# Batch point compression in the context of advanced pairing-based protocols

Dmitrii Koshelev [1]

Computer sciences and networks department, Télécom Paris

**Abstract.** This paper continues author's previous ones about compression of points on elliptic curves $E_b\colon y^2 = x^3 + b$ (with $j$-invariant 0) over a finite field $\mathbb{F}_q$. More precisely, we show in detail how any two (resp. three) points from $E_b(\mathbb{F}_q)$ can be quickly compressed to two (resp. three) elements of $\mathbb{F}_q$ (apart from a few auxiliary bits) in such a way that the corresponding decompression stage requires to extract only one cubic (resp. sextic) root in $\mathbb{F}_q$ (with several multiplications and without inversions). As a result, for many $q$ occurring in practice the new compression-decompression methods are more efficient than the classical one with the two (resp. three) $x$ or $y$ coordinates of the points, which extracts two (resp. three) roots in $\mathbb{F}_q$. We explain why the new methods are useful in the context of modern real-world pairing-based protocols. As a by-product, when $q \equiv 2 \pmod 3$ (in particular, $E_b$ is supersingular), we obtain a two-dimensional analogue of Boneh–Franklin's encoding, that is a way to sample two "independent" $\mathbb{F}_q$-points on $E_b$ at the cost of one cubic root in $\mathbb{F}_q$. Finally, we comment on the case of four and more points from $E_b(\mathbb{F}_q)$.

**Key words:** batch point compression, Boneh–Franklin's encoding, conic bundle structure, cubic and sextic roots, elliptic curves of $j$-invariant 0, Freeman's transformation, generalized Kummer varieties, high 2-adicity, rationality problems, recursive proof systems.

## 1 Introduction

Nowadays, pairing-based cryptography [1] can be certainly considered as an independent fruitful area of public-key cryptography, which is interesting from both mathematical and practical points of view. There are countless pairing-based protocols, many of which have found applications in the real world. It is worth noting protocols based on composite-order groups such as Boneh–Goh–Nissim's (BGN) *somewhat homomorphic encryption* [2] or Boneh–Sahai–Waters's *fully collusion resistant traitor tracing* [3]. It is also impossible not to mention *succinct non-interactive zero-knowledge (NIZK) proofs* among which the most popular one is possibly Groth16 [4]. And their *recursive compositions* are constructed via chains of elliptic curves as first suggested in [5].

Unfortunately, composite-order subgroups of $E_b(\mathbb{F}_q)$ must be very large to be protected against sub-exponential factorization algorithms. By virtue of Hasse's inequality (see, e.g., [1, Theorem 2.9]) we have $\#E_b(\mathbb{F}_q) \approx q$, hence pairing computation on $E_b$ turns out to be very cumbersome as confirmed in [6]. Fortunately, with the help of so-called *Freeman's transformation* [7] (cf. [8, §9-10]) we can almost always rewrite a protocol in the composite-order

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

setting to the prime-order one operating with point vectors from $E_b^n(\mathbb{F}_q)$ for a smaller $q$ and some $n \in \mathbb{N}$. In this case, an instance of the *subgroup decision problem* is a (prime-)order subgroup of $E_b^n(\mathbb{F}_q)$. For the majority of protocols it is sufficient to take $n = 2$, but there are some protocols (such as Katz–Sahai–Waters's *predicate encryption* [7, §7]) needing $n = 3$.

As said, e.g., in [9, §2.2] for the sake of efficiency of recursive proofs one needs to leverage pairing-friendly elliptic curves defined over *highly* 2*-adic fields* $\mathbb{F}_q$, that is the number $q - 1$ should be divided by a non-small power $2^m$, where $m \in \mathbb{N}$. More precisely, this allows to apply the fast Fourier transform (FFT) in order to speed up the polynomial arithmetic over $\mathbb{F}_q$. To be definite, we will suppose that high 2-adicity takes place if $m \geqslant 3$, but in practice usually $20 < m < 60$. Our choice follows from the fact that (as is known, e.g., from [1, §5.1.7]) for $q \equiv 1 \pmod 8$ it is problematic to express a square root in $\mathbb{F}_q$ via one exponentiation. Of course, we can always utilize Tonelli–Shanks's algorithm, namely [1, Algorithm 5.14] (cf. [10]), but it has a greater computational complexity.

Recall that curves $E_b$ are ordinary (a.k.a. non-supersingular) only if $q \equiv 1 \pmod 3$ or, equivalently, a primitive cubic root $\omega := \sqrt[3]{1}$ lies in $\mathbb{F}_q$. Since only curves $E_b$ possess order 6 automorphism (of the form $[-\omega](x, y) = (\omega x, -y)$), according to [1, §3.2.5] such pairing-friendly ordinary curves are preferred in pairing-based cryptography. To our knowledge, at the moment, the most popular curves are BLS12-381 [11, §4.2.1] for a general use and BLS12-377 [9, Table 2] for one layer proof composition, where the numbers after the hyphen equal $\lceil \log_2(q) \rceil$. Moreover, the field $\mathbb{F}_q$ of the latter curve (in contrast to the former one) is highly 2-adic with $m = 46$. Among other things, the pages [12], [13] specify 2-cycles of curves of $j$-invariant 0 (over highly 2-adic fields) among which only one is pairing-friendly.

In compliance with [14, Examples IV.1.3.5-6] elliptic curves are not *rational*. Therefore from the geometric point of view the most compact representation of them is on the affine plane $\mathbb{A}^2_{(x,y)}$, for example in the Weierstrass form. Consequently, any point from $E_b^n(\mathbb{F}_q) \subset \mathbb{F}_q^{2n}$ is obviously represented with the help of $2n\lceil \log_2(q) \rceil$ bits. In particular, for $n = 2$ (resp. $n = 3$) and $\log_2(q) \approx 380$ we obtain $\approx 1520$ (resp. $\approx 2280$) bits, which is quite a lot. In comparison, with the same 128-bit security level classical (i.e., non-pairing-friendly) elliptic curves are defined over 256-bit fields $\mathbb{F}_q$. And many widespread cryptosystems on such curves (e.g., ECDH or ECDSA) don't require simultaneous compressing several points, so it is sufficient to manipulate only 512 bits.

At the same time, by virtue of Hasse's inequality $\mathbb{F}_q$-points on $E_b$ can be compressed to about half with regard to the information theory. There is the classical compression-decompression method representing a point as its $x$ (resp. $y$) coordinate in addition to one (resp. two) bits to uniquely recover the initial $y$ (resp. $x$) coordinate via extracting in $\mathbb{F}_q$ the square (resp. cubic) root. In comparison with standard arithmetical operations in $\mathbb{F}_q$, the latter one is very costly, because even for thoroughly chosen $q$ it consists in one exponentiation in $\mathbb{F}_q$. As a result, after compressing $\mathbb{F}_q$-point vectors of length $n = 2$ (resp. $n = 3$) we obtain $\approx 760$ (resp. $\approx 1140$) bits at the price of $n$ exponentiations in the decompression stage.

Apart from $\tau_6 := [-\omega]$ there are on $E_b$ the automorphisms

$$\tau_2 := \tau_6^3 \colon (x, y) \mapsto (x, -y), \qquad \tau_3 := \tau_6^4 \colon (x, y) \mapsto (\omega x, y)$$

of orders 2 and 3 respectively. For any $n \in \mathbb{N}$ and $m \in \{2, 3, 6\}$ consider the diagonal subgroup $G_{n,m} := \langle(\tau_m, \ldots, \tau_m)\rangle \simeq \mathbb{Z}/m$ of the automorphism group on $E_b^n$. Notice that it is Frobenius invariant even if $\omega \not\in \mathbb{F}_q$. Further, introduce the $\mathbb{F}_q$-quotient $GK_{n,m} := E_b^n/G_{n,m}$, which is called *generalized Kummer variety* [15, §7], because for $m = 2$ this is a (usual) *Kummer variety* [15, Example 8.1]. Also, we need the notation of the quotient $\mathbb{F}_q$-cover $\varphi_{n,m}\colon E_b^n \to GK_{n,m}$, which, as usual [14, Theorem I.4.4], gives the function field extension $\mathbb{F}_q(GK_{n,m}) \hookrightarrow \mathbb{F}_q(E_b^n)$. Whenever $m = 2$ or $\omega \in \mathbb{F}_q$, by virtue of Artin's theorem (see, e.g., [16, Theorem VI.1.8]) $\varphi_{n,m}$ is a Galois cover whose the Galois group equals $G_{n,m}$. Therefore $\varphi_{n,m}$ is a *Kummer cover* due to [16, Theorem VI.6.2]. All of the above is illustrated with the famous examples $\varphi_{1,2}(x,y) = x$ and $\varphi_{1,3}(x,y) = y$.

We see that $GK_{1,m}$ are obviously rational curves. More generally, there is the analogous notion of *(geometrically) rational variety* as defined in [14, Example II.8.20.1]. Rationality of the surfaces $GK_{2,3}$, $GK_{2,6}$ is a classical fact. According to [17, §2] the threefold $GK_{3,6}$ is also rational and there are [18, Questions 1.3, 1.4] about rationality of $GK_{4,6}$, $GK_{5,6}$. In turn, the varieties $GK_{n,m}$ are never rational for $n \geqslant m$ in accordance with [15, Example 8.10], [17, Remark 2.9]. In fact, we are interested in $\mathbb{F}_q$-rationality of $GK_{n,m}$. In a cryptographic context this concept [19, Definition 6.1] first arose in so-called *torus-based cryptography* for compressing $\mathbb{F}_q$-points of *algebraic tori*. By the way, since pairing values can be interpreted as such points, this compression technique is known to be useful in pairing-based cryptography.

For the Kummer covers $\varphi_{n,m}$ computing an inverse image $\varphi_{n,m}^{-1}(P)$ of a point $P \in \varphi_{n,m}\big(E_b^n(\mathbb{F}_q)\big)$ can be implemented by means of extracting in $\mathbb{F}_q$ some root of degree $m$. Suppose that $GK_{n,m}$ is an $\mathbb{F}_q$-rational variety and there are explicit formulas of a birational $\mathbb{F}_q$-isomorphism $\psi_{n,m}\colon GK_{n,m} \overset{\simeq}{\dashrightarrow} \mathbb{A}^n$ and its inverse $\psi_{n,m}^{-1}\colon \mathbb{A}^n \overset{\simeq}{\dashrightarrow} GK_{n,m}$. As is customary in algebraic geometry, the arrow $\dashrightarrow$ (resp. $\overset{\simeq}{\dashrightarrow}$) means a (bi)rational map rather than an (iso)morphism, that is the map may be undefined at some points. Treating them separately, we thus get a new compression-decompression method for all $\mathbb{F}_q$-points on $E_b^n$. Indeed, the compression (resp. decompression) stage consists in evaluating the map $\chi_{n,m} := \psi_{n,m} \circ \varphi_{n,m}$ at a general point $Q \in E_b^n(\mathbb{F}_q)$ (resp. finding $\chi_{n,m}^{-1}(R)$, where $R := \chi_{n,m}(Q)$).

For the surface $GK_{2,3}$ (resp. $GK_{2,6}$) $\mathbb{F}_q$-rationality is explicitly established in §2 (resp. [20, §2-3]), although these results can't be considered very important for pure mathematics because of their simplicity. Besides, it turns out that $\mathbb{F}_q$-formulas of $\psi_{3,6}^{\pm 1}$, derived in [17, §2] for $b = -1$, are still valid for any $b \in \mathbb{F}_q^*$. However if the field $\mathbb{F}_q$ is not highly 2-adic, to compress points from $E_b^2(\mathbb{F}_q)$ (resp. $E_b^3(\mathbb{F}_q)$) we apply in §4 slightly another approach based on $\mathbb{F}_q$-rationality of $GK_{1,3}$ (resp. $GK_{2,3}$). Nevertheless, since the varieties $GK_{n,3}$ are not rational for $n > 2$, we can only hope for breakthroughs concerning $\mathbb{F}_q$-rationality of $GK_{4,6}$, $GK_{5,6}$. At the same time, cryptographers rarely come across protocols, obtained by Freeman's transformation, manipulating $\mathbb{F}_q$-point vectors of length greater than three.

We know that under the condition $q \equiv 2 \pmod 3$ a curve $E_b$ is supersingular and every element of $\mathbb{F}_q$ has a unique cubic root in $\mathbb{F}_q$. Moreover, in accordance with [21, Theorem 3.3.15] the group $E_b(\mathbb{F}_q) \simeq \mathbb{Z}/(q+1)$. Although $\varphi_{n,3}$ are no longer Galois covers, we still can find the inverse image under $\varphi_{n,3}$ via extracting a cubic root in $\mathbb{F}_q$. In particular, $\varphi_{1,3}^{-1}\colon \mathbb{F}_q \to E_b(\mathbb{F}_q)$ and $\varphi_{2,3}^{-1}\colon GK_{2,3}(\mathbb{F}_q) \to E_b^2(\mathbb{F}_q)$ are true maps. The former is widely known as *Boneh–Franklin's encoding* [1, §8.3.2]. The latter gives rise to the new encoding $\chi_{2,3}^{-1}\colon \mathbb{F}_q^2 \to E_b^2(\mathbb{F}_q)$, because points of a (possibly reducible) $\mathbb{F}_q$-curve, where $\psi_{2,3}^{-1}$ is not defined, as usual, can be easily processed independently. Thus $\chi_{2,3}^{-1}$ allows to generate in constant time two "independent" $\mathbb{F}_q$-points on $E_b$ twice as efficient as $\varphi_{1,3}^{-1}$ applied two times. "Independency" means that the discrete logarithm between these points is unknown to anyone.

As far as we know, at the moment, supersingular curves are not preferable in the pairing context, because of their small embedding degrees ($\leqslant 3$ in a large characteristic [1, §4.3]). The only exception is a recent *verifiable delay function (VDF)* developed in [22], where pairings are combined with isogenies. However this and other isogeny-based protocols (such as SIDH [23] or CSIDH [24]) deal with many supersingular curves. Of course, (C)SIDH has one starting curve, which may be of $j$-invariant 0, but these protocols don't require to (often) sample points on it. We hope that in the near future advanced isogeny-based protocols will appear for which the task of efficient regular sampling on the starting curve is important.

An idea of batch compressing points on an elliptic $\mathbb{F}_q$-curve is not new. It has already arisen in [25] for any number $n \in \mathbb{N}$ of points (and not necessarily for $j$-invariant 0) under the name *multiple point compression* similarly to *double* one in [26]. The methods of these papers compress to $n+1$ elements of $\mathbb{F}_q$ (i.e., the representation is not optimal), however their decompression stages don't need to extract any roots. If $n$ is large, then this approach is expected to be the best trade-off between compactness and efficiency. Nevertheless, for small $n$ our approach is the best if bandwidth/memory is more critical than speed.

# 2 Derivation of formulas

By analogy with [27, Theorem 9], we have

**Lemma 1.** *There is (up to a birational $\mathbb{F}_q$-isomorphism) the affine model*

$$GK_{2,3} = (y_1^2 - b)t^3 - (y_0^2 - b) \quad \subset \quad \mathbb{A}^3_{(t,y_0,y_1)}$$

*for which the corresponding quotient map has the form*

$$\varphi_{2,3}\colon E_b^2 \dashrightarrow GK_{2,3} \qquad (x_0, y_0, x_1, y_1) \mapsto \Big(\frac{x_0}{x_1}, y_0, y_1\Big).$$

**Theorem 1.** *The generalized Kummer surface $GK_{2,3}$ is $\mathbb{F}_q$-rational.*

*Proof.* We borrow the approach used for proving [27, Theorem 12]. It is based on the theory of *conic bundles* (see, e.g., [27, §1.4]), but the reader can verify the formulas below (e.g., in Magma [28]) without knowledge of this theory. There is the natural conic bundle structure

$$\pi\colon GK_{2,3} \to \mathbb{A}^1_t \qquad (t, y_0, y_1) \mapsto t.$$

In other words, $GK_{2,3}$ can be seen as an $\mathbb{F}_q(t)$-conic. In a diagonal form,

$$GK_{2,3} = -y_0^2 + t^3 y_1^2 + b(1 - t^3).$$

Therefore the degenerate (i.e., reducible or, equivalently, singular) fibers of $\pi$ lie over $t \in \{0, \infty\} \cup \{\omega^i\}_{i=0}^2$, where $\infty := (1:0) \in \mathbb{P}^1$. More precisely, for these $t$ we see that $\pi^{-1}(t) = L_t^+ \cup L_t^-$, where

$$L_0^{\pm} := \begin{cases} t = 0, \\ y_0 = \pm\sqrt{b}, \end{cases} \qquad L_\infty^{\pm} := \begin{cases} t = \infty, \\ y_1 = \pm\sqrt{b}, \end{cases} \qquad L_{\omega^i}^{\pm} := \begin{cases} t = \omega^i, \\ y_1 = \pm y_0. \end{cases}$$

First, after the transformation

$$\tau := \begin{cases} z_0 := y_0, \\ z_1 := ty_1, \end{cases} \qquad \tau^{-1} = \begin{cases} y_0 := z_0, \\ y_1 := z_1/t \end{cases}$$

we obtain the cubic surface

$$GK'_{2,3} := \tau(GK_{2,3}) \; = \; -z_0^2 + tz_1^2 + b(1-t^3) \quad \subset \quad \mathbb{A}^3_{(t,z_0,z_1)}.$$

We then *blow down* [14, §V.3] one of the components $\tau(L_1^{\pm})$ by means of the transformation

$$\theta := \begin{cases} y_0 := \dfrac{z_0 - z_1}{1-t}, \\ y_1 := \dfrac{z_0 - tz_1}{1-t}, \end{cases} \qquad \theta^{-1} = \begin{cases} z_0 := -ty_0 + y_1, \\ z_1 := -y_0 + y_1, \end{cases}$$

coming to

$$S := \theta(GK'_{2,3}) \; = \; ty_0^2 - y_1^2 + b(t^2+t+1) \quad \subset \quad \mathbb{A}^3_{(t,y_0,y_1)}.$$

Further, simultaneous blowing down some pair of components over $t \in \{\omega, \omega^2\}$ has the form

$$\eta := \begin{cases} z_0 := \dfrac{(t+1)y_0 + y_1}{t^2+t+1}, \\ z_1 := \dfrac{ty_0 + (t+1)y_1}{t^2+t+1}, \end{cases} \qquad \eta^{-1} = \begin{cases} y_0 := (t+1)z_0 - z_1, \\ y_1 := -tz_0 + (t+1)z_1, \end{cases}$$

which gives the simpler surface

$$T := \eta(S) \; = \; tz_0^2 - z_1^2 + b \quad \subset \quad \mathbb{A}^3_{(t,z_0,z_1)}.$$

Note that the maps $\tau$, $\theta$, $\eta$ respect the conic bundle $\pi$, that is they can be seen as $\mathbb{F}_q(t)$-isomorphisms of conics. That's why we avoid the tautology $t := t$ in their description. Finally, the projection $pr\colon T \overset{\sim}{\dashrightarrow} \mathbb{A}^2_{(z_0,z_1)}$ is a desired map, because $t = (z_1^2 - b)/z_0^2$. □

For the compositions $\psi_{2,3} := pr \circ \eta \circ \theta \circ \tau$ and $\chi_{2,3} := \psi_{2,3} \circ \varphi_{2,3}$ Magma [28] says that

$$\chi_{2,3}\colon E_b^2 \dashrightarrow \mathbb{A}^2_{(z_0,z_1)} \qquad \chi_{2,3} = \begin{cases} z_0 := \dfrac{x_1(2x_0^2y_1 - x_0x_1(y_0 - y_1) - 2y_0x_1^2)}{y_0^2 - y_1^2}, \\ z_1 := \dfrac{x_0^3y_1 + 2x_0x_1(x_0y_1 - y_0x_1) - y_0x_1^3}{y_0^2 - y_1^2}, \end{cases}$$

$$\psi_{2,3}^{-1}\colon \mathbb{A}^2_{(z_0,z_1)} \overset{\sim}{\dashrightarrow} GK_{2,3} \qquad \psi_{2,3}^{-1} = \begin{cases} t := \dfrac{z_1^2 - b}{z_0^2}, \\ y_0 := \dfrac{z_0^3z_1 - 2z_0(z_0 - z_1)(z_1^2 - b) - (z_1^2 - b)^2}{z_0^3}, \\ y_1 := -\dfrac{z_0^2(z_0 - 2z_1) + (2z_0 - z_1)(z_1^2 - b)}{z_1^2 - b}. \end{cases}$$

Let's consider the cases when the denominators equal zero. Obviously, $t \in \{0, \infty\} \Rightarrow x_0 x_1 = 0$, and

$$y_0^2 - y_1^2 = 0 \quad \Leftrightarrow \quad \exists k \in \mathbb{Z}/6 \colon (x_1, y_1) = [-\omega]^k (x_0, y_0).$$

In turn, it is readily checked that $z_0 = 0$ (i.e., $z_1 = \pm\sqrt{b}$ under the condition $t \neq 0$) if and only if $(t, y_0, y_1) \in \mathrm{Im}(\varrho_\pm)$ for the sections of $\pi$ given by

$$\varrho_\pm \colon \mathbb{A}^1_t \dashrightarrow GK_{2,3} \qquad \varrho_\pm := \begin{cases} y_0 := \pm\sqrt{b}(2t+1), \\ y_1 := \dfrac{\pm\sqrt{b}(t+2)}{t}. \end{cases}$$

# 3 New method for two points

We need the auxiliary sets

$$V' := \big\{(x,y) \in E_b \mid xy = 0\big\} \cup \big\{(0:1:0)\big\} \quad \subset \quad E_b[2] \cup E_b[3],$$

$$V := E_b \times V' \;\cup\; V' \times E_b.$$

Formally, for two points $P_i = (x_i, y_i)$ from $E_b(\mathbb{F}_q) \setminus V'$ the new compression map has the form

$$\mathrm{com}_{2,3} \colon E_b^2(\mathbb{F}_q) \setminus V \quad \hookrightarrow \quad \mathbb{F}_q^2 \times [0,5] \times [0,2]$$

$$\mathrm{com}_{2,3}(P_0, P_1) := \begin{cases} (x_0, y_0, k, 0) & \text{if} \quad \exists k \in \mathbb{Z}/6 \colon P_1 = [-\omega]^k(P_0), \\ (t, x_1, k, 1) & \text{if} \quad \big(t, (-1)^k y_0, (-1)^k y_1\big) \in \mathrm{Im}(\varrho_+), \\ (z_0, z_1, n, 2) & \text{otherwise}, \end{cases}$$

where $(z_0, z_1) = \chi_{2,3}(P_0, P_1)$ and $n \in [0,2]$ is the position number of the element $x_1 \in \mathbb{F}_q^*$ in the set $\big\{\omega^i x_1\big\}_{i=0}^2 \cap \mathbb{F}_q^*$ with respect to some order in $\mathbb{F}_q^*$. For example, in the case of a prime $q$ this can be the usual numerical one. The set $[0,5] \times [0,2]$ clearly requires 5 bits for representing its elements. Since in discrete logarithm cryptography points of small orders don't occur, we omit the definition of the compression map on $V(\mathbb{F}_q)$ for the sake of simplicity, although it can be easily defined if desired.

The corresponding decompression map is given as follows:

$$\mathrm{com}_{2,3}^{-1} \colon \mathrm{Im}(\mathrm{com}_{2,3}) \quad \xrightarrow{\sim} \quad E_b^2(\mathbb{F}_q) \setminus V$$

$$\mathrm{com}_{2,3}^{-1}(z_0, z_1, m, \ell) = \begin{cases} (z_0, z_1, x_1, y_1) & \text{if} \quad \ell = 0 \quad \text{and} \quad (x_1, y_1) = [-\omega]^m (z_0, z_1), \\ (z_0 z_1, y_0, z_1, y_1) & \text{if} \quad \ell = 1 \quad \text{and} \quad \big((-1)^m y_0, (-1)^m y_1\big) = \varrho_+(z_0), \\ (t x_1, y_0, x_1, y_1) & \text{if} \quad \ell = 2 \quad \text{and} \quad (t, y_0, y_1) = \psi_{2,3}^{-1}(z_0, z_1), \end{cases}$$

where for $\ell = 2$ the initial $x_1 = \sqrt[3]{g_1}$ (for $g_1 := y_1^2 - b$) can be determined with the help of $m = n$. According to [29, Equalities (2), (3)] and similar ones for other $q \not\equiv 1 \pmod{27}$ this cubic root can be extracted at the cost of one exponentiation in $\mathbb{F}_q$ (in particular, without inverting the denominator of $g_1$, namely $(z_1^2 - b)^2$).

Since the projective or *Jacobian coordinates* [1, §2.3.2, §10.7.9] are preferred in practice, the decompression stage doesn't require finding inverse elements at all. By definition, in these coordinates the curve $E_b$ possesses the equations

$$\overline{E_b}\colon Y^2Z = X^3 + bZ^3, \qquad \overline{E_b}\colon Y^2 = X^3 + bZ^6$$

respectively. And there are the birational isomorphisms

$$\sigma\colon \overline{E_b} \overset{\simeq}{\dashrightarrow} E_b \qquad (X:Y:Z) \mapsto \left(\frac{X}{Z}, \frac{Y}{Z}\right), \qquad (X:Y:Z) \mapsto \left(\frac{X}{Z^2}, \frac{Y}{Z^3}\right)$$

respectively. By the way, in both cases,

$$\sigma^{-1}\colon E_b \overset{\simeq}{\dashrightarrow} \overline{E_b} \qquad (x,y) \mapsto (x:y:1).$$

If the compression stage starts from the projective or Jacobian coordinates, then even in the classical method it is necessary to compute one inverse in $\mathbb{F}_q$. Indeed, given two points $(X_i : Y_i : Z_i) \in \overline{E_b}(\mathbb{F}_q)$ with $Z_i \neq 0$ one needs the value $v := (Z_0Z_1)^{-1}$ in order to get $Z_0^{-1} = vZ_1$ and $Z_1^{-1} = vZ_0$. This famous trick is clearly generalized to any number of inversions. In turn, in the compression stage of the new method instead of the two inversions $v$, $(y_0^2 - y_1^2)^{-1}$ only one is also enough, because

$$\chi_{2,3} \circ \sigma^{\times 2} = \left(\frac{\mathrm{num}_0}{\mathrm{den}}, \frac{\mathrm{num}_1}{\mathrm{den}}\right)\colon \quad \overline{E_b}^2 \dashrightarrow \mathbb{A}^2_{(z_0,z_1)}$$

for some polynomials $\mathrm{num}_i$, $\mathrm{den} \in \mathbb{F}_q[X_i, Y_i, Z_i]_{i=0}^1$ trivially obtained from the formulas of $\chi_{2,3}$. To determine the position number $n$ one needs to know $Z_1^{-1}$, hence we should in fact invert $Z_1 \cdot \mathrm{den}$. Finally, it is worth emphasizing that all of the above is equally valid for the degenerate cases $\ell \in \{0, 1\}$.

# 4 Folklore method for two points and its variation for three ones

First, we put $f_i := x_i^3 + b$ and $g_i := y_i^2 - b$. Since the numbers 2, 3 are relatively prime, the roots $y_0 = \sqrt{f_0}$ and $x_1 = \sqrt[3]{g_1}$ can be extracted simultaneously, that is at the cost of a sixth root in $\mathbb{F}_q$. Indeed, for $h := f_0^3 g_1^2$ it is sufficient to compute $\alpha := \sqrt[6]{h} = \sqrt{f_0}\sqrt[3]{g_1}$, because $\sqrt[3]{g_1} = f_0g_1/\alpha^2$ and $\sqrt{f_0} = \alpha/\sqrt[3]{g_1}$. Moreover, by analogy with [20, §3], whenever $q \not\equiv 1 \pmod 8$, $q \not\equiv 1 \pmod{27}$, the value $\alpha$ can be expressed via one exponentiation in $\mathbb{F}_q$.

Thus there is the compression map

$$E_b^2(\mathbb{F}_q) \setminus V \quad \hookrightarrow \quad \mathbb{F}_q^2 \times [0,5] \qquad\qquad (P_0, P_1) \mapsto (x_0, y_1, n),$$

where $n \in [0,5]$ is the position number of the element $y_0x_1 \in \mathbb{F}_q^*$ in the set $\big\{(-1)^i\omega^j \cdot y_0x_1\big\}_{i=0,j=0}^{1,2} \cap \mathbb{F}_q^*$ with respect to some order in $\mathbb{F}_q^*$. As above, $n$ is used in the decompression stage for recovering the original $y_0$, $x_1$.

Notice that at the heart of this method is $\mathbb{F}_q$-rationality of $E_b^2/G = E_b/G_{1,2} \times E_b/G_{1,3}$, where $G := G_{1,2} \times G_{1,3} \simeq \mathbb{Z}/6$. We call it folklore, because it doesn't require an algebraic

|  | Galois group | compression | decompression |
|---|---|---|---|
| classical method with $x_0$, $x_1$ | $G_{1,2}^2$ | one inversion | two $\sqrt{\cdot}$ |
| classical method with $y_0$, $y_1$ | $G_{1,3}^2$ |  | two $\sqrt[3]{\cdot}$ |
| folklore method with $x_0$, $y_1$ | $G_{1,2}\times G_{1,3}$ |  | one $\sqrt[6]{\cdot}$ |
| new method with $z_0$, $z_1$ | $G_{2,3}$ |  | one $\sqrt[3]{\cdot}$ |

Table 1: Worst-case complexity for compressing $\overline{E_b}^2(\mathbb{F}_q)$ (with respect to the projective or Jacobian coordinates)

geometry technique, so perhaps someone already knows it. However the significant drawback of the method consists in the fact that (in contrast to $\mathrm{com}_{2,3}$) it doesn't work over highly 2-adic fields $\mathbb{F}_q$. The same drawback exists for author's other method [20, §2-3] based on $\mathbb{F}_q$-rationality of $GK_{2,6}$. Since the folklore one has a slightly simpler definition, we conclude that it is more preferred for use when possible.

Similarly, one can apply the folklore method ideology to the new method with $z_0$, $z_1$ in order to compress three points $P_i = (x_i, y_i)$ from $E_b(\mathbb{F}_q) \setminus V'$. As earlier, consider the set

$$V := E_b^2 \times V' \ \cup\ E_b \times V' \times E_b \ \cup\ V' \times E_b^2.$$

It is about the compression map

$$E_b^3(\mathbb{F}_q) \setminus V \quad\hookrightarrow\quad \mathbb{F}_q^3 \times [0,5] \times [0,2] \times [0,1] \qquad\qquad (P_0, P_1, P_2) \mapsto (z_0, z_1, x_2, n, s),$$

where $(z_0, z_1, m, \ell) = \mathrm{com}_{2,3}(P_0, P_1)$ and in the non-degenerate case $\ell = 2$ the number $n \in [0,5]$ is the position of the element $x_1y_2 \in \mathbb{F}_q^*$. In turn, for $\ell \in \{0,1\}$ we put $n := m$ and the additional sign bit $s$ is utilized to recover $y_2$ (regardless of $P_0$, $P_1$). Since for these $\ell$ the latter points are obtained without root computations, the overall complexity doesn't go beyond one exponentiation in $\mathbb{F}_q$.

Besides, pay attention that for $\ell = 2$ the root $\sqrt[6]{h}$ (where $h := g_1^2 f_2^3$) can still be found at the cost of one exponentiation in $\mathbb{F}_q$ even if the inverse of the denominator of $h$ (i.e., of $g_1^2$) is unknown. By analogy with $\sqrt{\cdot}$ (see, e.g., [30, §5]) and $\sqrt[3]{\cdot}$, in [31, §2] we explain how to do this for $q \equiv 3 \pmod 4$, $q \equiv 2 \pmod 3$, or, equivalently, $q \equiv 11 \pmod{12}$. We invite the reader to independently check that this trick is easily generalized to other $q \not\equiv 1 \pmod 8$, $q \not\equiv 1 \pmod{27}$.

Thus we completely justified Tables 1, 2, which contain a complexity comparison (all the operations are carried out in $\mathbb{F}_q$) of the compression-decompression methods for two and three points respectively. As is customary, the addition, subtraction, and multiplication operations in $\mathbb{F}_q$ are omitted, because they are much cheaper. Let us stress that arguments of this paper, related to avoiding the inversion operation, are equally valid for author's previous compression-decompression methods. In other words, the number of inversions in [27, Theorem 13] and [20, Tables 1, 2] can be actually reduced to only one in the compression stage (at the price of several multiplications).

|  | Galois group | compression | decompression |
|---|---|---|---|
| classical method with $x_0$, $x_1$, $x_2$ | $G_{1,2}^3$ | one inversion | three $\sqrt{\cdot}$ |
| classical method with $y_0$, $y_1$, $y_2$ | $G_{1,3}^3$ |  | three $\sqrt[3]{\cdot}$ |
| folklore-classical method with $x_0$, $x_1$, $y_2$ | $G_{1,2}^2 \times G_{1,3}$ |  | one $\sqrt[6]{\cdot}$ and one $\sqrt{\cdot}$ |
| folklore-classical method with $x_0$, $y_1$, $y_2$ | $G_{1,2} \times G_{1,3}^2$ |  | one $\sqrt[6]{\cdot}$ and one $\sqrt[3]{\cdot}$ |
| new method with $z_0$, $z_1$, $x_2$ | $G_{2,3} \times G_{1,2}$ |  | one $\sqrt[6]{\cdot}$ |

Table 2: Worst-case complexity for compressing $\overline{E_b}^3(\mathbb{F}_q)$ (with respect to the projective or Jacobian coordinates)

# References

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

[2] Boneh D., Goh E. J., Nissim K., "Evaluating 2-DNF formulas on ciphertexts", Theory of Cryptography Conference 2005, LNCS, **3378**, ed. Kilian J., Springer, Berlin, Heidelberg, 2005, 325–341.

[3] Boneh D., Sahai A., Waters B., "Fully collusion resistant traitor tracing with short ciphertexts and private keys", Advances in Cryptology — EUROCRYPT 2006, LNCS, **4004**, ed. Vaudenay S., Springer, Berlin, Heidelberg, 2006, 573–592.

[4] Groth J., "On the size of pairing-based non-interactive arguments", Advances in Cryptology — EUROCRYPT 2016, LNCS, **9665**, eds. Fischlin M., Coron J.-S., Springer, Berlin, Heidelberg, 2016, 305–326.

[5] Ben-Sasson E., Chiesa A., Tromer E., Virza M., "Scalable zero knowledge via cycles of elliptic curves", Advances in Cryptology — CRYPTO 2014, LNCS, **8617**, eds. Garay J. A., Gennaro R., Springer, Berlin, Heidelberg, 2014, 276–294.

[6] Guillevic A., "Comparing the pairing efficiency over composite-order and prime-order elliptic curves", Applied Cryptography and Network Security 2013, LNCS, **7954**, eds. Jacobson M., Locasto M., Mohassel P., Safavi-Naini R., Springer, Berlin, Heidelberg, 2013, 357–372.

[7] Freeman D. M., "Converting pairing-based cryptosystems from composite-order groups to prime-order groups", Advances in Cryptology — EUROCRYPT 2010, LNCS, **6110**, eds. Gilbert H., Springer, Berlin, Heidelberg, 2010, 44–61.

[8] Groth J., Sahai A., "Efficient non-interactive proof systems for bilinear groups", Advances in Cryptology – EUROCRYPT 2008, LNCS, **4965**, eds. Smart N., Springer, Berlin, Heidelberg, 2008, 415–432.

[9] El Housni Y., Guillevic A., "Optimized and secure pairing-friendly elliptic curves suitable for one layer proof composition", Cryptology and Network Security 2020, LNCS, **12579**, eds. Krenn S., Shulman H., Vaudenay S., Springer, Cham, 2020, 259–279.

[10] Sarkar P., *Computing square roots faster than the Tonelli–Shanks/Bernstein algorithm*, https://eprint.iacr.org/2020/1407.

[11] Sakemi Y., Kobayashi T., Saito T., Wahby R. S., *Pairing-friendly curves*, https://datatracker.ietf.org/doc/draft-irtf-cfrg-pairing-friendly-curves, 2021.

[12] Hopwood D., *The pasta curves for Halo 2 and beyond*, https://electriccoin.co/blog/the-pasta-curves-for-halo-2-and-beyond, 2020.

[13] Hopwood D., *Pluto/Eris supporting evidence*, https://github.com/daira/pluto-eris, 2021.

[14] Hartshorne R., *Algebraic Geometry*, Graduate Texts in Mathematics, **52**, Springer, New York, 1977.

[15] Ueno K., "Classification of algebraic varieties, I", *Compositio Mathematica*, **27**:3 (1973), 277–342.

[16] Lang S., *Algebra*, Graduate Texts in Mathematics, **211**, Springer, New York, 2002.

[17] Oguiso K., Truong T. T., "Explicit examples of rational and Calabi–Yau threefolds with primitive automorphisms of positive entropy", *Journal of Mathematical Sciences, the University of Tokyo*, **22** (2015), 361–385.

[18] Catanese F., Oguiso K., Verra A., "On the unirationality of higher dimensional Ueno-type manifolds", *Revue Roumaine de Mathématiques Pures et Appliquées*, **60**:3 (2015), 337–353.

[19] Rubin K., Silverberg A., "Compression in finite fields and torus-based cryptography", *SIAM Journal on Computing*, **37**:5 (2008), 1401–1428.

[20] Koshelev D., *Faster point compression for elliptic curves of $j$-invariant* 0, https://eprint.iacr.org/2020/010, accepted in Mathematical Aspects of Cryptography, 2021.

[21] Tsfasman M., Vlăduţ S., Nogin D., *Algebraic Geometric Codes: Basic Notions*, Mathematical Surveys and Monographs, **139**, American Mathematical Society, Providence, 2007.

[22] De Feo L., Masson S., Petit C., Sanso A., "Verifiable delay functions from supersingular isogenies and pairings", Advances in Cryptology — ASIACRYPT 2019, LNCS, **11921**, eds. Galbraith S., Moriai S., Springer, Cham, 2019, 248–277.

[23] Jao D., De Feo L., "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies", PQCrypto 2011, LNCS, **7071**, eds. Yang B.-Y., Springer, Berlin, Heidelberg, 2011, 19–34.

[24] Castryck W., Lange T., Martindale C., Panny L., Renes J., "CSIDH: an efficient post-quantum commutative group action", Advances in Cryptology — ASIACRYPT 2018, LNCS, **11274**, eds. Peyrin T., Galbraith S., Springer, Cham, 2018, 395–427.

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

[26] Khabbazian M., Gulliver T. A., Bhargava V. K., "Double point compression with applications to speeding up random point multiplication", *IEEE Transactions on Computers*, **56**:3 (2007), 305–313.

[27] Koshelev D., "New point compression method for elliptic $\mathbb{F}_{q^2}$-curves of $j$-invariant 0", *Finite Fields and Their Applications*, **69** (2021), Article 101774.

[28] Koshelev D., *Magma code*, https://github.com/dishport/Batch-point-compression-in-the-context-of-advanced-pairing-based-protocols, 2021.

[29] Koshelev D., *Indifferentiable hashing to ordinary elliptic $\mathbb{F}_q$-curves of $j = 0$ with the cost of one exponentiation in $\mathbb{F}_q$*, https://eprint.iacr.org/2021/301, accepted in Designs, Codes and Cryptography, 2021.

[30] Bernstein D. J., Duif N., Lange T., Schwabe P., Yang B.-Y., "High-speed high-security signatures", *Journal of Cryptographic Engineering*, **2**:2 (2012), 77–89.

[31] Koshelev D., *Some remarks on how to hash faster onto elliptic curves*, https://eprint.iacr.org/2021/1082, 2021.