A new elliptic curve point compression method based on $F_p$-rationality of some generalized Kummer surfaces

Koshelev Dmitrii

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

Abstract. In the article we propose a new compression method (to $2 \log_2(p) + 3$ bits) for the $F_p^2$-points of an elliptic curve $E_b : y^2 = x^3 + b$ (for $b \in F_p^*$) of $j$-invariant 0. It is based on $F_p$-rationality of some generalized Kummer surface $GK_b$. This is the geometric quotient of the Weil restriction $R_b := R_{F_p^2/F_p}(E_b)$ 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 $F_p(t)$) to obtain explicit and quite simple formulas of a birational $F_p$-isomorphism between $GK_b$ and $A^2$. 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 $F_p$-root. For $p \not\equiv 1 \mod 27$ this is just a single exponentiation in $F_p$, hence the new method seems to be much faster than the classical one with $x$-coordinate, which requires two exponentiations in $F_p$.

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 $E \subset A^2(x,y)$ 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 $E_b : y^2 = x^3 + b$ for $b \in \mathbb{F}_q^*$ (of $j$-invariant 0). Despite the insignificant acceleration [17] of Pollard rho method, these curves (for $q = p \equiv 1 \mod 3$) 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 $[\omega] : (x,y) \mapsto (x^{2/3}, y)$ defined over $\mathbb{F}_p$. Therefore for a faster scalar multiplication on a curve $E_b$ we can apply the so-called GLV decomposition.
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 FourQ [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 [31] and products of the companies ZECC [7], Intel [8], Ethereum Foundation [20] (more information is represented in [59]).

As usual in cryptography, for a given elliptic curve $E/\mathbb{F}_p$ its order $n := |E(\mathbb{F}_p)|$ is often assumed to be a prime ($\neq p$). In this case, the embedding degree of $E$ is, by definition, the extension degree $k := |\mathbb{F}_p(\mu_n) : \mathbb{F}_p|$. Further, let $E'$ be a twist for $E$ of degree $d \mid k$ and $G \subset E'(\mathbb{F}_p^4)$ be the subgroup of order $n$. In practice, pairings (of type 2 [12 §2.3.2]) are mainly taken in the form

$$E(\mathbb{F}_p) \times G \to \mu_n \subset \mathbb{F}_p^*$$

where $k$ is the minimally possible number such that the discrete logarithm problem in $\mathbb{F}_p^*$ is hard, but $d$ is, conversely, the maximally possible one. It is a classical fact that $d \leq 6$ 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 [1] of embedding degree 12 (and only they as far as the author knows) are used in practice at the moment. Barreto–Naehrig curves also have the embedding degree $k = 12$, 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 $p \neq 1 (\text{mod } 8)$ 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 $p \neq 1 (\text{mod } 27)$ 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) $R_b := R_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_b)$ [23 §3.2] with respect to the order 3 automorphism $[\omega]_2 := R_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\omega)$. More precisely, we apply the theory of conic bundles [31, 32] (i.e., conics over the function field $\mathbb{F}_p(t)$) 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 $E_b(\mathbb{F}_{p^2}) \rightarrow R_b(\mathbb{F}_p)$ we need to find an inverse image of the natural map $\varrho : R_b \rightarrow GK_b$ 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 $\varrho^*$ 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 the two Jacobians $J_b$ [2] over the fields $\mathbb{F}_e$, where $b \in \mathbb{F}_2$ and $2, 3 \nmid e$. These are the unique (up to an $\mathbb{F}_2$-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

Introduction 1

1 Mathematical preliminaries and auxiliary results 4

1.1 Cubics ................................................................. 4

1.1.1 Cubic polynomials ............................................... 4

1.1.2 Cubic $\mathbb{F}_p$-surfaces $S_h$ with two $\mathbb{F}_p$-nodes .......... 5

1.2 Elliptic curves $E_b$ (of $j$-invariant 0) ......................... 7

1.2.1 The Weil restriction of $E_b/\mathbb{F}_p^2$ ....................... 8

1.3 Generalized Kummer surfaces .................................... 9

1.3.1 The generalized Kummer surfaces $GK_b$ .................. 9

1.4 Conic bundles (conics over the function field) ............... 10

1.4.1 A conic bundle on $S_h$ ....................................... 12

1.4.2 Blowing down components of degenerate fibers .......... 14

2 New point compression method 16

2.1 Usage of the method for some curves (including BLS12-381) . 18

3 Further questions 20
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 \( x^3 + ax^2 + bx + c \) over a field \( k \) of characteristic \( p \neq 2, 3 \). After the variable change \( x := y - \alpha / 3 \), we obtain the polynomial

\[
f(y) := y^3 + cy + d,
\]

where \( c := \beta - \alpha^2 / 3 \), \( d := \gamma - \alpha \beta / 3 + 2\alpha^3 / 27 \).

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

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

\[
(\Delta)_k = \begin{cases} 
0 & \text{if } f \text{ has a multiple root}, \\
1 & \text{if } G = 1 \text{ or } G \cong \mathbb{Z}/3, \\
-1 & \text{if } G \cong \mathbb{Z}/2 \text{ or } G \cong S_3.
\end{cases}
\]

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

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

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 \( \zeta_3 \) a fixed primitive 3-th root of unity, which is equal to \( (\frac{-1 + \sqrt{-3}}{2}) \). However for \( p = 0 \) we prefer the symbol \( \omega \).

Lemma 2. Assume that \( \zeta_3 \in k^* \), i.e., \( (\frac{-3}{k}) = 1 \). 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 \( n \in \mathbb{N} \):

\[
v_0 := 2, \quad v_1 := b, \quad v_n := bv_{n-1} - av_{n-2}.
\]

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

\[
-\frac{(3c)^{-\frac{1}{3}}v_n(C, D)}{3}, \quad \text{where} \quad C := -27c^3, \quad D := -27d, \quad n := \frac{p + 2(\frac{\Delta}{p})}{3}.
\]
Lemma 3 ([16] rem. 2]). For \(a \in \mathbb{F}_p^*\) we obtain:

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

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

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

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 \(h = h_1t + h_0 \in \mathbb{F}_p[t] \) \((h_1 \neq 0)\) consider a cubic surface

\[
S_h := x^2y - (t^2 + y^2)y - (h_1t + h_0y)z^2 \subset \mathbb{P}^3_{(x:y:z:t)}.
\]

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

\[
\frac{\partial S_h}{\partial x} = 2xy, \quad \frac{\partial S_h}{\partial y} = x^2 - (t^2 + 3y^2) - h_0z^2, \quad \frac{\partial S_h}{\partial z} = -2(h_1t + h_0y)z, \quad \frac{\partial S_h}{\partial t} = -2ty - h_1z^2.
\]

Besides, after the translation

\[
\tau_{P_\pm} : (x : y : z : t) \mapsto (\pm x - t : y : z : t), \quad \tau_{P_\pm}^{-1} : (x : y : z : t) \mapsto (\pm(x + t) : y : z : t)
\]

the tangent cone of

\[
S_{h,O} := \tau_{P_\pm}(S_h) = x^2y + 2txy - y^3 - (h_1t + h_0y)z^2
\]

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

\[
T_O(S_{h,O}) = 2xy - h_1z^2.
\]

Therefore the points \(P_\pm\) are nodes and the projection from one of them is the birational \(\mathbb{F}_p\)-isomorphism \(pr : S_h \sim \mathbb{A}^2\). □
Let \( N_h := h_0^2 + h_1^2 \) and note that
\[
S_{h,O} \cap T_O(S_{h,O}) = L_{P_+P_-} \cup M_O,
\]
where
\[
L_{P_+P_-} := \mathbb{V}(y,z), \quad M_O := \begin{cases} 
  h_1x = (h_0 \pm \sqrt{N_h})y, \\
  h_1z = \pm \sqrt{2h_1xy}.
\end{cases}
\]
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:
\[
pr_O: S_{h,O} \simeq \mathbb{A}^2_{(u,v)}, \quad (x : y : z : t) \mapsto \left( \frac{x}{y}, \frac{z}{y} \right),
\]
\[
pr^{-1}_O: \mathbb{A}^2_{(u,v)} \simeq S_{h,O}, \quad (u, v) \mapsto (uY : Y : vY : T),
\]
where
\[
Y := h_1v^2 - 2u, \quad T := u^2 - h_0v^2 - 1.
\]
Note that \( pr_O, pr^{-1}_O \) are isomorphisms on the open subsets
\[
U_O := S_{h,O} \setminus (T_O(S_{h,O}) \cup L_\infty), \quad V := \mathbb{A}^2_{(u,v)} \setminus \mathbb{V}(Y),
\]
where \( L_\infty := \mathbb{V}(y,t) \). Thus the maps
\[
pr = pr_O \circ \tau_{P_\pm}: S_h \simeq \mathbb{A}^2, \quad pr^{-1} = \tau^{-1}_{P_\pm} \circ pr^{-1}_O: \mathbb{A}^2 \simeq S_h
\]
are those on the open subsets \( V \) and
\[
U := \tau^{-1}_{P_\pm}(U_O) = S_h \setminus (T_{P_\pm}(S_h) \cup L_\infty),
\]
where
\[
T_{P_\pm}(S_h) = \tau^{-1}_{P_\pm}(S'_h) = \pm 2(x + t)y - h_1z^2.
\]
Thus we proved

**Lemma 5.** If \((\frac{N_h}{p}) = -1\), then \( pr: U(\mathbb{F}_p) \simeq V(\mathbb{F}_p) \), where
\[
U(\mathbb{F}_p) = S_h(\mathbb{F}_p) \setminus \mathbb{V}(y), \quad V(\mathbb{F}_p) = \mathbb{A}^2(\mathbb{F}_p) \setminus \mathbb{V}(Y).
\]

We are also interested in the involution
\[
[-1]: S_h \simeq S_h, \quad (x : y : z : t) \mapsto (x : y : -z : t),
\]
the meaning of which is explained in Remark 2. Let \( P \in S_h \setminus T_\infty(S_h) \) be a point outside the tangent plane
\[
T_\infty(S_h) = h_1t + h_0y \quad \text{at} \quad \infty := (0 : 0 : 1 : 0) \in S_h.
\]
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 \( \infty \) and \( P \) (see also [11, 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 $\mathbb{E}_b \subseteq \mathbb{P}^2$ (of $j = 0$) given by the affine model

$$E_b : y^2 = x^3 + b \quad \subseteq \mathbb{A}^2(x,y)$$

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

$$[\omega] : E_b \cong E_b, \quad (x, y) \mapsto (\zeta_3 x, y)$$

with fixed point set

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

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 $\mathbb{F}_q$ by the map

$$\varphi_{b,b'} : E_b \cong E_{b'}, \quad (x, y) \mapsto (\sqrt[3]{\beta} x, \sqrt{\beta} y),$$

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 $E_{\alpha_i}$ ($i \in \mathbb{Z}/6$) 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:

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

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

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

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 $a \in \mathbb{Z}[\omega] \setminus \langle \pi \rangle$ its 6-th power residue symbol $(\tfrac{a}{\pi})_6$ is, by definition, the 6-th root of unity that is congruent to $a^{\frac{n-1}{\pi}}$ modulo $\pi$. 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,

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

where $\overline{\pi_q} = \pi^e$ 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:

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

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

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

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 $\alpha$ be as in Theorem 4. If $2, 3 \nmid n_b$, then

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

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

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

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 $b := b_0 + b_1i$ 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

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

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

$$[\omega]_2: R_b \Rightarrow R_b, \quad (x_0, x_1, y_0, y_1) \mapsto (\zeta_3 x_0, \zeta_3 x_1, y_0, y_1).$$

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

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

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

$$[-1] : R_b \Rightarrow R_b, \quad (x_0, x_1, y_0, y_1) \mapsto (x_0, x_1, -y_0, -y_1).$$

8
1.3 Generalized Kummer surfaces

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

Let us recall some rationality properties of generalized Kummer surfaces.

\textbf{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 $\iff K_A$ is a Zariski surface [61];
2. If $p = 2$, then $A$ is supersingular $\iff K_A$ is a rational surface.

\textbf{Theorem 8} ([24, table 6], [60, §2]). For $k = \mathbb{C}$ there are only two abelian surfaces having $\sigma$ 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 $\sigma$ (of order 5) induced from the curve automorphism $(x,y) \mapsto (x\sqrt{1},y)$.

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

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

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

Note that the discriminant of $f/b_1$ is equal to $\Delta = 2^23^3N_b^2/b_1^4$ and hence $(\Delta/p) = -1$. By Lemma I there is the decomposition $f = \lambda\gamma$ into linear $\lambda$ and $\mathbb{F}_p$-irreducible quadratic $\gamma$ polynomials over $\mathbb{F}_q$. For uniqueness we suppose $\gamma$ 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

\textbf{Theorem 10.} There is the affine model

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

for which the corresponding quotient map has the form

$$\varrho: R_b \to GK_b, \quad (x_0, x_1, y_0, y_1) \mapsto \left(\frac{x_0}{x_1}, y_0, y_1\right).$$
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

\[
F := \mathbb{F}_p(t, y_0, y_1) \subset \mathbb{F}_p(GK_b), \quad \text{where} \quad t := \frac{x_0}{x_1},
\]

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 \( [\mathbb{F}_p(R_b) : F] \leq 3 \). 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. \( \square \)

It is known \([56, \text{exam. 8.10}]\) that the image of \( \text{Fix}([\omega]_2) \subset R_b \) under \( \varrho \) is the singular locus of \( GK_b \) 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 \( \mathbb{A}^1 \times \mathbb{P}^2(y_0:y_1:y_2) \), keeping the same notation. In this case the quotient map take the form

\[
\varrho: R_b \dashrightarrow GK_b, \quad (x_0, x_1, y_0, y_1) \mapsto \left( \frac{x_0}{x_1}, (y_0 : y_1 : 1) \right).
\]

An inverse image of \( \varrho \) is represented, for example, as

\[
(t, (y_0 : y_1 : y_2)) \mapsto (tX_1, X_1, Y_0, Y_1),
\]

where

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

In other words, these formulas give the map \( \varrho^{-1} \) 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 \( \infty \).

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 \( \pi: S \to \mathbb{P}^1 \) 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 (over \( \mathbb{F}_q(t_0) \)) of degree 2. As usually, a \( \mathbb{F}_q \)-section of \( \pi \) is a \( \mathbb{F}_q \)-morphism \( \sigma: \mathbb{P}^1 \to S \) such that \( \pi \circ \sigma = \text{id} \).

It is clear that \( \pi \) corresponds to its general fibre \( F_\pi \), which is a non-degenerate conic over the univariate function field \( \mathbb{F}_q(t) \). And besides, \( \mathbb{F}_q \)-sections of \( \pi \) correspond to \( \mathbb{F}_q(t) \)-points on \( F_\pi \). For one another conic bundle \( \pi': S' \to \mathbb{P}^1 \) any birational \( \mathbb{F}_q \)-isomorphism \( \varphi: S \sim \to S' \)
(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 \( \varphi_{\pi, \pi'} : F_{\pi} \cong F_{\pi'} \), and vice versa. If the general fibre \( F_{\pi} \) 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 \( \pi \) is called relatively \( \mathbb{F}_q \)-minimal if \( S \) has no \( \mathbb{F}_q \)-orbits of pairwise disjoint exceptional \((-1)\)-curves in fibers of \( \pi \). In other words, the surface \( S \) can not be contracted over \( \mathbb{F}_q \) with respect to \( \pi \). 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 \( \pi : S \to \mathbb{P}^1 \) to be a relatively \( \mathbb{F}_q \)-minimal conic bundle. Then we obtain:

1. The number of degenerate fibres of \( \pi \) (over \( \mathbb{F}_q \)) 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 \( K^2 \geq 5 \), 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

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

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 \( \pi : S \to \mathbb{P}^1_{(x_0:x_1)} \). The product \( \Delta := FGH \) is called discriminant of \( \pi \). After a simple check we obtain

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

1. The fibre of \( \pi \) over \( t_0 \) is degenerate \( \iff \Delta(t_0) = 0 \);

2. The fibre of \( \pi \) over \( t_0 \) contains a singular point on \( S \) \( \iff \) \( t_0 \) is a multiple root of \( \Delta \);

3. Singular curves on \( S \) may only be double fibers of \( \pi \).

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

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

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 \( \pi \)) a conic bundle despite the fact that \( S_{f,g,h} \) is not a projective surface. Thus its general fibre can be written as

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

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

and $a, b$ are orders at $t_0$ of $\alpha, \beta$ 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 $\pi : S_h \to \mathbb{P}^1_{(y:t)}$ from the line $L_\infty$, which is a conic bundle. The surfaces $S_h$ and $S'_h := x^2 - (t^2 + 1)y^2 - (h_1t + h_0)z^2 \subset \mathbb{A}^1_t \times \mathbb{P}^2_{(x:y:z)}$

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 $\pi' : S'_h \to \mathbb{A}^1_t$.

$$pr' : S'_h \cong \mathbb{A}^2_{(u,v)}, \quad (t, (x : y : z)) \mapsto \left(\pm \frac{x}{y} - t, \frac{z}{y}\right),$$

and

$$[-1] : S'_h \cong S'_h, \quad (t, (x : y : z)) \mapsto (t, (x : y : -z)).$$

Besides,

$$(pr')^{-1} : \mathbb{A}^2_{(u,v)} \cong S'_h, \quad (u, v) \mapsto \left(\frac{T}{Y}, (\pm (uY + T) : Y : vY)\right),$$

where

$$Y := h_1v^2 - 2u, \quad T := u^2 - h_0v^2 - 1.$$  

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 $\pi'$ has an $\mathbb{F}_p$-section $\iff \left(\frac{Na}{p}\right) = 1$.

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

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

12
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 \( r(t) = r_1t + r_0 \) such that \( g \mid h - r^2 \). The remainder of dividing \( h - r^2 \) by \( g \) is equal to
\[
(h_1 - 2r_0r_1)t + (h_0 - r_0^2 + r_1^2),
\]
hence we obtain the equation system
\[
\begin{cases}
r_0 = \frac{h_1}{2r_1}, \\
4r_1^4 + 4h_0r_1^2 - h_1^2 = 0.
\end{cases}
\]
Therefore \( r_1^2 = R_\pm \), where
\[
R_\pm := \frac{-h_0 \pm \sqrt{N_h}}{2}, \quad R_+R_- = -\frac{h_1^2}{4}.
\]
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 \( \mathbb{F}_p \). \( \Box \)

Provided \( \left( \frac{N_h}{p} \right) = -1 \) we see that \( pr' : U(\mathbb{F}_p) \hookrightarrow V(\mathbb{F}_p) \) by analogy with Lemma 5. For the next theorem consider the lines
\[
L_\pm := h_1x \pm y\sqrt{N_h}, \quad M_\pm := x - z\sqrt{h(\pm i)}, \quad M_\pm^{(1)} = x + z\sqrt{h(\pm i)}.
\]

**Theorem 13.** If \( \left( \frac{N_h}{p} \right) = -1 \), then:
1. The degenerate fibers of \( \pi' \) over \( t \neq \infty \) are represented in Figure 1.
2. The fibre of \( \pi' \) over \( \infty \) 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 \( \mathbb{F}_p \)) as
\[
s^2 - (1 + s^2)y^2 - (1 + \frac{h_0}{h_1}s)sz^2 \subset \mathbb{A}^3_{(y,z,s)}.
\]
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
\[
A = \sqrt{-s^2}, \quad B = \sqrt{-(1 + \frac{h_0}{h_1}s)} \in \mathbb{F}_p[[s]].
\]
Finally, the third fact follows from the Iskovskih theorem 11 and \( \mathbb{F}_p \)-rationality of \( S_h \) (see Lemma 4). \( \Box \)

Hereafter we will identify \( (S_h, \pi, pr) \) and \( (S_h', \pi', pr') \), saving for simplicity only the first notation.
We propose to start the searching a desired transformation in the form $L_{\pi}$. For better comprehension of the described situation see Figure 2.

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

As usual, the projection $\pi: S_h \to A^1_t$ 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 $\left(\frac{s_{\pm}}{p}\right) = 1$. Then for some $u \in \mathbb{F}_p^*$ there is a birational $\mathbb{F}_p$-isomorphism (respecting the conic bundles)

$$\varphi_q: S_h \cong S_{u^2 h}$$

such that $\varphi_q: S_h(\mathbb{F}_p) \cong S_{u^2 h}(\mathbb{F}_p)$.

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

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

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

$$(a_0^2 - a_1^2 d + d - 1)x_2^2, \quad (2a_0a_1 - a_1^2 c + c)x_2^2 t, \quad (a_0 + b_0 d - b_0 - b_1 c d)x_2 y_2,$$

$$(a_1 + b_0 c - b_1 (c^2 - d + 1))x_2 y_2 t, \quad (db_0^2 - b_0^2 - 2 c d b_0 b_1 + d(2c^2 - d + 1)b_1^2 + 1)y_2^2, \quad (cb_0^2 - 2(c^2 - d + 1)b_0 b_1 + c(c^2 - 2d + 1)b_1^2)y_2^2 t$$

**Figure 1:** The Frobenius action on degenerate fibers of the conic bundle $\pi': S'_h \to A_t^1$ two $\mathbb{F}_p$-conjugate degenerate fibers

**Figure 2:** Pairs of $\mathbb{F}_p$-conjugate lines lying in $\mathbb{F}_p$-conjugate degenerate fibers over roots $r_{\pm}$ of some $\mathbb{F}_p$-irreducible quadratic polynomial.
and the non-zero quotients \( ux_2^2, v(t)x_2y_2, w(t)y_2^2 \), where
\[
\begin{align*}
u(t) &:= 2(-b_1 t + b_1 c - b_0), \\
w(t) &:= -b_1^2 t^2 + b_1(-2b_0 + b_1 c)t - b_0^2 + 2b_0 b_1 c - b_1^2 (c^2 - d + 1).
\end{align*}
\]

Consider the trace and norm:
\[
T := \text{Tr}_{\mathbb{F}_p/\mathbb{F}_p}(s_\pm) = c^2 - 2d + 2, \quad N := N_{\mathbb{F}_p/\mathbb{F}_p}(s_\pm) = c^2 + d^2 - 2d + 1.
\]

Because of \( \left( \frac{a+1}{p} \right) = 1 \) we get \( \left( \frac{N}{p} \right) = 1 \). Also, it is easily checked that \( T^2 - c^2 D = 4N \). The system of reminders has two \( \mathbb{F}_p \)-solutions:
\[
\begin{align*}
a_0 &:= c \frac{(d+1)Nb_1^2 + 1 - d}{2Nb_1}, & a_1 &:= \frac{TNb_1^2 - c^2}{2Nb_1}, & b_0 &:= c \frac{Nb_1^2 + 1}{2Nb_1}, & b_1 &:= \pm \sqrt{\beta},
\end{align*}
\]
where \( \beta \) is exactly one (due to \( \left( \frac{2}{p} \right) = -1 \)) of the roots
\[
\frac{T \pm 2\sqrt{N}}{ND} \in \mathbb{F}_p, \quad \text{of} \quad DN^2 X^2 - 2TNX + c^2 \in \mathbb{F}_p[X]
\]
such that \( \left( \frac{\beta}{p} \right) = 1 \). Therefore
\[
\psi_q : S_h \cong S', \quad \text{where} \quad S' := ux_2^2 + v(t)x_2y_2 + w(t)y_2^2 - \frac{h(t)}{q(t)}z_2^2.
\]

Note that \( u, a_1 \neq 0 \). Thus after the \( \mathbb{F}_p \)-transformation \( \chi_q : S' \cong S_{u \frac{h}{q}} \) given by
\[
\chi_q := \begin{cases} x_3 := ux_2 + \frac{v(t)}{2} y_2, \\
y_3 := a_1 b_1 y_2, \\
z_3 := z_2, \end{cases} \quad \chi_q^{-1} = \begin{cases} x_2 := \frac{a_1 b_1}{u} x_3 - \frac{v(t)}{2u} y_3, \\
y_2 := y_3, \\
z_2 := a_1 b_1 z_3, \end{cases} \quad \det(\chi_q) = ua_1 b_1
\]
we obtain the desired surface \( S_{u \frac{h}{q}} \), i.e., \( \varphi_q := \chi_q \circ \psi_q \) satisfies the theorem conditions.

Under the conditions of this lemma as the lines of Figure 2 we can take
\[
L_\pm = x - \sqrt{s_\pm} y, \quad M_\pm = x + \sqrt{s_\pm} y.
\]

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 \( \left( \frac{a+1}{p} \right) = 1 \) is fulfilled. Thus, letting \( \delta := \sqrt{d(d - 1)} \), we obtain:
\[
\begin{align*}
u &:= -\frac{1}{d}, \quad v(t) = \mp \frac{2t}{\delta}, \quad w(t) = -\frac{t^2 - d + 1}{\delta^2}
\end{align*}
\]
(in particular, \( \left( \frac{u}{p} \right) = -1 \)) and (up to multiplication by elements of \( \mathbb{F}_p^* \))

15
Remark 1. If \( E \) is 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:

\[
E_b \subset \mathbb{A}^2_{(x,y)}, \quad R_b \subset \mathbb{A}^4_{(x_0,x_1,y_0,y_1)}, \quad GK_b \subset \mathbb{A}^1_1 \times \mathbb{P}^2_{(y_0:y_1:y_2)}.
\]

Note that the projection \( \pi : GK_b \to \mathbb{A}^1_1 \) 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 \( \mathbb{F}_p \)-points of \( E_b \). We also discuss some technical details of its implementation.

**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:

\[
E_b \subset \mathbb{A}^2_{(x,y)}, \quad R_b \subset \mathbb{A}^4_{(x_0,x_1,y_0,y_1)}, \quad GK_b \subset \mathbb{A}^1_1 \times \mathbb{P}^2_{(y_0:y_1:y_2)}.
\]

Proof. It is immediately checked that

\[
s_+ = s_- = 1 - d, \quad D = -4d, \quad T = -2(d - 1), \quad N = (d - 1)^2, \quad \beta = \frac{1}{d^2}
\]

and all other values are as stated.

First, we reduce \( GK_b \) to a diagonal form by the map \( \sigma : GK_b \sim \sim S_{\alpha_f} \) given by

\[
\sigma := \begin{cases} 
  x := \beta(t)y_0 + \alpha(t)y_1, \\
  y := g(t)y_0, \\
  z := y_2,
\end{cases} \quad \sigma^{-1} = \begin{cases} 
  y_0 := \alpha(t)y, \\
  y_1 := g(t)x - \beta(t)y, \\
  y_2 := \alpha(t)g(t)z,
\end{cases}
\]

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

\[
\varphi_{\alpha/3} : S_{\alpha_f} \sim \sim S_{\alpha_f}, \quad \varphi_\gamma : S_{\alpha_f} \sim \sim S_h,
\]

\[
\varphi_{\alpha/3} : S_{\alpha_f} \sim \sim S_{\alpha_f}, \quad \varphi_\gamma : S_{\alpha_f} \sim \sim S_h,
\]

\[
\varphi_{\alpha/3} : S_{\alpha_f} \sim \sim S_{\alpha_f}, \quad \varphi_\gamma : S_{\alpha_f} \sim \sim S_h,
\]

\[
\varphi_{\alpha/3} : S_{\alpha_f} \sim \sim S_{\alpha_f}, \quad \varphi_\gamma : S_{\alpha_f} \sim \sim S_h,
\]

\[
\varphi_{\alpha/3} : S_{\alpha_f} \sim \sim S_{\alpha_f}, \quad \varphi_\gamma : S_{\alpha_f} \sim \sim S_h,
\]

\[
\varphi_{\alpha/3} : S_{\alpha_f} \sim \sim S_{\alpha_f}, \quad \varphi_\gamma : S_{\alpha_f} \sim \sim S_h,
\]
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 1). Thus we obtain the maps

\[
\theta := \varphi_{\gamma} \circ \varphi_{\alpha/3} \circ \sigma: GK_b \simeq S_h; \quad \tau := pr \circ \theta: GK_b \simeq \mathbb{A}^2, \\
\theta_g := \theta \circ g: R_b \rightarrow S_h; \quad \tau_g := \tau \circ g: R_b \rightarrow \mathbb{A}^2.
\]

By analogy with \( \varphi^{-1} \) we also have the map \( \theta_g^{-1} \) (resp. \( \tau_g^{-1} \)) 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 \( \theta_g \), the involution \([-1]: R_b \to R_b \) 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 \( (\frac{N_b}{p}) = -1 \), otherwise the conic bundle \( \pi \) 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 \( \pi \) on \( GK_b \) has no an \( \mathbb{F}_p \)-section, in particular \( (\frac{b}{p}) = -1 \). Then we have the birational \( \mathbb{F}_p \)-isomorphism

\[
\tau: GK_b \simeq \mathbb{A}^2 \quad \text{such that} \quad \tau: GK_b(\mathbb{F}_p) \hookrightarrow \mathbb{A}^2(\mathbb{F}_p).
\]

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 \( g \) is not defined for \( x_1 = 0 \). We extend it to this case as follows. Let

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

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

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

\[
g_\infty^{-1}: Q_b \simeq R_{b, \infty}, \quad g_\infty^{-1}: (x_0, y_0) \mapsto \left( x_0, y_0, \frac{b_1}{2y_0} \right).
\]

It is obvious that \( g_\infty \) 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

\[
S_{h, \infty} := \begin{cases} x^2 - (h_1t + h_0)z^2 \subset \mathbb{A}^3_{(t,x,z)}, \end{cases}
\]

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

\[
pr_\infty^{-1}: \mathbb{A}^2_{(x,z)} \simeq S_{h, \infty}, \quad (x, z) \mapsto (x, z, \frac{x^2 - h_0z^2}{h_1z^2}).
\]
As a result we obtain the compression map

$$\text{com}_b : \mathbb{E}_b(\mathbb{F}_p^2) \hookrightarrow \mathbb{F}_p^2 \times \mathbb{F}_2^3,$$

$$\text{com}_b(P) := \begin{cases} (\vartheta(P), (0, 0, 0)) & \text{if } x_1(P) = 0, \\ ((0, 0), (0, 0, 1)) & \text{if } P = \mathcal{O}, \\ ((pr_\infty \circ \theta_v)(P), (v, 0)) & \text{if } y(\theta_v(P)) = 0, \\ (\tau_v(P), (v, 1)) & \text{otherwise}, \end{cases}$$

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 \(\{\zeta_i^j x_1(P) \pmod{p}\}_{i=0}^2\) ordered with respect to the usual numerical order. Therefore the corresponding decompression map has the form

$$\text{com}_b^{-1} : \text{Im}(\text{com}_b) \cong \mathbb{E}_b(\mathbb{F}_p^2), \quad \text{com}_b^{-1}(Q, w) = \begin{cases} \vartheta^{-1}(Q) & \text{if } w = (0, 0, 0), \\ \mathcal{O} & \text{if } w = (0, 0, 1), \\ (\theta_v^{-1} \circ pr_\infty^{-1})(Q) & \text{if } w = (v, 0), \\ \tau_v^{-1}(Q) & \text{if } w = (v, 1), \end{cases}$$

where in the two last cases the image of \(\text{com}_b^{-1}\) 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 of the most popular pairing-friendly curves today according to [59, table 1]. For this curve

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

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:

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

In particular, \(\left(\frac{a}{p}\right) = 1\), because the norm \(N(r_\pm) = 1\). As usually, we will suppose that \(\left(\frac{b}{p}\right) = -1\) (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

\[ n_S S + n_{M_1} M_1 + n_M M + n_I I + n_{CR} CR \]

if (for most arguments) it can be computed by means of \(n_S\) squarings, \(n_{M_1}\) 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 \(n_{M_1}\)) for multiplications by a constant \(c \in \mathbb{F}_p\) such that \(c \pmod{p} \leq 6\), 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 \( \varphi_{\gamma} \), 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 [7] takes the form:

\[
  u = 3, \quad v(t) = \mp 3t, \quad w(t) = -3\left(\frac{3}{4}t^2 + 1\right)
\]

and

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

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

**Corollary 3.** For \( q = \gamma \) Lemma [9] takes the form:

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

and

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

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

It is easily seen that after applying \( \varphi_{\gamma} \) 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 [10] in the language of the computer algebra system Magma.

**Lemma 10.** The maps \( \text{com}_b \), \( \text{com}_b^{-1} \) respectively have an algebraic complexity

\[
3S + 5M_c + 14M + 2I \quad \text{and} \quad 4S + 6M_c + 18M + 3I + CR.
\]

**Proof.** It is easily checked that the basic maps forming \( \text{com}_b \), \( \text{com}_b^{-1} \) have an algebraic complexity as in Table [11]. Therefore we know that of the maps \( \tau_e \), \( \tau_e^{-1} \). Exactly these functions are computed for most arguments. It remains to note that for finding \( v \in \mathbb{F}_p^2 \) (during computation of \( \text{com}_b \)) it is necessary to accomplish two multiplications by the constants \( \zeta_3, \zeta_3^2 \). And vice versa, this is also done to recover the initial value of \( x_1 \)-coordinate (during computation of \( \text{com}_b^{-1} \)). \( \square \)
Table 1: An algebraic complexity of the maps

<table>
<thead>
<tr>
<th>map</th>
<th>( \varrho_\infty )</th>
<th>pr_\infty</th>
<th>( \varrho )</th>
<th>( \sigma )</th>
<th>( \varphi_{\alpha/3} )</th>
<th>( \varphi_\gamma )</th>
<th>pr</th>
<th>( \varrho_\infty^{-1} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>alg. complexity</td>
<td>0</td>
<td>0</td>
<td>I</td>
<td>( S + 4M )</td>
<td>( S + 4M )</td>
<td>( S + 3M_c + 4M )</td>
<td>( 2M + I )</td>
<td>( M_c + I )</td>
</tr>
<tr>
<td>( pr_\infty^{-1} )</td>
<td>( \varrho^{-1} )</td>
<td>( \sigma^{-1} )</td>
<td>( \varphi_{\alpha/3}^{-1} )</td>
<td>( \varphi_\gamma^{-1} )</td>
<td>pr_\infty^{-1}</td>
<td>( 2S + M_c + M + I )</td>
<td>( S + 4M + 2I + CR )</td>
<td>( S + 6M )</td>
</tr>
</tbody>
</table>

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 the 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 \( \sigma \) be its \( \mathbb{F}_q \)-automorphism. If the generalized Kummer surface \( A/\sigma \) 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 \( R_{\mathbb{F}_q'/\mathbb{F}_q}(E_b) \) for any finite field \( \mathbb{F}_q \) of characteristic \( p > 3 \). 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 \( R_b/\mathbb{F}_p \), because compression of its points seemed to us more difficult and important for practice. However, the task of point compression for \( A_{b,b'} \) (so-called double point compression) also has reason to live. 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. Finally, according to Theorem 5 the Jacobian of a hyperelliptic curve \( y^2 = x^5 + b \) (for \( b \in \mathbb{F}_p^* \), \( p > 5 \)) seems to also have the \( \mathbb{F}_p \)-rational generalized Kummer surface.

Double point compression also occurred [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 \( E/\mathbb{F}_{p^2} \). Therefore our approach does not spread immediately to this case. However, over the algebraic closure \( \overline{\mathbb{F}}_p \) there is the unique (up to an isomorphism) superspecial abelian surface. Besides, any endomorphism of \( E^2 \) is defined over \( \mathbb{F}_{p^2} \). Thus every superspecial abelian \( \mathbb{F}_{p^2} \)-surface has an \( \mathbb{F}_{p^2} \)-automorphism \( \sigma \) such that the generalized Kummer surface \( E^2/\sigma \) is geometrically rational. According to Conjecture [11] it is even \( \mathbb{F}_{p^2} \)-rational. Of course, this can be very difficult to find \( \sigma \) and explicit formulas of an \( \mathbb{F}_{p^2} \)-birational isomorphism between \( E^2/\sigma \) and \( \mathbb{A}^2 \).

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 \( K \rightarrow \mathbb{A}^2 \) (or, equivalently, \( \mathbb{A}^2 \rightarrow K \)) 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 $\mathbb{F}_p$ 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 $[\omega]_m := R_{b,m}/\mathbb{F}_p([\omega])$ on the Weil restriction $R_{b,m} := R_{b,m}/\mathbb{F}_p(E_b)$ is no longer rational [56, lem. 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


