Fast subgroup membership testings and hashing to $\mathbb{G}_2$ on pairing-friendly curves

Yu Dai

Sun Yat-Sen university

July 12, 2023

Outline

Pairings on elliptic curves

Hashing to $\mathbb{G}_2$ on curves with the lack of twists

Fast Subgroup Membership Testings on Pairing-friendly Curves

Pairings on elliptic curves

Pairings on elliptic curves

A cryptographic pairing is a map

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T.$$

Pairing subgroups:

- $\mathbb{G}_1 = E(\mathbb{F}_p)[r]$;
- $\mathbb{G}_2 = E(\mathbb{F}_{p^k})[r] \cap \mathrm{Ker}(\pi - [p])$;
- $\mathbb{G}_T = \{\alpha \in \mathbb{F}_{p^k} | \alpha^r = 1\}$.

The embedding degree k is the smallest integer such that $r | p^k - 1$.

Pairings on elliptic curves

Two types of pairing-friendly curves:

- **curves admitting a twist**: the subgroup $\mathbb{G}_2$ can be represented as $E'(\mathbb{F}_{p^e})[r]$, where E' is a twist of E:

$$\phi : E' \to E : (x, y) \to (u^2x, u^3y), u \in \mathbb{F}_{p^k}.$$

- **curves with the lack of twists**: the subgroup $\mathbb{G}_2$ can be only represented as $E[r] \cap \mathrm{Ker}(\pi - [p])$.

If $p \geq 5$, E is a curve with the lack of twists $\Leftrightarrow$ $\gcd(k, 6) = 1$.

Hashing to $\mathbb{G}_2$ on curves with the lack of twists

Hashing to $\mathbb{G}_2$ on curves with the lack of twists

$$\begin{tikzcd} \{0,1\}^m \arrow[rr, bend left, "\text{standard hashing function}"] \arrow[rrrrrr, bend right, "\text{hashing to } \mathbb{G}_2"'] && \mathbb{F}_p \arrow[rr, bend left, "\text{hashing to curves}"] && E(\mathbb{F}_{p^k}) \arrow[rr, bend left, "?"] && \mathbb{G}_2 \end{tikzcd}$$

Question: How to efficiently map a point of $E(\mathbb{F}_{p^k})$ into $\mathbb{G}_2$?

Hashing to $\mathbb{G}_2$ on curves with the lack of twists

Cyclotomic zero subgroup of elliptic curves:

$$G_0 = \{Q \in E(\mathbb{F}_{p^k}) \mid \Phi_k(\pi)(Q) = \mathcal{O}_E\}.$$

Some important properties of G_0:

- $G_0 \subseteq E(\mathbb{F}_{p^k})$;
- $$\begin{aligned}\#G_0 = \#\mathrm{Ker}(\Phi_k(\pi)) &= \prod_{d|k} \#\mathrm{Ker}(\pi^d - 1)^{\mu(k/d)} \\ &= \prod_{d|k} \#E(\mathbb{F}_{p^d})^{\mu(k/d)},\end{aligned}$$
  where $\mu(\cdot)$ is the Moebius function.
- if $r \nmid \Phi_k(1)$, then $E[r] \cap G_0 = \mathbb{G}_2$.

Hashing to $\mathbb{G}_2$ on curves with the lack of twists

Define

- $G_0 \cong \mathbb{Z}_m \oplus \mathbb{Z}_{mnr}$ for some integers m and n.
- $H = mG_0$. Then the subgroup H is cyclic as $H \cong \mathbb{Z}_{nr}$.

The sequence of mapping a random point of $E(\mathbb{F}_{p^k})$ to $\mathbb{G}_2$:

$$E(\mathbb{F}_{p^k}) \xrightarrow{\rho} G_0 \xrightarrow{m} H \xrightarrow{n} \mathbb{G}_2,$$

where $\rho = (\pi^k - 1)/\Phi_k(\pi))$.

Hashing to $\mathbb{G}_2$ on curves with the lack of twists

The characteristic polynomial of π is

$$\pi^2 - t\pi + p,$$

where t is the tace of E over $\mathbb{F}_p$.

The action of π on H:

- For any point $P \in H$, $\pi(P) = [a]P$ for some $a \in \mathbb{Z}$.
- Computing the scalar a:
    1. $$\Phi_k(\pi)(P) = \mathcal{O}_E \Rightarrow \Phi_k(a) = 0 \bmod nr.$$
       $$\pi^2(P) - [t]\pi(P) + [p]P = \mathcal{O}_E \Rightarrow a^2 - t \cdot a + p = 0 \bmod nr.$$
    2. Let $a_0, a_1 \in \mathbb{Z}$ such that
       $$a_0 + a_1 \cdot x = \Phi_k(x) \bmod (x^2 - tx + p).$$

  Putting 1. and 2. together, $a_0 + a_1 \cdot a \equiv 0 \bmod nr$.

Hashing to $\mathbb{G}_2$ on curves with the lack of twists

GLV endomorphism τ on ordinary curves:

- if $j(E) = 0$, $\tau : (x, y) \to (\omega \cdot x, y)$, where ω is a primitive cube root of unity in $\mathbb{F}_p^*$. The characteristic equation of τ is $\tau^2 + \tau + 1 = 0$;
- if $j(E) = 1728$, $\tau : (x, y) \to (-x, i \cdot y)$, where i is a primitive fourth root of unity in $\mathbb{F}_p^*$. The characteristic equation of $\tau^2 + 1 = 0$.

Hashing to $\mathbb{G}_2$ on curves with the lack of twists

The action of τ on H:

- For any point $P \in H$, $\tau(P) = [b]P$ for some $b \in \mathbb{Z}$.
- Computing the scalar b(in the case of $j(E) = 0$):
    1. Computing $\sqrt{-3}$ in $\mathbb{Z}_{nr}$.

$$
\begin{aligned}
& a^2 - a \cdot t + p \equiv 0 \bmod nr. \\
\Rightarrow & a \equiv \frac{1}{2}(t \pm \sqrt{t^2 - 4p}) \equiv \frac{1}{2}(t \pm f\sqrt{-3}) \bmod nr, \\
\Rightarrow & \sqrt{-3} \equiv \pm(2a - t)/f \bmod nr.
\end{aligned}
$$

    2. Computing b using the characteristic equation of τ

$$
\begin{aligned}
& b^2 + b + 1 \equiv 0 \bmod nr \\
\Rightarrow & b = \frac{-1 \pm \sqrt{-3}}{2} = \frac{-f \pm (2a - t)}{2f} \bmod nr.
\end{aligned}
$$

Hashing to $\mathbb{G}_2$ on curves with the lack of twists

The action of $\Psi = \pi \circ \tau$ on H:
Let $\Psi = \pi \circ \tau$ and $\lambda = a \cdot b$. Then $\Psi(P) = [\lambda]P$. On curves with the lack of twists,

- if $j(E) = 0$, we have $\gcd(k, 3) = 1$ and thus $\Phi_{3k}(\lambda) \equiv 0 \bmod nr$, where $\deg(\Phi_{3k}) = 2\varphi(k)$;
- if $j(E) = 1728$, we have $\gcd(k, 4) = 1$ and thus $\Phi_{4k}(\lambda) \equiv 0 \bmod nr$, where $\deg(\Phi_{4k}) = 2\varphi(k)$;

Hashing to $\mathbb{G}_2$ on curves with the lack of twists

How to efficiently map a random point $P \in H$ to $\mathbb{G}_2$?

- Applying the LLL algorithm in the following $2\varphi(k)$-dimensional lattice, we obtain a short coefficient vector $h = (h_0, \cdots, h_{2\varphi(k)-1})$ such that

$$n \mid (h_0 + h_1 \cdot \lambda + \cdots + h_{2\varphi(k)-1} \cdot \lambda^{2\varphi(k)-1}),$$

where $\|h\| \approx \log n/(2\varphi(k))$.

$$\begin{pmatrix} n & 0 & 0 & \cdots & 0 \\ -\lambda & 1 & 0 & \cdots & 0 \\ -\lambda^2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \\ -\lambda^{2\varphi(k)-1} & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

- $[h_0]P + [h_1]\Psi(P) + \cdots + [h_{2\varphi(k)-1}]\Psi^{2\varphi(k)-1}(P) \in \mathbb{G}_2$.

Conclusion:

- We propose a fast method for mapping a random point of $E(\mathbb{F}_{p^k})$ to $\mathbb{G}_2$ on curves with the lack of twists.

- In the case of $j(E) \in \{0, 1728\}$, Frobenius endomporshim and GLV endomporshim can be combined to build a $2\varphi(k)$dimensional decomposition.

- The method is suitable for some interesting curves, such as BW13-P310 and BW19-P286.

Fast Subgroup Membership Testings on Pairing-friendly Curves

$\mathbb{G}_2$ membership testing on curves admitting a twist

Notations:

- $\psi = \phi^{-1} \circ \pi \circ \phi$.
- $\mathcal{L}_\psi = \{(\alpha_0, \alpha_1, \cdots, \alpha_{\varphi(k)-1}) \in \mathbb{Z}^{\varphi(k)} \mid \sum_{i=0}^{\varphi(k)-1} \alpha_i \cdot p^i \equiv 0 \bmod r\}$.

Question:

Given a point $Q \in E'(\mathbb{F}_{p^e})$, how to efficiently check

$Q \overset{?}{\in} \mathbb{G}_2 = E'(\mathbb{F}_{p^e})[r]$?

$\mathbb{G}_2$ membership testing on curves admitting a twist

Basic idea:

Let $(c_0, c_1, \cdots, c_{\varphi(k)-1}) \in \mathcal{L}_\psi$.

$$Q \in \mathbb{G}_2 \Rightarrow \sum_{i=0}^{\varphi(k)-1} [c_i]\psi^i(Q) = \sum_{i=0}^{\varphi(k)-1} [c_i \cdot p^i]R = \mathcal{O}_{E'}.$$

$$\sum_{i=0}^{\varphi(k)-1} [c_i]\psi^i(Q) = \mathcal{O}_{E'} \Rightarrow Q \overset{?}{\in} \mathbb{G}_2.$$

Or can we obtain some information about the order of Q?

$\mathbb{G}_2$ membership testing on curves admitting a twist

The characteristic polynomial of ψ is

$$\psi^2 - t\psi + p,$$

where t is the trace of E over $\mathbb{F}_p$.

Let b_0 and b_1 given as follows:

$$b_0 + b_1\psi = \sum\nolimits_{i=0}^{\varphi(k)-1} c_i \psi^i \bmod (\psi^2 - t\psi + p).$$

$$\begin{aligned}\sum_{i=0}^{\varphi(k)-1} [c_i]\psi^i(Q) = \mathcal{O}_{E'} &\Rightarrow (b_0 + b_1\psi)(Q) = \mathcal{O}_{E'}\\ &\Rightarrow (b_0 + b_1\hat{\psi})(b_0 + b_1\psi)(Q) = \mathcal{O}_{E'}\\ &\Rightarrow [b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p]Q = \mathcal{O}_{E'}.\end{aligned}$$

$\mathbb{G}_2$ membership testing on curves admitting a twist

What's the meaning of the value $b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p$?

$$\begin{aligned} & b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p \\ = & b_1^2((-b_0/b_1)^2 - t(-b_0/b_1) + p) \\ = & \text{Res}(b_0 + b_1\psi, \psi^2 - t\psi + p) \\ = & \text{Res}(\sum_{i=0}^{\varphi(k)-1} c_i\psi^i, \psi^2 - t\psi + p), \end{aligned}$$

where $\text{Res}(f, g)$ represents the **resultant** of two polynomials f and g.

$\mathbb{G}_2$ membership testing on curves admitting a twist

Notations:

- $g(\psi)$: the characteristic polynomial of ψ.
- $f(\psi) = \sum_{i=0}^{\varphi(k)-1} c_i \psi^i$, $(c_0, c_1, \cdots, c_{\varphi(k)-1}) \in \mathcal{L}_\psi$.
- $h_2 = \#E'(\mathbb{F}_{p^e})/r$, $h_2' = Res(f(\psi), g(\psi))/r$.

Putting it all together:

- $Q \in E'(\mathbb{F}_{p^e}) \Rightarrow [h_2 \cdot r]Q = \mathcal{O}_{E'}$.
- $\sum_{i=0}^{\varphi(k)-1} [c_i]\psi^i(Q) = \mathcal{O}_{E'} \Rightarrow [h_2' \cdot r]Q = \mathcal{O}_{E'}$.

Conclusion:

Restrict the selected short vector satisfy $\gcd(h_2, h_2') = 1$. Then,

$$Q \in \mathbb{G}_2 \Leftrightarrow \sum_{i=0}^{\varphi(k)-1} [c_i]\psi^i(Q) = \mathcal{O}_{E'}.$$

$\mathbb{G}_2$ membership testing on curves admitting a twist

How to find a valid vector $(c_0, c_1, \cdots, c_{\varphi(k)-1})$?

- We can enumerate vectors in $\mathcal{L}_\psi$ until the condition $\gcd(h_2, h_2') = 1$ holds. There always exists one vector meeting the condition as we can select it as $(r, 0, \cdots, 0)$, which corresponds to the naive method.

- For efficiency, we expect the target vector is as short as possible.

Magma code for finding valid short vectors on different pairing-friendly curves:
https://github.com/eccdaiy39/smt-magma/tree/main/vector

$\mathbb{G}_2$ membership testing on curves with the lack of twists

On curves with the lack of twists,

$$\mathbb{G}_2 = E(\mathbb{F}_{p^k})[r] \cap \mathsf{Ker}(\pi - [p]) = E[r] \cap G_0.$$

The group $\mathbb{G}_2$ is the unique subgroup of G_0 with order r.

$\mathbb{G}_2$ membership testing on curves with the lack of twists

Notations:

- $g(\pi)$: the characteristic polynomial of π.
- $f(\pi) = \sum_{i=0}^{\varphi(k)-1} c_i \pi^i$, $(c_0, c_1, \cdots, c_{\varphi(k)-1}) \in \mathcal{L}_\psi$.
- $h_2 = \#G_0/r$, $h_2' = Res(g(\pi), f(\pi))/r$,

Conclusion:

Restrict the selected short vector satisfies $\gcd(h_2, h_2') = 1$. Then,

$$Q \in \mathbb{G}_2 \Leftrightarrow Q \in G_0 \text{ and } \sum_{i=0}^{\varphi(k)-1} [c_i]\pi^i(Q) = \mathcal{O}_E.$$

$\mathbb{G}_2$ membership testing on curves with the lack of twists

An optimized method on curves with $j(E) \in \{0, 1728\}$:

The characteristic equation of $\Psi = \pi \circ \tau$ is

(1) $j(E) = 0: \quad \Psi^2 + \frac{t \pm 3f}{2}\Psi + p = 0$ with $t^2 - 4p = -3f^2$;

(2) $j(E) = 1728: \quad \Psi^2 \pm f\Psi + p = 0$ with $t^2 - 4p = -f^2$.

$\mathbb{G}_2$ membership testing on curves with the lack of twists

Notations:

- ℓ: $\Psi(Q) = [\ell]Q$ for $Q \in \mathbb{G}_2$.
- $\mathcal{L}_\Psi = \{(\alpha_0, \alpha_1, \cdots, \alpha_{2\varphi(k)-1}) \in \mathbb{Z}^{2\varphi(k)} \mid \sum_{i=0}^{2\varphi(k)-1} \alpha_i \cdot \ell^i \equiv 0 \bmod r\}$.
- $g(\Psi)$: the characteristic polynomial of Ψ.
- $f(\Psi) = \sum_{i=0}^{2\varphi(k)-1} c_i \Psi^i$, $(c_0, c_1, \cdots, c_{2\varphi(k)-1}) \in \mathcal{L}_\Psi$.
- $h_2' = Res(f(\Psi), g(\Psi))/r$.

Conclusion:

Restrict the selected short vector satisfies $\gcd(h_2, h_2') = 1$. Then,

$$Q \in \mathbb{G}_2 \Leftrightarrow Q \in G_0 \text{ and } \sum_{i=0}^{2\varphi(k)-1} [c_i]\Psi^i(Q) = \mathcal{O}_E.$$

$\mathbb{G}_2$ membership testing

Table 1: The short vectors of $\mathbb{G}_2$ membership testing on a list of pairing-friendly curves at the 128-bit security level. On KSS16-P330, $u = (-z - 25)/70$.

Curve	Short vector
BW6-P761	$(\frac{z-1}{3}(z^2-2)+z, \frac{z-1}{3}(z^2-2)-1)$
CP6-P782	$(\frac{2z-2}{3}(z^2-2)+z-1, \frac{1-z}{3}(z^2-2)+1)$
BN-P446	$(z+1, z, z, -2z)$
BLS12-P461	$(z, -1, 0, 0)$
KSS16-P330	$(11u+4, -9u-3, 3u+1, 3u+1,$ $-13u-5, 7u+3, u, 11u+4)$
KSS18-P348	$(\frac{2z}{7}, 1, 0, \frac{z}{7}, 0, 0)$
BW13-P310	$(-z, 1, 0, \cdots, 0)$
BW19-P286	$(-z, 1, 0, \cdots, 0)$

$\mathbb{G}_1$ membership testing

On ordinary curves with j-invariant 0 or 1728, the GLV endomorphism τ can be used be seep up $\mathbb{G}_1$ membership testing.

Notations:

- $\lambda : \tau(P) = [\lambda]P$ for $P \in \mathbb{G}_1$.
- $\mathcal{L}_\tau = \{(\alpha_0, \alpha_1 \in \mathbb{Z}^2 \mid a_0 + a_1 \cdot \lambda \equiv 0 \bmod r\}$.
- $g(\tau)$: the characteristic polynomial of τ.
- $f(\tau) = a_0 + a_1\tau$, $(a_0, a_1) \in \mathcal{L}$.
- $h_1 = \#E(\mathbb{F}_p)/r$.
- $h_1' = Res(g(\tau), f(\tau))/r$.

Conclusion:

Restrict the selected short vector (a_0, a_1)satisfies $\gcd(h_1, h_1') = 1$. Then,

$$P \in \mathbb{G}_1 \Leftrightarrow [a_0]P + [a_1]\tau(P) = \mathcal{O}_E.$$

$\mathbb{G}_1$ membership testing

Table 2: The short vectors for $\mathbb{G}_1$ membership testing on a list of pairing-friendly curves with j-invariant 0 or 1728.

Curve	(a_0, a_1)
BW6-P761	$(\frac{z-1}{3}(z^2-2)-1, \frac{1-z}{3}(z^2-2)-z)$
BLS12-P461	$(z^2, 1)$
KSS16-P330	$(\frac{31z^4+625}{8750}, \frac{-17z^4-625}{8750})$
KSS18-P348	$((\frac{z}{7})^3, -18a_0-1)$
BW13-P310	$(-(z^7+z)(z^4+z^3-z-1), a_0 \cdot z-1)$
BW19-P286	$((z-z^{10})(z^6-z^3+1)(z+1), a_0 \cdot z-1)$

$\mathbb{G}_T$ membership testing

Let $(c_0, c_1, \cdots, c_{\varphi(k)-1}) \in \mathcal{L}_\psi$ and $\eta = \sum_{i=0}^{\varphi(k)-1} c_i \cdot p^i$ such that $\gcd(\Phi_k(p), \eta) = r$. Then,

$$\alpha \in \mathbb{G}_T \Leftrightarrow \alpha^{\Phi_k(p)} = 1 \text{ and } \prod_{i=0}^{\varphi(k)-1} \alpha^{c_i \cdot p^i} = 1.$$

$\mathbb{G}_T$ membership testing

Table 3: The short vectors of $\mathbb{G}_T$ membership testing for a list of pairing-friendly curves at the 128-bit security level. On KSS16-P330, the value u is equal to $(-z-25)/70$.

Curve	Short vector
BW6-P761	$(\frac{z-1}{3}(z^2-2)+z, \frac{z-1}{3}(z^2-2)-1)$
CP6-P782	$(\frac{z-1}{3}(z^2-2)-1, \frac{z-1}{3}(z^2-2)+z)$
BN-P446	$(z+1, z, z, -2z)$
BLS12-P461	$(z, -1, 0, 0)$
KSS16-P330	$(11u+4, -9u-3, 3u+1, 3u+1,$ $-13u-5, 7u+3, u, 11u+4)$
KSS18-P348	$(\frac{2z}{7}, 1, 0, \frac{z}{7}, 0, 0)$
BW13-P310	$(z^2, -z, 1, 0, \ldots, 0)$
BW19-P286	$(z^2, -z, 1, 0, \cdots, 0)$

subgroup membership testing

Conclusion:

- The new method for $\mathbb{G}_2$ and $\mathbb{G}_T$ membership testing requires approximately $\log r/\varphi(k)$ iterations on many popular pairing-friendly curve. The number of iterations for $\mathbb{G}_2$ membership testing can be reduced to approximately $\log r/(2\varphi(k))$ on some special curves.
- The new method for $\mathbb{G}_1$ membership testing is only suitable for ordinary curves with $j(E) \in \{0, 1728\}$, which requires approximately $\log r/2$ iterations on many popular pairing-friendly curves.

Thank you!

eccdaiy39@gmail.com