Double point compression for elliptic curves of j-invariant 0

Abstract. The article provides a new double point compression method (to $2\log_2(q)+4$ bits) for an elliptic curve $E\colon y^2=x^3+b$ 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 $P_0, P_1 \in E(\mathbb{F}_q)$ to some two elements $t, s \in \mathbb{F}_q$ with four auxiliary bits. To recover (in the decompression stage) the points P_0, P_1 it is proposed to extract a sixth root $\sqrt[6]{w} \in \mathbb{F}_q$ of some element $w \in \mathbb{F}_q$. It is easily seen 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 $\mathbb{F}_q$.

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

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 $\mathbb{F}_q$.

The simultaneous compression of two points from $E(\mathbb{F}_q)$ (so-called *double point compression*) also has reason to live. It 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 of this 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 speed, because it should not solve any equations in the decompression stage.

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

There is an order 6 automorphism

$$\sigma\colon E \xrightarrow{\sim} E, \qquad (x,y) \mapsto (\zeta x, -y),$$

where $\zeta^2+\zeta+1=0$, i.e., $\zeta^3=1$, $\zeta \neq 1$. Note that $\zeta \in \mathbb{F}_q$, because $q \equiv 1 \pmod 3$. Consider the quotient $GK := E^2/\sigma\times\sigma$, which is an example of so-called *generalized Kummer surface* [1, §1.3].

Our double compression is based on $\mathbb{F}_q$-*rationality* of GK, which is almost obvious (see §2). This concept of algebraic geometry means that for almost all (in some topological sense) points of GK their compression (and subsequent decompression) can be accomplished by computing some rational functions defined over $\mathbb{F}_q$. Finally, to recover the original points $P_0, P_1 \in E(\mathbb{F}_q)$ from a given $\mathbb{F}_q$-point on GK we find an inverse image of the natural map $\varrho\colon E^2 \to GK$ of degree 6. Since $\zeta \in \mathbb{F}_q$, it is a *Kummer map*, that is the field $\mathbb{F}_q(E^2)$ is generated by a sixth root of some rational function from $\mathbb{F}_q(GK)$.

In the article [1] the author solves a similar task (almost in the same way), namely compression of $E(\mathbb{F}_{p^2})$, where $p \equiv 1 \pmod 3$, $p \equiv 3 \pmod 4$. There it is used so-called *Weil restriction* (*descent*) R of E with respect to the extension $\mathbb{F}_{p^2}/\mathbb{F}_p$ (see [1, §1.2.1]). For this $\mathbb{F}_p$-surface we have $R(\mathbb{F}_p) = E(\mathbb{F}_{p^2})$. The map $\sigma\colon E \xrightarrow{\sim} E$ is naturally induced to the order 6 map $\sigma_R\colon R \xrightarrow{\sim} R$. Next we consider the generalized Kummer surface R/σ_R^2 under the order 3 map σ_R^2. To prove $\mathbb{F}_p$-rationality of R/σ_R^2 we use quite complicated algebraic geometry (unlike GK). As a result, the quotient surface R/σ_R is also $\mathbb{F}_p$-rational. Actually, it is easy to derive simple compression (decompression) formulas for R/σ_R that are very similar to those for GK (for details see Remark 1).

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

Contents

1 Double compression

For sake of generality we will consider any pair of elliptic $\mathbb{F}_q$-curves of j-invariant 0, where $q \equiv 1 \pmod 3$, i.e., $\zeta \in \mathbb{F}_q$. Namely, for $i = 0, 1$ let $E_i\colon y_i^2 = x_i^3 + b_i$. 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 $\varphi_k := \varphi \circ \sigma^k = \sigma^k \circ \varphi$ and

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

Finally, using the fractions

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

we obtain the compression map

$$\mathrm{com}\colon (E_0 \times E_1)(\mathbb{F}_q) \setminus S_0 \times S_1 \quad \hookrightarrow \quad \mathbb{F}_q^2 \times \mathbb{Z}/6 \times \mathbb{Z}/2,$$

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

where $n \in \mathbb{Z}/6$ is the position number of $z := x_1 y_1 \in \mathbb{F}_q^*$ in the set $\big\{(-1)^i \zeta^j z\big\}_{i=0,j=0}^{1,2}$ 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 $(S_0 \times S_1)(\mathbb{F}_q)$ can be separately processed, using few additional bits.

2 Double decompression

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

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

and

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

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

$$z = x_1 y_1 = \sqrt[3]{u}\sqrt{v} = \sqrt[6]{w} = \sqrt[3]{\sqrt{w}}.$$

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

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

for some $\theta \in \mathbb{F}_q^*$, $\theta^9 = 1$ and $e \in \mathbb{Z}/(q-1)$. Moreover, e has an explicit simple expression depending only on q. We eventually obtain the equalities

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

If $Y^2 = X^3$, then

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

This means that $\varphi_k(P_0) = P_1$ for $k \in \{j, j+3\}$. Thus the decompression map has the form

$$\mathrm{com}^{-1} : \mathrm{Im}(\mathrm{com}) \quad \twoheadrightarrow \quad (E_0 \times E_1)(\mathbb{F}_q) \setminus S_0 \times S_1,$$

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

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

Remark 1. *Let $q \equiv 3 \pmod 4$, i.e., $i := \sqrt{-1} \notin \mathbb{F}_q$. Our approach also works well for compressing $\mathbb{F}_{q^2}$-points on the curve $E_b\colon y^2 = x^3 + b$, where $b \in \mathbb{F}_{q^2}^*$.*

More precisely, let $b = b_0 + b_1 i$ (such that $b_0, b_1 \in \mathbb{F}_q$) and

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

Building on the equations of the Weil restriction $R_b = \mathrm{R}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(E_b)$ (see [1, §1.2.1]), we obtain

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

where

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

As above, the degenerate cases (whenever the denominator of X, Y, u, or v equals 0) can be easily handled independently.

References

[1] Koshelev D. *A new elliptic curve point compression method based on $\mathbb{F}_p$-rationality of some generalized Kummer surfaces.* // Submitted to Finite Fields and Their Applications, 2019.

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

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

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

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

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