_{b,m}$ by the order 6 automorphism $-[\omega]_m$. Thus instead of m exponentiations in $\mathbb{F}_p$ it is sufficient to accomplish 2 ones.

References

[1] Adj G., Rodríguez-Henríquez F. *Square root computation over even extension fields.* // IEEE Transactions on Computers, 2013. Vol. 63(11). P. 2829–2841.

[2] Aranha D. at al. *Optimal Eta pairing on supersingular genus-2 binary hyperelliptic curves.* // Cryptographers' Track at the RSA Conference, 2012. P. 98–115.

[3] Azarderakhsh R., Jao D. at al. *Key compression for isogeny-based cryptosystems.* // 3rd ACM International Workshop on ASIA Public-Key Cryptography, 2016. P. 1–10.

[4] Barreto P., Lynn B., Scott M. *Constructing elliptic curves with prescribed embedding degrees.* // 3rd International Conference on Security in Communication Networks, 2002. P. 257–267.

[5] Barreto P., Naehrig M. *Pairing-friendly elliptic curves of prime order.* // 12th International Workshop on Selected Areas in Cryptography, 2006. P. 319–331.

[6] Bos J., Naehrig M. et al. *Elliptic curve cryptography in practice.* // 18th International Conference on Financial Cryptography and Data Security, 2014. P. 157–175.

[7] Bowe S. *BLS12-381: New zk-SNARK elliptic curve construction.* // Zcash Company blog, URL: https://z.cash/blog/new-snark-curve/.

[8] Brickell E., Li J. *Enhanced privacy ID from bilinear pairing for hardware authentication and attestation.* // IEEE Second International Conference on Social Computing. 2010. P. 768–775.

[9] Catanese F., Oguiso K., Verra A. *On the unirationality of higher dimensional Ueno-type manifolds*, 2015. URL: https://arxiv.org/abs/1506.01925.

[10] Cho G. at al. *New cube root algorithm based on the third order linear recurrence relations in finite fields.* // Designs, Codes and Cryptography, 2015. Vol. 75(3). P. 483–495.

[11] Coray D., Tsfasman M. *Arithmetic on singular del Pezzo surfaces.* // Proceedings of the London Mathematical Society, 1988. Vol. 3(1). P. 25–87.

[12] Costello C. *Fast formulas for computing cryptographic pairings.* PhD thesis, 2012.

[13] Costello C., Longa P. *Four*$\mathbb{Q}$: *Four-dimensional decompositions on a* $\mathbb{Q}$*-curve over the Mersenne prime.* // 21st Intern. Conf. on the Theory and App. of Crypto. and Inform. Secur., 2015. P. 214–235.

[14] De Feo L., Jao D., Plût J. *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.* // Journal of Math. Cryptology, 2014. Vol. 8(3). P. 209–247.

[15] Diem C. *The GHS attack in odd characteristic.* // Journal of the Ramanujan Mathematical Society, 2003. Vol. 18(1). P. 1–32.

[16] Dudeanu A., Oancea G.-R., Iftene S. *An x-coordinate point compression method for elliptic curves over $\mathbb{F}_p$.* // 12th Intern. Symp. on Symbolic and Numeric Algorithms for Scien. Comp., 2010. P. 65–71.

[17] Duursma I., Gaudry P., Morain F. *Speeding up the discrete log computation on curves with automorphisms.* // Intern. Conf. on the Theory and Appl. of Crypto. and Inform. Secur., 1999. P. 103–121.

[18] Eagle P., Galbraith S., Ong J. *Point compression for Koblitz elliptic curves.* // Advances in Mathematics of Communications, 2011. Vol. 5(1). P. 1–10.

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

[20] Ethereum Foundation, *Program code*. URL: https://github.com/ethereum/.

[21] Fan X., Otemissov A., Sica F., Sidorenko A. *Multiple point compression on elliptic curves.* // Designs, Codes and Cryptography, 2017. Vol. 83(3). P. 565–588.

[22] Freeman D., Scott M., Teske E. *A taxonomy of pairing-friendly elliptic curves.* // Journal of Cryptology, 2010. Vol. 23(2). P. 224–280.

[23] Frey G. *Applications of arithmetical geometry to cryptographic constructions.* // 5th International Conference on Finite Fields and Applications, 2001. P. 128–161.

[24] Fujiki A. *Finite automorphism groups of complex tori of dimension two.* // Publications of the Research Institute for Mathematical Sciences, Kyoto University, 1988. Vol. 24(1). P. 1–97.

[25] Galbraith S., Lin X., Scott M. *Endomorphisms for faster elliptic curve cryptography on a large class of curves.* // Journal of Cryptology, 2011. Vol. 24(3). P. 446–469.

[26] Gallant R., Lambert R., Vanstone S. *Faster point multiplication on elliptic curves with efficient endomorphisms.* // 21st Annual International Cryptography Conference, 2001. P. 190–200.

[27] Hess F., Smart N., Vercauteren F. *The eta pairing revisited.* // IEEE Transactions on Information Theory, 2006. Vol. 52(10). P. 4595–4602.

[28] Hu Z., Longa P., Xu M. *Implementing* 4*-dimensional GLV method on GLS elliptic curves with j-invariant* 0. // Designs, Codes and Cryptography, 2012. Vol. 63(3). P. 331–343.

[29] Hwang W. *On a classification of the automorphism groups of polarized abelian surfaces over finite fields*, 2018. URL: https://arxiv.org/abs/1809.06251.

[30] IEEE Computer Society, *Standard* (Std 1363.3) *for identity based cryptographic techniques using pairings.* // IEEE Standard Specifications for Public-Key Cryptography, 2013.

[31] Iskovskih V. *Rational surfaces with a pencil of rational curves.* // Mathematics of the USSR-Sbornik, 1967. Vol. 3(4). P. 563–587.

[32] Iskovskih V. *Rational surfaces with a pencil of rational curves and with positive square of the canonical class.* // Mathematics of the USSR-Sbornik, 1970. Vol. 12(1). P. 91–117.

[33] ISO/IEC, *Cryptographic techniques based on elliptic curves* (ISO/IEC 15946), 2017.

[34] ISO/IEC, *Key management — Part 3: Mechanisms using asymmetric techniques* (ISO/IEC 11770-3), 2015.

[35] Janson S. *Roots of polynomials of degrees* 3 and 4, 2010. URL: https://arxiv.org/abs/1009.2373.

[36] Katsura T. *Generalized Kummer surfaces and their unirationality in characteristic p.* // Journal of the Faculty of Science, the University of Tokyo, 1987. Vol. 34. P. 1–41.

[37] Katsura T. *On Kummer surfaces in characteristic* 2. // International Symposium on Algebraic Geometry, 1977. P. 525–542.

[38] Katsura T., Schütt M. *Zariski K3 surfaces*, 2017. URL: https://arxiv.org/abs/1710.08661.

[39] Khabbazian M., Gulliver T., Bhargava V. *Double point compression with applications to speeding up random point multiplication.* // IEEE Transactions on Computers, 2007. Vol. 56(3). P. 305–313.

[40] Koshelev D. *Magma code*. URL: https://www.researchgate.net/publication/331581937_Verification_of_the_formulas_Magmadoc.

[41] Koshelev D. *On rationality of Kummer surfaces over the field of two elements in the context of the discrete logarithm problem.* Master thesis (in russian), 2017. URL: https://www.hse.ru/en/edu/vkr/206737687.

[42] Lindemann R. et al. *FIDO ECDAA algorithm*, 2018.

[43] Longa P., Sica F. *Four-dimensional Gallant–Lambert–Vanstone scalar multiplication.* // Journal of Cryptology, 2014. Vol. 27(2). P. 248–283.

[44] Manin Yu. *Cubic forms: algebra, geometry, arithmetic.* — Amsterdam.: North Holland, 2012.

[45] Naehrig M. *Constructive and computational aspects of cryptographic pairings.* PhD thesis, 2009.

[46] Oguiso K., Truong T. *Explicit examples of rational and Calabi–Yau threefolds with primitive automorphisms of positive entropy.* // Jour. of Math. Sciences, the Univ. of Tokyo, 2015. Vol. 22. P. 361–385.

[47] Open Mobile Alliance, *Wireless Application Protocol Wireless Transport Layer Security* (WAP WTLS) *Specification*, 2001.

[48] Popov V., Vinberg E. *Invariant theory.* // Algebraic Geometry IV, 1994. P. 123–278.

[49] Schicho J. *The parametrization problem for algebraic surfaces.* // ACM SIGSAM Bulletin, 1999. Vol. 33(3). P. 13.

[50] SECG, *SEC* 2: *Recommended elliptic curve domain parameters. Version* 2.0. // Standards for Efficient Cryptography, 2010.

[51] *Secp256k1.* // BitcoinWiki. URL: https://en.bitcoin.it/wiki/Secp256k1.

[52] Seroussi G. *Compact representation of elliptic curve points over $\mathbb{F}_{2^n}$.* // HP Labs Tech. Reports, 1998.

[53] Shamir A. *Identity-based cryptosystems and signature schemes.* // Workshop on the Theory and Application of Cryptographic Techniques, 1985. P. 47–53.

[54] Shoup V. *A computational introduction to number theory and algebra.* — Cambridge.: Cambridge University Press, 2009.

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

[56] Ueno K. *Classification of algebraic varieties,* I. // Compositio Math., 1973. Vol. 27(3). P. 277–342.

[57] van Hoeij M., Cremona J. *Solving conics over function fields.* // Journal de Théorie des Nombres de Bordeaux, 2006. Vol. 18(3). P. 595–606.

[58] W3C, *Web Authentication: An API for accessing public key credentials*, 2019.

[59] Yonezawa S. et al. *Pairing-friendly curves.* // Internet-Draft, IETF Secretariat, 2019.

[60] Yoshihara H. *Quotients of abelian surfaces.* // Publications of the Research Institute for Mathematical Sciences, Kyoto University, 1995. Vol. 31(1). P. 135–143.

[61] Zariski O. *On Castelnuovo's criterion of rationality* $p_a = P_2 = 0$ *of an algebraic surface.* // Illinois Journal of Mathematics, 1958. Vol. 2. P. 303–315.