Faster point compression for elliptic curves of j-invariant 0

Dmitrii Koshelev

Versailles Saint-Quentin-en-Yvelines University, France
Infotecs, Russia
Institute for Information Transmission Problems, Russia

dimitri.koshelev@gmail.com
https://www.researchgate.net/profile/Dimitri-Koshelev

Abstract

The article provides a new double point compression method (to $2\lceil \log_2(q) \rceil + 4$ bits) for an elliptic curve $E_b\colon y^2 = x^3 + b$ of j-invariant 0 over a finite field $\mathbb{F}_q$ such that $q \equiv 1 \pmod 3$. More precisely, we obtain explicit simple formulas transforming the coordinates x_0, y_0, x_1, y_1 of two points $P_0, P_1 \in E_b(\mathbb{F}_q)$ to some two elements of $\mathbb{F}_q$ with four auxiliary bits. In order to recover (in the decompression stage) the points P_0, P_1 it is proposed to extract a sixth root $\sqrt[6]{Z} \in \mathbb{F}_q$ of some element $Z \in \mathbb{F}_q$. It is known that for $q \equiv 3 \pmod 4$, $q \not\equiv 1 \pmod{27}$ this can be implemented by means of just one exponentiation in $\mathbb{F}_q$. Therefore the new compression method seems to be much faster than the classical one with the coordinates x_0, x_1, whose decompression stage requires two exponentiations in $\mathbb{F}_q$. We also successfully adapt the new approach for compressing one $\mathbb{F}_{q^2}$-point on a curve E_b with $b \in \mathbb{F}_{q^2}^*$.

Keywords: finite fields, pairing-based cryptography, elliptic curves of j-invariant 0, point compression.

1 Introduction

In many protocols of elliptic cryptography one needs a *compression method* for points of an elliptic curve E over a finite field $\mathbb{F}_q$ of characteristic p. This is done for quick transmission of the information over a communication channel or for its compact storage in a memory. There exists a classical method, which considers an $\mathbb{F}_q$-point on $E \subset \mathbb{A}^2_{(x,y)}$ as the x-coordinate with one auxiliary bit to uniquely recover the y-coordinate by solving the quadratic equation over $\mathbb{F}_q$.

Consider an elliptic curve $E_b\colon y^2 = x^3 + b$ for $b \in \mathbb{F}_q^*$, which is of j-invariant 0. Ordinary curves of such the form have become very useful in elliptic cryptography, especially in *pairing-based cryptography* [1]. This is due to the existence of (maximally possible) degree 6 twists for them, leading to faster pairing computation [1, §3.3]. One of the latest reviews of standards, commercial products and libraries for this type of cryptography is given in [2, §5]. Today, the most popular choice for the 128-bit security level is the so-called Barreto-Lynn-Scott $\mathbb{F}_p$-curve BLS12-381 [3], where $p \equiv 3 \pmod 4$, $p \equiv 10 \pmod{27}$, and $\lceil \log_2(p) \rceil = 381$.

The simultaneous compression of two points $(x_0, y_0), (x_1, y_1)$ from $E(\mathbb{F}_q)$ (so-called *double point compression*) is also an important task. It occurs, for example, in pairing-based protocols of succinct *non-interactive zero-knowledge proof (NIZK)*. One of the most notable recent works in this field is [4].

Double point compression has already been discussed in [5] not only for $j(E) = 0$, but in a slightly different way. In that article authors do not try to compress points as compact as possible. Instead, they find formulas transforming the coordinates x_0, y_0, x_1, y_1 to some three elements of the field $\mathbb{F}_q$. The advantage of their approach is the speed, because it should not solve any equations in the decompression stage.

By virtue of [6, Example V.4.4] the ordinariness of the curve E_b means that $p \equiv 1 \pmod 3$ or, equivalently, $\omega := \sqrt[3]{1} \in \mathbb{F}_p$, where $\omega \neq 1$. There is on E_b the order 6 automorphism $[-\omega]\colon (x, y) \mapsto (\omega x, -y)$. Consider the geometric quotient $GK_b' := E_b^2/[-\omega]^{\times 2}$, which is an example of so-called *generalized Kummer surface* [7, §1.3].

Our double compression is based on $\mathbb{F}_q$-*rationality* of GK_b', which is almost obvious (see §3). This concept of algebraic geometry means that for almost all (in some topological sense) points of GK_b' their compression (and subsequent decompression) can be accomplished by computing some rational functions defined over $\mathbb{F}_q$. To recover the original point belonging to $E_b^2(\mathbb{F}_q)$ from a given $\mathbb{F}_q$-point on GK_b' we find an inverse image of the natural map $E_b^2 \to GK_b'$ of degree 6. Since $\omega \in \mathbb{F}_q$, it is a *Kummer map*, that is the field $\mathbb{F}_q(E_b^2)$ is generated by a sixth root of some rational function from $\mathbb{F}_q(GK_b')$.

In the article [7] the author solves a similar task (almost in the same way), namely the compression task of points from $E_b(\mathbb{F}_{q^2})$, where $q \equiv 1 \pmod 3$, $q \equiv 3 \pmod 4$, and $b \in \mathbb{F}_{q^2}^*$. Its actuality for pairing-based cryptography is explained in the introduction of [7]. There we use so-called *Weil restriction* (*descent*) R_b of E_b with respect to the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$ (see [8, Chapter 7]). For this $\mathbb{F}_q$-surface we have $R_b(\mathbb{F}_q) = E_b(\mathbb{F}_{q^2})$. Besides, the map $[-\omega]$ is naturally induced to the order 6 automorphism $[-\omega]_2\colon R_b \xrightarrow{\sim} R_b$.

We next consider the generalized Kummer surface $GK_b := R_b/[\omega]_2$ under the order 3 automorphism $[\omega]_2 := ([-\omega]_2)^2$. In order to prove $\mathbb{F}_q$-rationality of GK_b we use quite complicated algebraic geometry (unlike GK_b'). In accordance with [9, §8] from $\mathbb{F}_q$-rationality of GK_b it follows $\mathbb{F}_q$-rationality of the generalized Kummer surface $R_b/[-\omega]_2 \simeq_{\mathbb{F}_q} GK_b/[-1]$. However, this fact does not provide explicit formulas of a birational $\mathbb{F}_q$-isomorphism $R_b/[-\omega]_2 \stackrel{\simeq}{\dashrightarrow} \mathbb{A}^2$. Nevertheless, such formulas can be easily derived in the same way as for GK_b' (for details see §4).

2 Double compression

For the sake of generality we will consider any pair of elliptic $\mathbb{F}_q$-curves of j-invariant 0, but for $q \equiv 1 \pmod 3$, i.e., $\omega \in \mathbb{F}_q$. Namely, for $i = 0, 1$ let $E_i\colon y_i^2 = x_i^3 + b_i$, that is E_{b_i} in our old notation. These curves are isomorphic at most over $\mathbb{F}_{q^6}$ by the map

$$\varphi\colon E_0 \xrightarrow{\sim} E_1, \qquad (x_0, y_0) \mapsto \big(\sqrt[3]{\beta}x_0, \sqrt{\beta}y_0\big),$$

where $\beta := b_1/b_0$. Also, for $k \in \mathbb{Z}/6$ let $\varphi_k := \varphi \circ [-\omega]^k = [-\omega]^k \circ \varphi$. Finally,

$$S_i := \big\{(x_i, y_i) \in E_i \mid x_i y_i = 0\big\} \cup \big\{(0:1:0)\big\} \quad \subset \quad E_i[2] \cup E_i[3],$$

$$S := E_0 \times S_1 \ \cup \ S_0 \times E_1.$$

Using the fractions

$$X := \frac{x_0}{x_1}, \qquad Y := \frac{y_0}{y_1},$$

we obtain the compression map

$$\mathrm{com}\colon (E_0 \times E_1)(\mathbb{F}_q) \setminus S \quad \hookrightarrow \quad \mathbb{F}_q^2 \times \mathbb{Z}/6 \times \mathbb{Z}/2,$$

$$\mathrm{com}(P_0, P_1) := \begin{cases} \big(X, Y, n, 0\big) & \text{if} \quad \forall k \in \mathbb{Z}/6\colon \varphi_k(P_0) \neq P_1, \\ \big(x_0, y_0, k, 1\big) & \text{if} \quad \exists k \in \mathbb{Z}/6\colon \varphi_k(P_0) = P_1, \end{cases}$$

where $n \in \mathbb{Z}/6$ is the position number of the element $z := x_1 y_1 \in \mathbb{F}_q^*$ in the set $\big\{(-1)^i \omega^j z\big\}_{i=0,j=0}^{1,2}$ ordered with respect to some order in $\mathbb{F}_q^*$. For example, in the case $q = p$ this can be the usual numerical one.

Note that the condition $\varphi_k(P_0) = P_1$ is possible only if the isomorphism φ is defined over $\mathbb{F}_q$, that is $\sqrt[6]{\beta} \in \mathbb{F}_q$. Finally, if it is necessary, points from $S(\mathbb{F}_q)$ can be separately worked out, using few additional bits. However they do not arise in practice, because, as is well known, from $E_i(\mathbb{F}_q)$ points of large prime order are only utilized for security reasons.

3 Double decompression

Let $u := x_1^3$, $v := y_1^2$, and $Z := u^2v^3 = z^6$. Since $x_0 = Xx_1$, we have $x_0^3 = X^3u$. Hence

$$Y^2 = \frac{y_0^2}{y_1^2} = \frac{x_0^3 + b_0}{x_1^3 + b_1} = \frac{X^3u + b_0}{u + b_1}$$

and

$$u = \frac{b_0 - b_1Y^2}{Y^2 - X^3}, \qquad v = u + b_1.$$

Using the number $n \in \mathbb{Z}/6$, we can extract the original sixth root

$$z = x_1y_1 = \sqrt[3]{u}\sqrt{v} = \sqrt[6]{Z} = \sqrt[3]{\sqrt{Z}}.$$

For $q \equiv 3 \pmod 4$, $q \not\equiv 1 \pmod{27}$ according to [1, §5.1.7], [10, §4]

$$a := \sqrt{Z} = \pm Z^{\frac{q+1}{4}}, \qquad \sqrt[3]{a} = \theta a^e, \qquad \text{hence} \qquad z = \pm\theta Z^{e\frac{q+1}{4}}$$

for some $\theta \in \mathbb{F}_q^*$, $\theta^9 = 1$ and $e \in \mathbb{Z}/(q-1)$. Besides, e has an explicit simple expression depending only on q. In the case $q \not\equiv 1 \pmod 9$, moreover, $\theta^3 = 1$. In the opposite case a suitable θ can be found with the help of at most two supplementary multiplications of $Z^{e\frac{q+1}{4}}$ by representatives of the quotient group μ_9/μ_3.

We eventually obtain the equalities

$$x_1 = f_n(X, Y) := \frac{uv}{z^2}, \qquad y_1 = g_n(X, Y) := \frac{z}{x_1}$$

making sense when the denominator of u is not zero, i.e., $Y^2 \neq X^3$. Otherwise

$$\frac{x_0^3 + b_0}{x_1^3 + b_1} = \frac{x_0^3}{x_1^3} \quad\Leftrightarrow\quad b_0x_1^3 = b_1x_0^3 \quad\Leftrightarrow\quad \exists j \in \mathbb{Z}/3\colon x_1 = \omega^j\sqrt[3]{\beta}x_0.$$

This means that $\varphi_k(P_0) = P_1$ for $k \in \{j, j+3\}$.

Thus the decompression map has the form

$$\mathrm{com}^{-1}\colon \mathrm{Im}(\mathrm{com}) \ \xrightarrow{\sim}\ (E_0 \times E_1)(\mathbb{F}_q) \setminus S,$$

$$\mathrm{com}^{-1}\big(t, s, m, bit\big) = \begin{cases} \big(tf_m, sg_m, f_m, g_m\big) & \text{if} \quad bit = 0, \\ \big((t, s), \varphi_m(t, s)\big) & \text{if} \quad bit = 1, \end{cases}$$

where $f_m := f_m(t, s)$, $g_m := g_m(t, s)$.

4 Compression-decompression over $\mathbb{F}_{q^2}$

Our approach still works well for compressing $\mathbb{F}_{q^2}$-points on the curve $E_b\colon y^2 = x^3 + b$, where $b \in \mathbb{F}_{q^2}^*$ and $q \equiv 1 \pmod 3$ as earlier. For simplicity we also suppose that $q \equiv 3 \pmod 4$, i.e., $i := \sqrt{-1} \notin \mathbb{F}_q$. Let $b = b_0 + b_1 i$ (such that $b_0, b_1 \in \mathbb{F}_q$) and

$$x = x_0 + x_1 i, \qquad y = y_0 + y_1 i, \qquad z := x_1 y_1, \qquad X := \frac{x_0}{x_1}, \qquad Y := \frac{y_0}{y_1}.$$

Due to [7, Remark 2] the elements $b_0, b_1 \neq 0$ in practice, hence let us assume this condition, to be definite. We will focus on general $\mathbb{F}_{q^2}$-points, that is on those outside the set

$$S := \big\{(x, y) \in E_b(\mathbb{F}_{q^2}) \mid x_0 y_0 x_1 y_1 = 0\big\} \cup \big\{(0 : 1 : 0)\big\}.$$

Consider the equations

$$R_b = \begin{cases} y_0^2 - y_1^2 = \rho_1(x_0, x_1) := x_0^3 - 3x_0 x_1^2 + b_0, \\ 2y_0 y_1 = \rho_i(x_0, x_1) := -x_1^3 + 3x_0^2 x_1 + b_1 \end{cases} \subset \quad \mathbb{A}^4_{(x_0, y_0, x_1, y_1)}$$

of the Weil restriction $R_b := \mathrm{R}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(E_b)$ (cf. [7, §1.2.1]). Similarly as in §3 we obtain the formulas (verified in [11])

$$u := x_1^3 = \frac{2b_0 Y - b_1 \gamma(Y)}{\alpha(X)\gamma(Y) - 2\beta(X)Y}, \qquad v := y_1^2 = \frac{\beta(X)u + b_0}{\gamma(Y)},$$

where

$$\alpha(X) := 3X^2 - 1, \qquad \beta(X) := X(X^2 - 3), \qquad \gamma(Y) := Y^2 - 1.$$

We eventually obtain the equalities

$$x_1 = f_n(X, Y) := \frac{uv}{z^2}, \qquad y_1 = g_n(X, Y) := \frac{z}{x_1},$$

where z is computed as a sixth root of $Z := u^2 v^3$ and the index $n \in \mathbb{Z}/6$ plays the same role as in §2, §3.

It remains to handle degenerate cases. It is readily checked (e.g., in [11]) that

$$\alpha(X)\gamma(Y) - 2\beta(X)Y = 0 \quad \Leftrightarrow \quad F := b_1 x_0^3 - 3b_0 x_0^2 x_1 - 3b_1 x_0 x_1^2 + b_0 x_1^3 = 0,$$

$$\gamma(Y) = 0 \quad \Leftrightarrow \quad y_1 = \pm y_0 \quad \Leftrightarrow \quad x_1 = h_\ell(x_0) := \sqrt{\frac{x_0^3 + b_0}{3x_0}},$$

where $\ell \in \mathbb{Z}/2$ is the position number of x_1 among $\pm x_1$ with respect to some order in $\mathbb{F}_q^*$. For example, in the case $q = p$ this can be the usual numerical one, that is $\ell = 1$ if and only if $x_1 > (p-1)/2$.

The polynomial F is the homogenization of one from [7, §1.3.1]. Therefore F is decomposed over $\mathbb{F}_q$ into linear L and irreducible quadratic Q homogeneous polynomials. Of course, Q is the product of two different $\mathbb{F}_q$-conjugate linear factors having the unique common point $(0,0)$. As a result, $F(x_0, x_1) = 0$ if and only if $L(x_0, x_1) = 0$ whenever $(x_0, x_1) \in \mathbb{F}_q^2$. Since $b_0, b_1 \neq 0$, we see that (up to a constant) $L = -cx_0 + x_1$ for some $c \in \mathbb{F}_q^*$. For instance, in the case $b_0 = b_1$ (including the $\mathbb{F}_{p^2}$-curve BLS12-381) we have $c = -1$ and $Q = b_0(x_0^2 - 4x_0x_1 + x_1^2)$ (cf. [7, §3.1]).

The compression map is given as follows:

$$\mathrm{com}\colon E_b(\mathbb{F}_{q^2}) \setminus S \quad \hookrightarrow \quad \mathbb{F}_q^2 \times \mathbb{Z}/6 \times \mathbb{Z}/3,$$

$$\mathrm{com}(x,y) := \begin{cases} \big(x_0, y_0, 0, 0\big) & \text{if} \quad x_1 = cx_0, \\ \big(x_0, y_0, 2k+\ell, 1\big) & \text{if} \quad y_1 = (-1)^k y_0, \\ \big(X, Y, n, 2\big) & \text{otherwise,} \end{cases}$$

where $k \in \mathbb{Z}/2$ and $2k + \ell \in \mathbb{Z}/4$. Be careful that here $\mathbb{Z}/j$ (for $j \in \{2,4,6\}$) denotes only the set (without the group structure) of the first j non-negative integers and $+$ is the addition in $\mathbb{Z}$.

The corresponding decompression map has the form

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

$$\mathrm{com}^{-1}\big(t, s, m, bits\big) = \begin{cases} \Big((t, s, ct, \dfrac{\rho_i(t, ct)}{2s}\Big) & \text{if} \quad bits = 0, \\ \big(t, s, h_\ell(t), (-1)^k s\big) & \text{if} \quad bits = 1, \\ \big(tf_m, sg_m, f_m, g_m\big) & \text{if} \quad bits = 2, \end{cases}$$

where $f_m := f_m(t,s)$, $g_m := g_m(t,s)$. In order not to complicate the exposition we leave to the reader to process the remaining simple cases when at least one of the coordinates x_0, y_0, x_1, y_1 is zero.

5 Complexity comparison

Tables 1, 2 display the worst-case complexity in terms of the number of the most cumbersome operations in the field $\mathbb{F}_q$. The inversion (resp. exponen-

	two $\mathbb{F}_q$-points	one $\mathbb{F}_{q^2}$-point
compression	there's nothing to do	
decompression	2 exp.	1 inv., 1 Legendre symbol, 2 exp. [1, Algorithm 5.18]

Table 1: Worst-case complexity of the classical method with x-coordinate(s)

	two $\mathbb{F}_q$-points	one $\mathbb{F}_{q^2}$-point
compression	2 inv.	2 inv.
decompression	3 inv., 1 exp.	4 inv., 1 exp.

Table 2: Worst-case complexity of the new method

tiation) operation is indicated as inv. (resp. exp.) for the sake of compactness.

Although the new point compression-decompression method contains a little more inversions than the classical one, this does not significantly affect the performance for q of a cryptographic size. The point is that compression is mainly applied to public data, which are not vulnerable to timing attacks [1, §8.2.2, §12.1.1]. Therefore all inversions (as well as the Legendre symbol) can be safely implemented via (an algorithm very close to) the extended Euclidean one (see, e.g., [1, §5.1.6, Algorithm 2.3]). And the latter is much faster than a general exponentiation in $\mathbb{F}_q^*$ even if an exponent is fixed and of small Hamming weight. A good survey of the exponentiation technique (not necessarily in $\mathbb{F}_q^*$) is represented in [8, Chapter 9].

6 Extension of the compression technique

At least theoretically, pairing-based cryptography also deals with the elliptic $\mathbb{F}_{q^2}$-curves $E_a\colon y^2 = x^3 + ax$ of j-invariant 1728, where $q \equiv 1 \pmod 4$. According to [1, Example 2.28] the latter condition is necessary for the ordinariness of E_a. Our technique remains valid for compressing $\mathbb{F}_q$-points of E_a^2 (if $a \in \mathbb{F}_q^*$) and $\mathbb{F}_{q^2}$-points of E_a, because there is on E_a the $\mathbb{F}_q$-automorphism $[i]\colon (x, y) \mapsto (-x, iy)$ of order 4. However in the second case one needs to remember that $\{1, i\}$ is obviously no longer a basis of the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$.

Further, given $m > 2$ it is very natural to think about compressing points from $E_b^m(\mathbb{F}_q)$ or $E_a^m(\mathbb{F}_q)$, where $b, a \in \mathbb{F}_q^*$. This so-called *multiple point compression* is discussed in [12] by analogy with double one in [5]. If m is large, then that approach is expected to be the best trade-off between compactness and efficiency of compression-decompression stages. In turn, one can try to generalize the idea of this article to other small values m.

As is known [13, §1], for $m > 6$ (resp. $m > 4$) the *generalized Kummer variety* $GK'_{b,m} := E_b^m/[-\omega]^{\times m}$ (resp. $GK'_{a,m} := E_a^m/[i]^{\times m}$) is no longer rational even over the algebraic closure $\overline{\mathbb{F}_q}$. Nevertheless, for $b = -1$ the $\mathbb{F}_q$-rationality of $GK'_{b,3}$ is proved in [14, §2] and for $a = -1$ the $\mathbb{F}_q$-rationality of $GK'_{a,3}$ is shown in [15], based on [16]. The geometrical rationality of $GK'_{b,4}$, $GK'_{b,5}$ is conjectured in [13, Questions 1.3, 1.4].

It turns out that the $\mathbb{F}_q$-formulas of a birational isomorphism $GK'_{b,3} \simeq\dashrightarrow \mathbb{A}^3$, derived in [14, §2] for $b = -1$, are immediately extended to $\mathbb{F}_q$-formulas for any $b \in \mathbb{F}_q^*$. In turn, the $\mathbb{F}_q$-formulas of [16], established for $a = -1$, are also valid for any $a \in \mathbb{F}_q^*$ and hence the proof of [15] is so. Although the latter does not provide explicit formulas for $GK'_{a,3} \simeq\dashrightarrow \mathbb{A}^3$, in our view, such $\mathbb{F}_q$-formulas can be obtained if desired.

In pairing-based cryptography the embedding degree k (see, e.g., [1, §1.2.3]) will probably exceed in the near future the value 12, which is popular today for the 128-bit security level. Therefore we will have to use elliptic curve twists (of degree $d \in \{6, 4\}$) defined over the field $\mathbb{F}_{q^m}$, where $m = k/d \in \mathbb{N}_{>2}$. Thus given $b, a \in \mathbb{F}_{q^m}^*$ the compression task of points from $E_b(\mathbb{F}_{q^m})$ or $E_a(\mathbb{F}_{q^m})$ is quite important.

More formally, introduce the order 6 automorphism $[-\omega]_m := \mathrm{R}_{\mathbb{F}_{q^m}/\mathbb{F}_q}([-\omega])$ on the Weil restriction $R_{b,m} := \mathrm{R}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(E_b)$. Similarly, $[i]_m := \mathrm{R}_{\mathbb{F}_{q^m}/\mathbb{F}_q}([i])$ is an order 4 automorphism on the Weil restriction $R_{a,m} := \mathrm{R}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(E_a)$. As is well known [8, §7.3], there are $\overline{\mathbb{F}_q}$-isomorphisms $\psi_{b,m}\colon R_{b,m} \simeq\to E_b^m$ and $\psi_{a,m}\colon R_{a,m} \simeq\to E_a^m$. Moreover, it is readily checked that

$$[-\omega]^m \circ \psi_{b,m} = \psi_{b,m} \circ [-\omega]_m, \qquad [i]^m \circ \psi_{a,m} = \psi_{a,m} \circ [i]_m.$$

Hence in view of the above, it is sufficient to focus on $m = 3$. In our opinion, the $\mathbb{F}_q$-rationality questions of $R_{b,3}/[-\omega]_3$ and $R_{a,3}/[i]_3$ seem difficult, but solvable.

7 Acknowledgements

The author expresses his deep gratitude to his scientific advisor M. Tsfasman.

8 Funding

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

References

[1] El Mrabet N., Joye M., *Guide to Pairing-Based Cryptography*, Cryptography and Network Security Series, Chapman and Hall/CRC, New York, 2016.

[2] Sakemi Y., Kobayashi T., Saito T., Wahby R., *Pairing-friendly curves*, 2021, IETF draft.

[3] Bowe S., *BLS12-381: New zk-SNARK elliptic curve construction*, Zcash Company blog: https://z.cash/blog/new-snark-curve/, 2017.

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

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

[6] Silverman J., *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, **106**, Springer, New York, 2009.

[7] 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.

[8] Cohen H. et al., *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and Its Applications, **34**, Chapman and Hall/CRC, New York, 2005.

[9] Liedtke C., "Algebraic surfaces in positive characteristic", *Birational Geometry, Rational Curves, and Arithmetic*, Simons Symposia, eds. Bogomolov F., Hassett B., Tschinkel Y., Springer, New York, 2013, 229–292.

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

[11] Koshelev D., *Magma code*, https://github.com/dishport/Faster-point-compression-for-elliptic-curves-of-j-invariant-0, 2021.

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

[13] 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.

[14] Oguiso K., Truong 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.

[15] Colliot-Thélene J.-L., "Rationalité d'un fibré en coniques", *Manuscripta Mathematica*, **147**:3 (2015), 305–310.

[16] Catanese F., Oguiso K., Truong T., "Unirationality of Ueno-Campana's threefold", *Manuscripta Mathematica*, **145**:3 (2014), 399–406.