Double point compression for elliptic curves of $j$-invariant 0

Koshelev Dmitrii

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

Abstract. The article provides a new double point compression method (to $2 \log_2(q) + 4$ bits) for an elliptic $\mathbb{F}_q$-curve $E: y^2 = x^3 + b$ 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 [4] 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 $E: y^2 = x^3 + b$ for $b \in \mathbb{F}_q^*$, which is of $j$-invariant 0. Ordinary curves of such the form (in this case, $q \equiv 1 \pmod{3}$) have become very popular in elliptic cryptography, especially in pairing-based cryptography [3]. This is due to the existence of (maximally possible) degree 6 twists for them, leading to faster pairing computation [3, §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 $BLS12-381$ [1], where $p \equiv 3 \pmod{4}, p \equiv 10 \pmod{27}$.

---

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

1
There is an order 6 automorphism
\[ \sigma : E \ni (x, y) \mapsto (\zeta x, -y), \]
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 \([5, \S 1.3]\).

Our double compression is based on \( \mathbb{F}_q \)-rationality of \( GK \), which is almost obvious (see \( \S 2 \)). 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 \( \varrho : E^2 \to GK \) 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 \([5]\) 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 \([5, \S 1.2.1]\)). For this \( \mathbb{F}_p \)-surface we have \( R(\mathbb{F}_p) = E(\mathbb{F}_p^2) \). The map \( \sigma : E \ni (x, y) \mapsto (\zeta x, -y) \) is naturally induced to the order 6 map \( \sigma_R : R \ni (x, y) \mapsto (\zeta x, -y) \). Next we consider the generalized Kummer surface \( R/\sigma^2_R \) under the order 3 map \( \sigma^2_R \). To prove \( \mathbb{F}_p \)-rationality of \( R/\sigma^2_R \) we use quite complicated algebraic geometry (unlike \( GK \)). As a result, the quotient surface \( R/\sigma^2_R \) is also \( \mathbb{F}_p \)-rational and we expect that (in comparison with \( R/\sigma^2_R \)) there are much simpler compression (decompression) formulas for \( \mathbb{F}_p \)-points of \( R/\sigma^2_R \).

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

Contents

1 Double compression

2 Double decompression

References

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 \( E_i : y^2_i = x^3_i + b_i \). These curves are isomorphic at most over \( \mathbb{F}_q^6 \) by the map
\[ \varphi : E_0 \ni (x_0, y_0) \mapsto (\sqrt{\beta}x_0, \sqrt{\beta}y_0), \]
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
\[ S_i := \{(x_i, y_i) \in E_i \mid x_i y_i = 0\} \cup \{(0 : 1 : 0)\} \subset E_i[2] \cup E_i[3]. \]
Finally, using the fractions
\[ X := \frac{x_0}{x_1}, \quad Y := \frac{y_0}{y_1}, \]
we obtain the compression map
\[
\text{com}: (E_0 \times E_1)(\mathbb{F}_q) \setminus S_0 \times S_1 \to \mathbb{F}_q^2 \times \mathbb{Z}/6 \times \mathbb{Z}/2,
\]
\[
\text{com}(P_0, P_1) := \begin{cases} 
(X, Y, n, 0) & \text{if } \forall k \in \mathbb{Z}/6 : \varphi_k(P_0) \neq P_1, \\
(x_0, y_0, k, 1) & \text{if } \exists k \in \mathbb{Z}/6 : \varphi_k(P_0) = P_1,
\end{cases}
\]
where \( n \in \mathbb{Z}/6 \) is the position number of \( z := x_1y_1 \in \mathbb{F}_q^* \) in the set \( \{-1\}^{1,2} \mathbb{J}z^{1,2} \) 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 \( \varphi \) 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 \( u := x_1^3, \quad v := y_1^2, \quad \text{and } w := u^2v^3 = z^6 \). 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
\[
u = \frac{b_0 - b_1Y^2}{Y^2 - X^3}, \quad v = u + b_1.
\]
We eventually obtain the equalities
\[
x_1 = f_n(X, Y) := \frac{uv}{z^2}, \quad y_1 = g_n(X, Y) := \frac{z}{x_1).
\]
Using the number \( n \), we can extract the original sixth root
\[
z = x_1y_1 = \sqrt[6]{u}\sqrt{v} = \sqrt[6]{w} = \sqrt[3]{\sqrt[3]{w}}.
\]
For \( q \equiv 3 \mod 4, q \not\equiv 1 \mod 27 \) according to [3 §5.1.7, [2 §4]
\[
a := \sqrt{w} = \pm \omega^\frac{q+1}{4}, \quad \sqrt[3]{a} = \theta a^m, \quad \text{hence } \quad z = \pm \theta w^\frac{m+1}{3}
\]
for some \( \theta \in \mathbb{F}_q^*, \theta^9 = 1 \) and \( m \in \mathbb{Z}/(q - 1) \). Moreover, \( m \) has an explicit simple expression depending only on \( q \).

If \( Y^2 = X^3 \), then
\[
\frac{x_0^3 + b_0}{x_1^3 + b_1} = \frac{x_0^3}{x_1^3} \iff b_0x_1^3 = b_1x_0^3 \iff \exists j \in \mathbb{Z}/3 : x_1 = \zeta^j \sqrt[3]{\beta}x_0.
\]
This means that \( \varphi_k(P_0) = P_1 \) for \( k \in \{j, j+3\} \). Thus the decompression map has the form

\[
\text{com}^{-1}: \text{Im}(\text{com}) \ni (E_0 \times E_1)(\mathbb{F}_q) \setminus S_0 \times S_1,
\]

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

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

References


