Double point compression for elliptic curves of j-invariant 0

Dimitri Koshelev

Laboratory of Mathematics, Versailles Saint-Quentin-en-Yvelines University (France)
Center for Research and Advanced Development, Infotecs

CTCrypt IX, 17.09.2020

Point compression

Many protocols of elliptic cryptography use a *compression method* (to $\approx \log_2(q)$ bits) for $\mathbb{F}_q$-points of an elliptic curve $E : y^2 = f(x)$ over a finite field $\mathbb{F}_q$ of characteristic $p > 3$.

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 $\mathbb{F}_q$ (an exponentiation in $\mathbb{F}_q$ for $q \equiv 3 \pmod 4$).

The simultaneous compression (to $\approx 2\log_2(q)$ bits) of two points from $E(\mathbb{F}_q)$ 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)*.

Pairing-based cryptography

Consider an elliptic $\mathbb{F}_q$-curve $E_b\colon y^2 = x^3 + b$, whose j-invariant is 0. Ordinary (i.e., non-supersingular) curves of such the form have become very popular in *pairing-based cryptography*. This is due to the existence of (maximally possible) degree 6 twists for them, leading to faster pairing computation.

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 $\omega \neq 1$. Therefore the order 6 automorphism $[-\omega]\colon (x, y) \mapsto (\omega x, -y)$ on E_b is defined over $\mathbb{F}_q$.

Double point compression

Let

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

Also, take two $\mathbb{F}_q$-points of E_b, namely $P_i := (x_i, y_i)$ for $i = 0, 1$. Using the fractions

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

we obtain the compression map

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

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

where $n \in \mathbb{Z}/6$ is the position number of $z := x_1 y_1 \in \mathbb{F}_q^*$ in the set $\{(-1)^i \omega^j z\}_{i=0,j=0}^{1,2}$ ordered with respect to some order in $\mathbb{F}_q^*$.

Double point decompression

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

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

and

$$u = b\frac{1 - Y^2}{Y^2 - X^3}, \qquad v = u + b.$$

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

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

For $q \equiv 3 \pmod 4$, $q \not\equiv 1 \pmod 9$ we have

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

for some $e \in \mathbb{Z}/(q-1)$. Moreover, e has an explicit simple expression depending only on q.

Double point decompression

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

$$\frac{x_0^3 + b}{x_1^3 + b} = \frac{x_0^3}{x_1^3} \quad \Leftrightarrow \quad x_1^3 = x_0^3 \quad \Leftrightarrow \quad \exists j \in \mathbb{Z}/3 \colon x_1 = \omega^j x_0.$$

Thus the decompression map has the form

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

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

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

Complexity and security of the new method

Although the new point compression-decompression method contains a lot of inversion operations in the field $\mathbb{F}_q$, this is often harmless in regard to *timing attacks*. The point is that this type of conversion is mainly applied to public data.

There are two common approaches for computing an inverse element in $\mathbb{F}_q$. The first uses the identity $\gamma^{-1} = \gamma^{q-2}$ (for $\gamma \in \mathbb{F}_q^*$), but requires the very inefficient exponentiation operation in $\mathbb{F}_q$. The second is based on the extended Euclidean algorithm. It is much more efficient, despite the difficulty to implement it in *constant time*.

Thus the new method can be implemented by means of just 1 exponentiation in the field $\mathbb{F}_q$. Therefore it is much faster than the classical one with the coordinates x_0, x_1, whose decompression stage requires 2 exponentiations in $\mathbb{F}_q$.

Idea behind the formulas

Consider the geometric quotient $GK_b := E_b^2/[-\omega]^{\times 2}$, which is an example of so-called *generalized Kummer surface*.

Our double compression is based on $\mathbb{F}_q$-*rationality* of GK_b, which is almost obvious. This concept of algebraic geometry means that for almost all points of GK_b their compression (and subsequent decompression) can be accomplished by computing a certain rational $\mathbb{F}_q$-map $\varphi^{-1}\colon GK_b \dashrightarrow \mathbb{A}^2$ (respectively $\varphi\colon \mathbb{A}^2 \dashrightarrow GK_b$).

In order 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 $\mathbb{F}_q(GK_b)$.

$\mathbb{F}_{q^2}$-point compression

Our approach still works well for compressing $\mathbb{F}_{q^2}$-points on the curve $E_b\colon y^2 = x^3 + b$, where $b \in \mathbb{F}_{q^2}^*$. For simplicity we take $q \equiv 3 \pmod 4$, 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

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

It can be checked that

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

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.

Idea behind the formulas

Consider the so-called *Weil restriction* (*descent*)

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

of the curve E_b with respect to the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$. 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

$$[-\omega]_2 \colon R_b \xrightarrow{\sim} R_b, \qquad (x_0, x_1, y_0, y_1) \mapsto (\omega x_0, \omega x_1, -y_0, -y_1).$$

As above, the new $\mathbb{F}_{q^2}$-point compression method is based on $\mathbb{F}_q$-rationality of the generalized Kummer surface $R_b/[-\omega]_2$.

Actuality of the $\mathbb{F}_{q^2}$-point compression task

As usual in cryptography, an elliptic curve $E/\mathbb{F}_q$ is assumed to have a subgroup $G \subset E(\mathbb{F}_q)$ of large prime order $\ell \neq p$. The *embedding degree* of E (with respect to ℓ) is the extension degree $k := [\mathbb{F}_q(\mu_\ell) : \mathbb{F}_q]$. Further, let E' be a *twist* for E of degree $d \mid k$ (i.e., $E \simeq_{\mathbb{F}_{q^d}} E'$ and $E \not\simeq_{\mathbb{F}_{q^e}} E'$ for all $e \mid d$) and $G' \subset E'(\mathbb{F}_{q^{\frac{k}{d}}})$ be the subgroup of order ℓ.

In practice, pairings are mainly taken in the form

$$G \times G' \to \mu_\ell \subset \mathbb{F}_{q^k}^*,$$

where k is the minimally possible number such that the discrete logarithm problem in $\mathbb{F}_{q^k}^*$ is hard, but d is, conversely, the maximally possible one. It is a classical fact that $d \leqslant 6$ and this bound is only attained by the elliptic curves E_b. At the moment, $k = 12$ is the optimal choice for the 128-bit security level. Thus $G' \subset E_{b'}(\mathbb{F}_{q^2})$ for some $b' \in \mathbb{F}_{q^2}^*$.

3-dimensional case

The geometrical rationality (i.e., rationality over the algebraic closure $\overline{\mathbb{F}_q}$) is also known for the generalized Kummer threefold $E_b^3/[-\omega]^3$.

Therefore it seems that our compression technique can be extended to points of

$$E_b^3(\mathbb{F}_q), \qquad E_b(\mathbb{F}_q) \times E_b(\mathbb{F}_{q^2}), \qquad E_b(\mathbb{F}_{q^3})$$

In other words, instead of 2 exponentiations in $\mathbb{F}_q$ (respectively 1 exponentiation in $\mathbb{F}_{q^3}$ for the third case) it is sufficient to perform only 1 exponentiation in $\mathbb{F}_q$.

The first two cases are actual, e.g., for pairing-based protocols of succinct NIZK. The third will become so later. Indeed, in pairing-based cryptography the optimal embedding degree k will exceed 12 in the near future. Therefore we will have to use $k = 18$ and twists of degree 6 defined over $\mathbb{F}_{q^3}$.

Case of j-invariant 1728

Consider an elliptic $\mathbb{F}_{q^2}$-curve $E_a : y^2 = x^3 + ax$ of j-invariant 1728, where $p \equiv 1 \pmod 4$, that is $i := \sqrt{-1} \in \mathbb{F}_p$. The latter condition is necessary and sufficient for the ordinariness of E_a.

Our technique also remains to be 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 $[i] : (x, y) \mapsto (-x, iy)$ of order 4. However in the second case one needs to take another basis of the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$.

Main references

1. El Mrabet N., Joye M. *Guide to pairing-based cryptography.* — New York.: Chapman & Hall, 2016.

2. Groth J. *On the size of pairing-based non-interactive arguments.* // Eurocrypt, 2016. P. 305–326.

3. Sakemi Y., Kobayashi T., Saito T., Wahby R. *Pairing-friendly curves.* // IETF Secretariat, 2020.

Thank you for your attention!