Revisiting Pairing-Friendly Curves with Embedding Degrees 10 and 14

Yu Dai [1] Debiao He[2] Cong Peng[2] Zhijian Yang[1] Chang-An Zhao[3]

[1] School of Mathematics and Statistics, Wuhan University, Wuhan, China.

[2] School of Cyber Science and Engineering, Wuhan University, Wuhan, China.

[3] School of Mathematics, Sun Yat-sen University, Guangzhou, China.

Talk at the Asiacrypt 2024.

Background

Elliptic curves

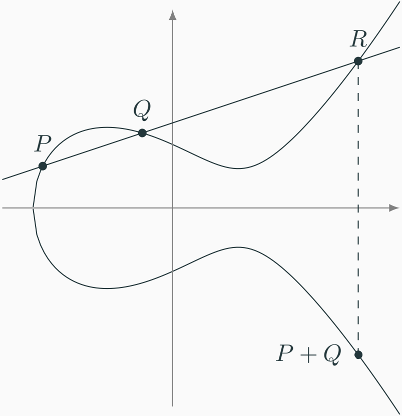

Figure 1: Group law on elliptic curve[a]

An elliptic curve E over $\mathbb{F}_p$ with $p > 3$ can be defined by an equation $y^2 = x^3 + ax + b$.

- $E(\bar{\mathbb{F}}_p)$ forms an addition group.
- $j(E) = 1728\frac{4a^3}{4a^3+27b^2}$.
- $\#E(\mathbb{F}_p) = p + 1 - t$, where $|t| \leq 2\sqrt{p}$.
- If $t \neq 0$, then E is ordinary.
- Cryptographic applications: $\#E(\mathbb{F}_p)$ has a large prime divisor r.

[a] This picture comes from Luca De Feo's github.

Pairings on elliptic curves

A cryptographic pairing on elliptic curves

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T,$$

where e is bilinear and non-degenerate.

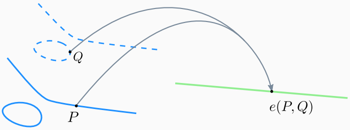

Figure 2: pairing[a]

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

[a] This picture is provided by Diego.F Aranha.

Pairings on elliptic curves

A cryptographic pairing on elliptic curves

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

where e is bilinear and non-degenerate.

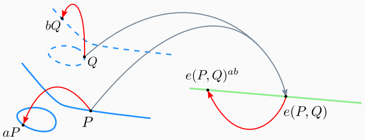

Figure 3: pairing[a]

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

[a] This picture is provided by Diego.F Aranha.

Building blocks

A cryptographic pairing on elliptic curves

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

Main building blocks in pairings-based protocols:

- Hashing to $\mathbb{G}_1$ and $\mathbb{G}_2$.
- group exponentiations in $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$.
- subgroup membership testing for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$.
- pairing computation.

Pairing-friendly curves: small values of k and $\rho = \log p / \log r$.

Optimal pairing

Optimal pairing

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

$$(P,Q) \to \left(\prod_{i=0}^{L} f_{c_i,Q}^{p^i}(P) \cdot \prod_{i=0}^{L-1} \frac{\ell_{[s_{i+1}]Q,[c_i p^i]Q}(P)}{\nu_{[s_i]Q}(P)} \right)^{\frac{(p^k-1)}{r}}$$

- $f_{m,Q}$: a rational function with divisor
$$div(f_{m,Q}) = m(Q) - ([m]Q) - (m-1)(\mathcal{O}_E).$$
- $\ell_{[i]R,[j]R}$: straight line passing through $[i]R$ and $[j]R$.
- $\nu_{[i+j]R}$: a vertical line passing through $[i+j]R$.
- $\mathbf{c} = (c_0, c_1, \cdots, c_L) \in \mathbb{Z}^{L+1}$ with $\sum_{i=0}^{L} c_i p^i \equiv 0$ mod r.
- $s_i = \sum_{j=i}^{L} c_j p^j$.

The shortest target vector satisfies that $\|\mathbf{c}\| \approx r^{1/\varphi(k)}$.

Miller's algorithm

Algorithm 1 MillerLoop(x, Q, P)

Input: $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$, $x = \sum_{i=0}^{\lfloor log_2 x \rfloor} x_i 2^i$
Output: $f_{x,Q}(P)$

1: $T \leftarrow Q$, $f \leftarrow 1$
2: **for** $i = \lfloor \log_2 x \rfloor - 1$ **downto** 0 **do**
3: $\quad f \leftarrow f^2 \cdot \frac{\ell_{T,T}(P)}{\nu_{2T}(P)}, T \longleftarrow 2T$
4: $\quad$ **if** $x_i = 1$ **then**
5: $\quad\quad f \leftarrow f \cdot \frac{\ell_{T,Q}(P)}{\nu_{T+Q}(P)}, T \leftarrow T + Q$
return f

Efficient implementation of Miller's algorithm:

- Optimal pairing$\rightarrow$ $\log r/\varphi(k)$ iterations.
- Fast point operation in projective coordinates.
- Denominator elimination$\rightarrow$ ν_R can be ignored if $2 \mid k$.

Pairing-friendly curves

Most of mainstream pairing-friendly curves can be parameterized by polynomials.

family	k	p	r	t
BN	12	$36z^4+36z^3+24z^2+6z+1$	$36z^4+36z^3+18z^2+6z+1$	$6z^2+1$
BLS12	12	$(z-1)^2(z^4-z^2+1)/3+z$	z^4-z^2+1	$z+1$
BW13	13	$(z+1)^2(z^{26}-z^{13}+1)/3-z^{27}$	$\Phi_{78}(z)$	$-z^{14}+z+1$

- the seed z should guarantee p and r are prime (or r has a large prime divisor).
- the sizes of p and r depend on the selected security level.

Parameters

Pairing-friendly curves at around 128-bit security level under the attack of the variant of number field sieve(NFS):

curve	seed z	$\lceil \log_2 p \rceil$	$\lceil \log_2 r \rceil$	$\lceil \log_2 p^k \rceil$	DL cost in $\mathbb{F}_{p^k}$
optimistic curves					
BLS12-381	$-2^{63}-2^{62}-2^{60}-2^{57}-2^{48}-2^{16}$	381	255	4569	126
BN-382	$-2^{94}-2^{78}-2^{67}-2^{64}-2^{48}-1$	382	382	4584	126
conservative curves					
BLS12-446	$-2^{74}-2^{73}-2^{63}-2^{57}-2^{50}-2^{17}-1$	446	299	5376	132
BN446	$2^{110}+2^{36}+1$	446	446	5376	132
BW13-310	$-2^{11}-2^{7}-2^{5}-2^{4}$	310	267	4027	140

Parameters

Pairing-friendly curves at around 128-bit security level under the attack of the variant of number field sieve(NFS):

curve	seed z	$\lceil \log_2 p \rceil$	$\lceil \log_2 r \rceil$	$\lceil \log_2 p^k \rceil$	DL cost in $\mathbb{F}_{p^k}$
		optimistic curves			
BLS12-381	$-2^{63}-2^{62}-2^{60}-2^{57}-2^{48}-2^{16}$	381	255	4569	126
BN-382	$-2^{94}-2^{78}-2^{67}-2^{64}-2^{48}-1$	382	382	4584	126
		conservative curves			
BLS12-446	$-2^{74}-2^{73}-2^{63}-2^{57}-2^{50}-2^{17}-1$	446	299	5376	132
BN446	$2^{110}+2^{36}+1$	446	446	5376	132
BW13-310	$-2^{11}-2^{7}-2^{5}-2^{4}$	310	267	4027	140

How to choose pairing-friendly curves:

- BLS12-381: fast pairing for non-conservative curves.
- BLS12-446: fast pairing for conservative curves.
- BW13-310: fast group exponentiation in $\mathbb{G}_1$.

BW13-310

The performance difference of pairing computation between BW13-310 and BN446 is slight. More details for pairing computation on BW13-310:

- The point doubling/addition is costly as $\mathbb{G}_2$ is defined over $\mathbb{F}_{p^{13}}$.
- The trick of denominator elimination is not suitable any more.
- **The length of Miller loop can be reduced to around** $\log r/(2\varphi(k))$**.**

BW13-310

The performance difference of pairing computation between BW13-310 and BN446 is slight. More details for pairing computation on BW13-310:

- The point doubling/addition is costly as $\mathbb{G}_2$ is defined over $\mathbb{F}_{p^{13}}$.
- The trick of denominator elimination is not suitable any more.
- **The length of Miller loop can be reduced to around $\log r/(2\varphi(k))$.**

Question

Are there pairing-friendly curves with such that the Miller loop can be performed in $\log r/(2\varphi(k))$ iterations, and the trick of denominator elimination applies as well?

Yes! Pairing-friendly curves with embedding degrees 10 and 14.

Curves with embedding degrees 10 and 14

Curve parameters and pairing formulas

Freeman, Scott and Teske construct a list of pairing-friendly curves with embedding degrees 10 and 14.

family-k	$j(E)$	p	r	t
Cyclo(6.3)-10	1728	$\frac{1}{4}(z^{14} - 2z^{12} + z^{10} + z^4 + 2z^2 + 1)$	$\Phi_{20}(z)$	$z^2 + 1$
Cyclo(6.5)- 10	1728	$\frac{1}{4}(z^{12} - z^{10} + z^8 - 5z^6 + 5z^4 - 4z^2 + 4)$	$\Phi_{20}(z)$	$-z^6 + z^4 - z^2 + 2$
Cyclo(6.6)-10	0	$\frac{1}{3}(z^3 - 1)^2(z^{10} - z^5 + 1) + z^3$	$\Phi_{30}(z)$	$z^3 + 1$
Cyclo(6.3)-14	1728	$\frac{1}{4}(z^{18} - 2z^{16} + z^{14} + z^4 + 2z^2 + 1)$	$\Phi_{28}(z)$	$z^2 + 1$
Cyclo(6.6)-14	0	$\frac{1}{3}(z - 1)^2(z^{14} - z^7 + 1) + z^{15}$	$\Phi_{42}(z)$	$z^8 - z + 1$

Curve parameters and pairing formulas

Freeman, Scott and Teske construct a list of pairing-friendly curves with embedding degrees 10 and 14.

family-k	$j(E)$	p	r	t
Cyclo(6.3)-10	1728	$\frac{1}{4}(z^{14}-2z^{12}+z^{10}+z^4+2z^2+1)$	$\Phi_{20}(z)$	z^2+1
Cyclo(6.5)- 10	1728	$\frac{1}{4}(z^{12}-z^{10}+z^8-5z^6+5z^4-4z^2+4)$	$\Phi_{20}(z)$	$-z^6+z^4-z^2+2$
Cyclo(6.6)-10	0	$\frac{1}{3}(z^3-1)^2(z^{10}-z^5+1)+z^3$	$\Phi_{30}(z)$	z^3+1
Cyclo(6.3)-14	1728	$\frac{1}{4}(z^{18}-2z^{16}+z^{14}+z^4+2z^2+1)$	$\Phi_{28}(z)$	z^2+1
Cyclo(6.6)-14	0	$\frac{1}{3}(z-1)^2(z^{14}-z^7+1)+z^{15}$	$\Phi_{42}(z)$	z^8-z+1

family-k	short vector	optimal pairing
Cyclo(6.3)-10	$[z^2,-1,0,0]$	$\left(f_{z^2,Q}(P)\right)^{(p^{10}-1)/r}$
Cyclo(6.5)-10	$[-1,z^2,0,0]$	$\left(f_{z^2,Q}(P)\right)^{(p^{10}-1)/r}$
Cyclo(6.6)-10	$[z,0,-1,z^2]$	$\left(f_{z,Q}(P)\cdot f^{p^3}_{z^2,Q}(P)\cdot \ell_{\pi^7(Q),\pi^3([z^2]Q)}(P)\right)^{(p^{10}-1)/r}$
Cyclo(6.3)-14	$[z^2,-1,0,0,0,0]$	$\left(f_{z^2,Q}(P)\right)^{(p^{14}-1)/r}$
Cyclo(6.6)-14	$[z^2,z,1,0,0,0]$	$\left(f_{z^2,Q}(P)\cdot f^{p}_{z,Q}(P)\cdot \ell_{\pi^2(Q),\pi([z]Q)}(P)\right)^{(p^{14}-1)/r}$

New pairing formulas

Efficiently computable endomorphisms on ordinary curves:

- the Frobenius map: $\pi : (x, y) \to (x^p, y^p)$.
- the GLV map:
$$\tau : \begin{cases} (x, y) \to (\omega \cdot x, y), & j(E) = 0, \omega^2 + \omega + 1 = 0 \text{ mod } p; \\ (x, y) \to (-x, i \cdot y), & j(E) = 1728, i^2 + 1 = 0 \text{ mod } p. \end{cases}$$

New pairing formulas

Efficiently computable endomorphisms on ordinary curves:

- the Frobenius map: $\pi : (x, y) \to (x^p, y^p)$.
- the GLV map:
$$\tau : \begin{cases} (x, y) \to (\omega \cdot x, y), & j(E) = 0, \omega^2 + \omega + 1 = 0 \text{ mod } p; \\ (x, y) \to (-x, i \cdot y), & j(E) = 1728, i^2 + 1 = 0 \text{ mod } p. \end{cases}$$

Main idea

Restricting the above two endomorphisms on $\mathbb{G}_2$ for our target curves, the GLV map is not a power of the Frobenius map. More interesting, there always exists an integer m such that $\pi^m \tau(Q) = [z]Q$ for $\mathbb{G}_2 \in Q$.

New pairing formulas

Optimized formulas of the optimal pairing on pairing-friendly curves with embedding degrees 10 and 14:

1. Rewrite $f_{z^2,Q}(P)$ as

$$\begin{aligned} f_{z^2,Q}(P) &= f_{z,Q}^{z}(P) \cdot f_{z,[z]Q}(P) = f_{z,Q}^{z}(P) \cdot f_{z,\pi^m \tau(Q)}(P) \\ &= f_{z,Q}^{z}(P) \cdot f_{z,Q}^{p^m}(\hat{\tau}(P)) \end{aligned}$$

   where $\hat{\tau}$ is the dual of τ.

New pairing formulas

Optimized formulas of the optimal pairing on pairing-friendly curves with embedding degrees 10 and 14:

1. Rewrite $f_{z^2,Q}(P)$ as
$$\begin{aligned} f_{z^2,Q}(P) &= f^z_{z,Q}(P) \cdot f_{z,[z]Q}(P) = f^z_{z,Q}(P) \cdot f_{z,\pi^m\tau(Q)}(P) \\ &= f^z_{z,Q}(P) \cdot f^{p^m}_{z,Q}(\hat{\tau}(P)) \end{aligned}$$
where $\hat{\tau}$ is the dual of τ.
2. Raise the output of the Miller loop to a power of p^{k-m} such that the exponent of $f_{z,Q}(\hat{\tau}(P))$ is equal to 1.

New pairing formulas

Optimized formulas of the optimal pairing on pairing-friendly curves with embedding degrees 10 and 14:

1. Rewrite $f_{z^2,Q}(P)$ as
$$\begin{aligned} f_{z^2,Q}(P) &= f_{z,Q}^{z}(P) \cdot f_{z,[z]Q}(P) = f_{z,Q}^{z}(P) \cdot f_{z,\pi^m\tau(Q)}(P) \\ &= f_{z,Q}^{z}(P) \cdot f_{z,Q}^{p^m}(\hat{\tau}(P)) \end{aligned}$$
where $\hat{\tau}$ is the dual of τ.
2. Raise the output of the Miller loop to a power of p^{k-m} such that the exponent of $f_{z,Q}(\hat{\tau}(P))$ is equal to 1.

family	k	new pairing formula
Cyclo(6.3)	10	$\left(f_{z,Q}^{z\cdot p^7}(P) \cdot f_{z,Q}(\hat{\tau}(P))\right)^{(p^{10}-1)/r}$
Cyclo(6.5)	10	$\left(f_{z,Q}^{z\cdot p^3}(P) \cdot f_{z,Q}(\hat{\tau}(P))\right)^{(p^{10}-1)/r}$
Cyclo(6.6)	10	$\left(f_{z,Q}^{1+z\cdot p^3}(P) \cdot f_{z,Q}(\hat{\tau}(P)) \cdot (y_P - y_Q)^{p^7}\right)^{(p^{10}-1)/r}$
Cyclo(6.3)	14	$\left(f_{z,Q}^{z\cdot p^{10}}(P) \cdot f_{z,Q}(\hat{\tau}(P))\right)^{(p^{14}-1)/r}$
Cyclo(6.6)	14	$\left(f_{z,Q}^{1+z\cdot p^{13}}(P) \cdot f_{z,Q}(\hat{\tau}(P)) \cdot (y_P - y_Q)^{p}\right)^{(p^{14}-1)/r}$

Shared Miller's algorithm

The computation of $f_{z,Q}^{z\cdot p^{k-m}}(P) \cdot f_{z,Q}(\hat{\tau}(P))$ can be performed in a shared Miller's algorithm at around $\log z \approx \log r/2(\varphi(k))$ iterations.

Algorithm 2 Computing $f_{z,Q}^{z\cdot p^{k-m}}(P) \cdot f_{z,Q}(\hat{\tau}(P))$

Require: $P \in \mathbb{G}_1, Q \in \mathbb{G}_2, z = \sum_{i=0}^{L} z_i \cdot 2^i$ with $z_i \in \{-1, 0, 1\}$
Ensure: $f_{z,Q}^{z\cdot p^{k-m}}(P) \cdot f_{z,Q}(\hat{\tau}(P))$

$T \leftarrow Q, f \leftarrow 1$, tab$\leftarrow [\,], j \leftarrow 0$
for $i = L-1$ **down to** 0 **do**
  $f \leftarrow f^2 \cdot \ell_{T,T}(P)$, tab$[j] \leftarrow \ell_{T,T}(\hat{\tau}(P))$
  $T \longleftarrow 2T, j \leftarrow j+1$
  if $z_i = 1$ **then**
    $f \leftarrow f \cdot \ell_{T,Q}(P)$,tab$[j] \leftarrow \ell_{T,Q}(\hat{\tau}(P))$
    $T \leftarrow T+Q, j \leftarrow j+1$
  elif $z_i = -1$ **then**
    $f \leftarrow f \cdot \ell_{T,-Q}(P)$, tab$[j] \leftarrow \ell_{T,-Q}(\hat{\tau}(P))$
    $T \leftarrow T-Q, j \leftarrow j+1$
  end if
end for
$g \leftarrow f^{p^{k-m}}, h \leftarrow g, j \leftarrow 0$
for $i = L-1$ **down to** 0 **do**
  $h \leftarrow h^2 \cdot$tab$[j], j \leftarrow j+1$
  if $z_i = 1$ **then**
    $h \leftarrow h \cdot g \cdot$tab$[j], j \leftarrow j+1$
  elif $z_i = -1$ **then**
    $h \leftarrow h \cdot \bar{g} \cdot$tab$[j], j \leftarrow j+1$
  end if
end for
return h

Five candidate curves

The best seed z can guarantee that:

- the size of $\mathbb{F}_{p^k}$ is large enough to resist the attacks of the variant of NFS.
- the sum of bit length and Hamming weight (in non-adjacent form) of the selected seed z is as small as possible.
- the selected prime p satisfies that $p \equiv 1 \bmod k$.

Five candidate curves

The best seed z can guarantee that:

- the size of $\mathbb{F}_{p^k}$ is large enough to resist the attacks of the variant of NFS.
- the sum of bit length and Hamming weight (in non-adjacent form) of the selected seed z is as small as possible.
- the selected prime p satisfies that $p \equiv 1 \bmod k$.

curve	family-k	seed z	r bits	p bits	p^k bits	DL cost in $\mathbb{F}_{p^k}$
BW10-480	Cyclo(6.5)-10	$2^5+2^{14}+2^{15}+2^{18}+2^{36}+2^{40}$	321	480	4791	128
BW10-511	Cyclo(6.6)-10	$2^7+2^{13}+2^{26}-2^{32}$	256	511	5101	150
BW10-512	Cyclo(6.3)-10	$1+2^3+2^{17}+2^{32}+2^{35}+2^{36}$	294	512	5111	129
BW14-351	Cyclo(6.6)-14	$2^6-2^{12}-2^{14}-2^{22}$	265	351	4908	149
BW14-382	Cyclo(6.3)-14	$1+2^{10}+2^{13}-2^{16}+2^{19}+2^{21}$	256	382	5338	129

Remark1: The candidate curves are conservative 128-bit secure.

Remark2: The candidate curves are collectively called BW curves since they are essentially generated using the Brezing-Weng method.

The fist pairing group

Recall that the first pairing group $\mathbb{G}_1 = E(\mathbb{F}_p)[r]$. There exists an efficiently computable endomorphism on $\mathbb{G}_1$:

$$\tau : \begin{cases} (x,y) \to (\omega \cdot x, y), & j(E) = 0, \omega^2 + \omega + 1 = 0 \text{ mod } p; \\ (x,y) \to (-x, i \cdot y), & j(E) = 1728, i^2 + 1 = 0 \text{ mod } p. \end{cases}$$

The operations in $\mathbb{G}_1$:

- group exponentiation in $\mathbb{G}_1$: log $r/2$ iterations by using GLV method.
- membership testing for $\mathbb{G}_1$: log $r/2$ iterations with a fixed scalar.
- hashing to $\mathbb{G}_1$: hashing to $E(\mathbb{F}_p)+$ cofactor clearing.

cofactor clearing for $\mathbb{G}_1$

The process of cofactor clearing for $\mathbb{G}_1$:

$$E(\mathbb{F}_p) \xrightarrow{m_1} E(\mathbb{F}_p)[n_1 \cdot r] \to E(\mathbb{F}_p)[r] = \mathbb{G}_1$$

where $E(\mathbb{F}_p) \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_1 \cdot n_1 \cdot r}$.

The process of cofactor clearing for $\mathbb{G}_1$:

$$E(\mathbb{F}_p) \xrightarrow{m_1} E(\mathbb{F}_p)[n_1 \cdot r] \to E(\mathbb{F}_p)[r] = \mathbb{G}_1$$

where $E(\mathbb{F}_p) \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_1 \cdot n_1 \cdot r}$.

How to clear n_1:

1. Determine the integer λ_1 such that $\tau = \lambda_1$ in $E(\mathbb{F}_p)[n_1 \cdot r]$.
2. Applying the LLL algorithm, find a short vector **a** $= (a_0, a_1)$ such that $a_0 + a_1 \cdot \lambda_1 \equiv 0 \bmod n_1$ with $\max\{\log|a_0|, \log|a_1|\} \approx \log n_1/2$.
3. Clearing the cofactor n_1 by using the endomorphism $a_0 + a_1\tau$.

The second pairing group

The degree-2 twisted curve

For our target curves, there exists a twisted curve E' over $\mathbb{F}_{p^e}$ of degree 2 such that $E' \cong E$ over $\mathbb{F}_{p^k}$ under a twisted map ϕ, where $e = k/2$.

The group $\mathbb{G}_2 = E[r] \cap \ker(\pi - [p])$ can be efficiently represented as $E'(\mathbb{F}_{p^e})[r]$.

The second pairing group

The degree-2 twisted curve

For our target curves, there exists a twisted curve E' over $\mathbb{F}_{p^e}$ of degree 2 such that $E' \cong E$ over $\mathbb{F}_{p^k}$ under a twisted map ϕ, where $e = k/2$.

The group $\mathbb{G}_2 = E[r] \cap \ker(\pi - [p])$ can be efficiently represented as $E'(\mathbb{F}_{p^e})[r]$.
The endomorphism on $\mathbb{G}_2$:

$$\tau, \pi' = \phi^{-1} \circ \pi \circ \phi, \Psi = \tau \circ \pi',$$

where the order of Ψ restricting on $\mathbb{G}_2$ is $2k$ (if $j(E) = 1728$) or $3k$ (if $j(E) = 0$).

The second pairing group

The degree-2 twisted curve

For our target curves, there exists a twisted curve E' over $\mathbb{F}_{p^e}$ of degree 2 such that $E' \cong E$ over $\mathbb{F}_{p^k}$ under a twisted map ϕ, where $e = k/2$.

The group $\mathbb{G}_2 = E[r] \cap \ker(\pi - [p])$ can be efficiently represented as $E'(\mathbb{F}_{p^e})[r]$.
The endomorphism on $\mathbb{G}_2$:

$$\tau, \pi' = \phi^{-1} \circ \pi \circ \phi, \Psi = \tau \circ \pi',$$

where the order of Ψ restricting on $\mathbb{G}_2$ is $2k$ (if $j(E) = 1728$) or $3k$ (if $j(E) = 0$).
The operations in $\mathbb{G}_2$:

- group exponentiation in $\mathbb{G}_2$: log $r/(2\varphi(k))$ iterations by combining the GLV and GLS methods.
- subgroup membership testing for $\mathbb{G}_2$: log $r/(2\varphi(k))$ iterations with a fixed scalar.
- hashing to $\mathbb{G}_2$: hashing to $E'(\mathbb{F}_{p^e})+$ cofactor clearing.

The subgroup $\mathbb{G}'_0$

Cyclotomic zero subgroup of E'

Define $\mathbb{G}'_0 = \{Q \in E'(\mathbb{F}_{p^e}) | \Phi_k(\pi')(Q) = \mathcal{O}_{E'}\}$, where Φ_k is the k—th cyclotomic polynomial.

- $\mathbb{G}_2 \subseteq \mathbb{G}'_0 \subseteq E'(\mathbb{F}_{p^e})$.
- the order of $\mathbb{G}'_0$ is equal to $\frac{\#E'(\mathbb{F}_{p^e}) \cdot \#E(\mathbb{F}_p)}{\#E(\mathbb{F}_{p^2})}$.
- Given a random point $Q \in E'(\mathbb{F}_{p^e})$, then $R = (\pi' + 1)Q \in \mathbb{G}'_0$ as

$$\Phi_k(\pi')(R) = (\pi'^e + 1)Q = \mathcal{O}_{E'}.$$

cofactor clearing for $\mathbb{G}_2$

The process of cofactor clearing for $\mathbb{G}_2$:

$$E'(\mathbb{F}_{p^e}) \to \mathbb{G}_0' \xrightarrow{m_2} E'(\mathbb{F}_{p^e})[n_2 \cdot r] \to \mathbb{G}_2,$$

where $\mathbb{G}_0' \cong \mathbb{Z}_{m_2} \oplus \mathbb{Z}_{m_2 \cdot n_2 \cdot r}$ for some integers m_2 and n_2.

cofactor clearing for $\mathbb{G}_2$

The process of cofactor clearing for $\mathbb{G}_2$:

$$E'(\mathbb{F}_{p^e}) \to \mathbb{G}_0' \xrightarrow{m_2} E'(\mathbb{F}_{p^e})[n_2 \cdot r] \to \mathbb{G}_2,$$

where $\mathbb{G}_0' \cong \mathbb{Z}_{m_2} \oplus \mathbb{Z}_{m_2 \cdot n_2 \cdot r}$ for some integers m_2 and n_2.

How to clear n_2:

1. Determine the integer λ_2 such that $\Psi = \lambda_2$ in $E'(\mathbb{F}_{p^{k/2}})[n_2 \cdot r]$.
2. Applying the LLL algorithm, find **a** $= (a_0, a_1, \cdots, a_{2\varphi(k)-1})$ such that

$$a_0 + a_1 \cdot \lambda_2 + \cdots + a_{2\varphi(k)-1} \cdot \lambda_2^{2\varphi(k)-1} \equiv 0 \bmod n_2$$

   with $\max\{\log |a_i|\} \approx \log n_2/(2\varphi(k))$.

3. Clearing the cofactor n_2 by using the endomorphism

$$a_0 + a_1\Psi + \cdots + a_{2\varphi(k)-1}\Psi^{2\varphi(k)-1}.$$

The third pairing group

The operations in $\mathbb{G}_T$:

- group exponentiation in $\mathbb{G}_T$: $\log r/\varphi(k)$ iterations by using the GLS method.
- subgroup membership testing for $\mathbb{G}_T$: $\log r/\varphi(k)$ iterations with a fixed exponent.

The third pairing group

The operations in $\mathbb{G}_T$:

- group exponentiation in $\mathbb{G}_T$: $\log r/\varphi(k)$ iterations by using the GLS method.
- subgroup membership testing for $\mathbb{G}_T$: $\log r/\varphi(k)$ iterations with a fixed exponent.

Remark 1: Inversion in $\mathbb{G}_T$ is almost free as it is equal to its conjugate.

Remark 2: Squaring in $\mathbb{G}_T$ is slightly faster than the squaring in $\mathbb{F}_{p^k}$.

Implementation results

conservative curves: BLS12-446, BN-446, BW13-310 VS BW10-511, BW14-351

Target platform: Intel Core i9-12900K processor

Library: RELIC

Operation\Curve	BLS12-446	BN446	BW13-310	BW10-511	BW14-351
hashing to $\mathbb{G}_1$	327	149	125	621	204
hashing to $\mathbb{G}_2$	1630	1361	16699	11981	7236
exp in $\mathbb{G}_1$	541	791	268	592	362
exp in $\mathbb{G}_2$	918	1394	7247	4621	3531
exp in $\mathbb{G}_T$	1322	2243	1062	1476	1098
test in $\mathbb{G}_1$	389	8	269	723	345
test in $\mathbb{G}_2$	333	487	1176	1262	923
test in $\mathbb{G}_T$	372	540	223	586	384
ML	1554	2480	1719	2819	1600
FE	1835	1589	2579	3872	2337
Single pairing	3389	4069	4298	6691	3937
2-pairings	4439	5717	5640	9016	5205
5-pairings	7614	10532	9621	15621	9008
8-pairings	10790	15349	13603	22191	12811

Table 1: Timings in 10^3 cycles averaged over 10^4 executions.

`https://github.com/eccdaiy39/BW10-14`

eccdaiy39@gmail.com

Thank you!