Co-factor clearing and subgroup membership testing in pairing groups

Youssef El Housni[1,2] Aurore Guillevic[3] Thomas Piellard[1]

[1]ConsenSys

[2]Ecole Polytechnique / Inria Saclay

[3]Université de Lorraine / Inria Nancy / Aarhus University

AFRICACRYPT, July 2022


DALL·E mini
AI model generating images from any prompt!
Co-factor clearing and subgroup membership testing in pairing groups
Run

(Pairing)

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

- Pairing groups: $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ are sub-groups of some prime order order r.
- Co-factors: They are defined over some larger groups of composite orders $c_{1,2,T} \times r$

Let P be a random element of order $c_{1,2,T} \times r$

- Co-factor clearing: $[c_{1,2,T}]P = Q$
- Subgroup membership testing: $[r]Q \stackrel{?}{=} \mathcal{O}$

References

Youssef El Housni and Aurore Guillevic.
Families of SNARK-friendly 2-chains of elliptic curves.
In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022*, volume 13276 of *LNCS*, pages 367–396. Springer, 2022.
ePrint 2021/1359.

Youssef El Housni, Aurore Guillevic, and Thomas Piellard.
Co-factor clearing and subgroup membership testing on pairing-friendly curves.
In Lejla Batina and Joan Daemen, editors, *AFRICACRYPT'2022*, LNCS, Fes, Morocco, 7 2022. Springer.
to appear, ePrint 2022/352.

(Pairing)

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

- Pairing groups: $\mathbb{G}_1, \mathbb{G}_2$ are sub-groups of some prime order order r.
- Co-factors: They are defined over some larger groups of composite orders $c_{1,2} \times r$

Let P and Q be random elements of order $c_1 \times r$ and resp. $c_2 \times r$,

- Co-factor clearing: $[c_1]P$
- Subgroup membership testing: $[r]P \stackrel{?}{=} \mathcal{O}$ and $[r]Q \stackrel{?}{=} \mathcal{O}$

Outline

Outline

1. Motivation
2. Faster co-factor clearing
3. GLV on elliptic curves
4. Subgroup membership testing with GLV
5. Ensuring correct subgroup membership testing in $\mathbb{G}_1$ and $\mathbb{G}_2$

Motivation

- Hash-to-curve: encoding an arbitrary input to a point on an elliptic curve
  - authenticated key exchanges [BM92] [J96] [BMP00]
  - Identity-Based Encryption [BF01]
  - Boneh-Lynn-Shacham signatures [BLS01]
  - Verifiable Random Functions [MRV99]
  - Oblivious Pseudorandom Functions [NR97]
- Pitfalls: small-subgroup-attacks [MO06] (MQV, Monero), non-injective behavior, implementation-defined behavior

Outline

Bilinear pairing

- $E\colon y^2 = x^3 + ax + b$ elliptic curve defined over $\mathbb{F}_q$, q a prime power.
- r prime divisor of $\#E(\mathbb{F}_q) = q + 1 - t$, t Frobenius trace.
- k embedding degree, smallest integer $k \in \mathbb{N}^*$ s.t. $r \mid q^k - 1$.
- a bilinear pairing

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

  - $\mathbb{G}_1 \subset E(\mathbb{F}_q)$ a group of order r
  - $\mathbb{G}_2 \subset E(\mathbb{F}_{q^k})$ a group of order r
  - $\mathbb{G}_T \subset \mathbb{F}^*_{q^k}$ group of r-th roots of unity

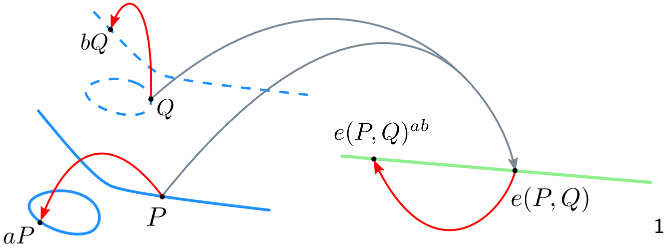
Bilinear pairing

$$e : (\mathbb{G}_1, +) \times (\mathbb{G}_2, +) \to (\mathbb{G}_T, \cdot)$$

non-degenerate: $\forall P \in \mathbb{G}_1,\ P \neq \mathcal{O},\ \exists Q \in \mathbb{G}_2, e(P,Q) \neq 1_{\mathbb{G}_T}$
$\forall Q \in \mathbb{G}_2,\ Q \neq \mathcal{O},\ \exists P \in \mathbb{G}_1, e(P,Q) \neq 1_{\mathbb{G}_T}$

bilinear: $e([a]P,[b]Q) = e(P,[b]Q)^a = e([a]P,Q)^b = e(P,Q)^{ab}$

efficiently computable



BLS12

Order $\#E(\mathbb{F}_q) = 3\ell^2 r$ where $\ell = (u-1)/3$, $r = u^4 - u^2 + 1$

Co-factor clearing

Given $P \in E(\mathbb{F}_q)$ (e.g. result of a hash map $\{0,1\}^* \to E(\mathbb{F}_q)$), compute $[c_1]P$ where $c_1 = \#E(\mathbb{F}_q)/\#\mathbb{G}_1$

Wahby–Boneh, CHES'2019: $c_1 = 3\ell^2$ but no point of order ℓ^2 **for BLS12-381 curve**, only points of order dividing ℓ

$\implies$ compute only $[\ell]P$

Luck or generic pattern?

Schoof's theorem 3.7 (1987)

René Schoof.
Nonsingular plane cubic curves over finite fields.
Journal of Combinatorial Theory, Series A, 46(2):183–211, 1987.

$$E[\ell] \subset E(\mathbb{F}_q) \iff \begin{cases} \ell^2 \mid \#E(\mathbb{F}_q) \\ \ell \mid q-1 \\ \mathcal{O}\left(\frac{t^2-4q}{n^2}\right) \subset \mathrm{End}_{\mathbb{F}_q}(E) \text{ (or } \pi_q \in \mathbb{Z}) \end{cases}$$

Generic pattern for all BLS curves

BLS-k curves, $3 \mid k$

- $c = (x-1)^2/3(x^{2k/3} + x^{k/3} + 1)/\Phi_k(x)$, $k = 3 \bmod 6$
- $c = (x-1)^2/3(x^{k/3} - x^{k/6} + 1)/\Phi_k(x)$, $k = 0 \bmod 6$

and $E(\mathbb{F}_q)[\ell] = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ where $\ell = (x-1)/3$.

Other pairing-friendly curves

Freeman, Scott, Teske.
A taxonomy of pairing-friendly elliptic curves.
Journal of Cryptology, doi: "10.1007/s00145-009-9048-z", 2010.

For all curves in the Taxonomy paper,

- we identify the families such that the cofactor has a square factor
- we check the conditions of Schoof's theorem
- we list the curves with faster co-factor clearing: all but KSS and 6.6 where $k \equiv 2, 3 \bmod 6$.

SageMath verification script at

`gitlab.inria.fr/zk-curves/cofactor`

Outline

Scalar multiplication on elliptic curves (Double-and-Add)

Input: Elliptic curve E over $\mathbb{F}_q$, point $P \in E(\mathbb{F}_q)$, scalar $m \in \mathbb{Z}$

Output: $[m]P$

if $m = 0$ **then**
    return $\mathcal{O}$
if $m < 0$ **then**
    $m \leftarrow -m$; $P \leftarrow -P$
write m in binary expansion $m = \sum_{i=0}^{n-1} b_i 2^i$, where $b_i \in \{0, 1\}$
$R \leftarrow P$
for $i = n - 2$ *downto* 0 **do**
    $R \leftarrow [2]R$
    if $b_i = 1$ **then**
        $R \leftarrow R + P$
return R

Scalar multiplication on elliptic curves (Double-and-Add)

Input: Elliptic curve E over $\mathbb{F}_q$, point $P \in E(\mathbb{F}_q)$, scalar $m \in \mathbb{Z}$
Output: $[m]P$

if $m = 0$ **then**
    return $\mathcal{O}$
if $m < 0$ **then**
    $m \leftarrow -m$; $P \leftarrow -P$
write m in binary expansion $m = \sum_{i=0}^{n-1} b_i 2^i$, where $b_i \in \{0, 1\}$
$R \leftarrow P$
for $i = n-2$ *downto* 0 **do**
    $R \leftarrow [2]R$
    if $b_i = 1$ **then**
        $R \leftarrow R + P$
return R

$\log_2 m$ **(Dbl +** $\frac{1}{2}$ **Add) in average**

Multi-scalar multiplication

Input: Elliptic curve E over $\mathbb{F}_q$, points $P, Q \in E(\mathbb{F}_q)$, scalars $m \geq m' > 0 \in \mathbb{Z}^{+*}$
Output: $[m]P + [m']Q$

```
write m = Σ_{i=0}^{n-1} b_i 2^i, m' = Σ_{i=0}^{n'-1} b'_i 2^i, where b_i, b'_i ∈ {0,1}
S ← P + Q
if n > n' then  R ← P
else  R ← S  (n = n')
for i = n − 2 downto 0 do
    R ← [2]R
    if b_i = 1 and n' ≥ i and b'_i = 1 then
        R ← R + S
    else if b_i = 1 and (n' < i or b'_i = 0) then
        R ← R + P
    else if n' ≥ i and b'_i = 1 then
        R ← R + Q
return R
```

Multi-scalar multiplication

Input: Elliptic curve E over $\mathbb{F}_q$, points $P, Q \in E(\mathbb{F}_q)$, scalars $m \geq m' > 0 \in \mathbb{Z}^{+*}$
Output: $[m]P + [m']Q$

write $m = \sum_{i=0}^{n-1} b_i 2^i$, $m' = \sum_{i=0}^{n'-1} b'_i 2^i$, where $b_i, b'_i \in \{0, 1\}$
$S \leftarrow P + Q$
if $n > n'$ **then** $R \leftarrow P$
else $R \leftarrow S \quad (n = n')$
for $i = n - 2$ *downto* 0 **do**
  $R \leftarrow [2]R$
  if $b_i = 1$ *and* $n' \geq i$ *and* $b'_i = 1$ **then**
    $R \leftarrow R + S$
  else if $b_i = 1$ *and* $(n' < i$ *or* $b'_i = 0)$ **then**
    $R \leftarrow R + P$
  else if $n' \geq i$ *and* $b'_i = 1$ **then**
    $R \leftarrow R + Q$
return R

$\log_2 m$ **(Dbl +** $\frac{3}{4}$ **Add) in average**

Gallant–Lambert–Vanstone (GLV) with endomorphism

Gallant, Lambert, Vanstone.
Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms.
CRYPTO 2001.

An example: $j = 0$

Let $E\colon y^2 = x^3 + b$ defined over a prime field $\mathbb{F}_q$ where $q = 1 \bmod 3$.
There exists $\omega \in \mathbb{F}_q$ such that $\omega^3 = 1$, $\omega \neq 1$

$$\omega^3 - 1 = \underbrace{(\omega - 1)}_{\neq 0}\underbrace{(1 + \omega + \omega^2)}_{=0} = 0$$

$$\begin{array}{rcl} \phi\colon E(\mathbb{F}_q) & \to & E(\mathbb{F}_q) \\ P(x, y) & \mapsto & (\omega x, y), \text{ where } \omega \in \mathbb{F}_q,\ \omega^2 + \omega + 1 = 0 \end{array}$$

ϕ is an **endomorphism**,
$\phi^2\colon (x, y) \mapsto (\omega^2 x, y)$, $\phi^3 = \mathrm{Id}$ because $\omega^3 = 1$, but $\phi \neq \mathrm{Id} \implies \phi^2 + \phi + 1 = 0$

Gallant–Lambert–Vanstone (GLV)

$$E\colon y^2 = x^3 + b$$
$$r \text{ is prime, } r \mid \#E(\mathbb{F}_q),\ r^2 \nmid \#E(\mathbb{F}_q)\text{:}$$

$$P \in E(\mathbb{F}_q)[r], Q \notin E(\mathbb{F}_q) \text{ but over an extension of } \mathbb{F}_q$$

$$\implies \phi(P) = [a]P + [0]Q = [\lambda]P$$

where λ mod r is the **eigenvalue** of ϕ: $\lambda^2 + \lambda + 1 = 0 \bmod r$, $\approx \sqrt{r} \leq |\lambda| \leq r - 1$.

Gallant–Lambert–Vanstone (GLV)

$$E\colon y^2 = x^3 + b$$
r is prime, $r \mid \#E(\mathbb{F}_q)$, $r^2 \nmid \#E(\mathbb{F}_q)$:

$P \in E(\mathbb{F}_q)[r], Q \notin E(\mathbb{F}_q)$ but over an extension of $\mathbb{F}_q$

$$\implies \phi(P) = [a]P + [0]Q = [\lambda]P$$

where λ mod r is the **eigenvalue** of ϕ: $\lambda^2 + \lambda + 1 = 0 \bmod r$, $\approx \sqrt{r} \leq |\lambda| \leq r - 1$.

To speed-up $[m]P$, decompose $m = m_0 + m_1\lambda$ with $|m_0|, |m_1| \approx \sqrt{r}$ and use $[m]P = [m_0]P + [m_1\lambda]P = [m_0]P + [m_1]\underbrace{\phi(P)}_{\text{cheap}}$ with **multi-scalar** mutliplication

$$\frac{1}{2}\log_2 r \left(\mathrm{Dbl} + \frac{3}{4}\mathrm{Add}\right)$$

instead of $\log_2 |m| \left(\mathrm{Dbl} + \frac{1}{2}\mathrm{Add}\right) \implies$ factor ≈ 2 speed-up but cost of decomposition

Outline

BLS12

Barreto, Lynn, Scott method to get pairing-friendly curves.
Becomes more and more popular, replacing BN curves

$$E_{BLS}: \; y^2 = x^3 + b/\mathbb{F}_q, \; q \equiv 1 \bmod 3, \; j(E) = 0, \; D = -3 \text{ (ordinary)}$$

$$\begin{array}{rcl} q & = & (u-1)^2/3(u^4-u^2+1)+u \\ t & = & u+1 \\ r & = & (u^4-u^2+1) = \Phi_{12}(u) \\ q+1-t & = & (u-1)^2/3(u^4-u^2+1) \\ t^2-4q & = & -3y(u)^2 \;\rightarrow\; \text{no CM method needed} \end{array}$$

BLS12-381 with seed $u_0 =$-0xd201000000010000

BLS12 curves, testing if $P \in \mathbb{G}_1$ for $P \in E(\mathbb{F}_q)$

Well-known GLV trick: write $r_0 + r_1\lambda = 0 \bmod r$
with λ the eigenvalue of ϕ mod r, $\lambda = -u^2$.

$$\underbrace{1}_{r_0} + (\underbrace{1 - u^2}_{r_1})\lambda = r = u^4 - u^2 + 1$$

Compute $P + [1 - u^2]\phi(P) = ?\mathcal{O}$

$$P \in E(\mathbb{F}_q)[r] \implies \phi(P) = [\lambda]P$$

$$\phi(P) = [\lambda]P \not\Longrightarrow P \in E(\mathbb{F}_q)[r]$$

$\mathbb{G}_2$ technicalities

$\mathbb{G}_2$ is more tricky and the endomorphism is ψ, of characteristic polynomial

$$X^2 - tX + q$$

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

GLV on $\mathbb{G}_1 \to$ GLS (Galbraith Lin Scott) on $\mathbb{G}_2$

A point $Q \in E'(\mathbb{F}_{q^i})$ has some eigenvalue μ under ψ is a *consequence* of Q having order r

Michael Scott.
A note on group membership tests for G1, G2 and GT on BLS pairing-friendly curves.
ePrint, https://eprint.iacr.org/2021/1130.pdf.

- $\phi(P) = [\lambda]P \iff P \in \mathbb{G}_1$ (proof by contradition)
- $\psi(Q) = [\mu]Q \iff P \in \mathbb{G}_2$ (proof incorrect)

Outline

General criterion

Let $\tilde{E}(\mathbb{F}_{\tilde{q}})$ be a family of elliptic curves (i.e. it can be $E(\mathbb{F}_q)$ or $E'(\mathbb{F}_{q^{k/d}})$ for instance). Let $\mathbb{G}$ be a cryptographic group of $\tilde{E}$ of order r equipped with an efficient endomorphism $\tilde{\phi}$. It has a minimal polynomial $\tilde{\chi}$ and an eigenvalue $\tilde{\lambda}$. Let c be the cofactor of $\mathbb{G}$.

Proposition

If $\tilde{\phi}$ acts as the multiplication by $\tilde{\lambda}$ on $\tilde{E}(\mathbb{F}_{\tilde{q}})[r]$ and $\gcd(\tilde{\chi}(\tilde{\lambda}), c) = 1$ then

$$\tilde{\phi}(Q) = [\tilde{\lambda}]Q \iff Q \in \tilde{E}(\mathbb{F}_{\tilde{q}})[r] \ .$$

Example (Barreto–Naehrig family)

Let $E(\mathbb{F}_{q(x)})$ define the BN pairing-friendly family. It is parameterized by

$$q(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1;\ r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1;\ t(x) = 6x^2 + 1$$

and $E(\mathbb{F}_{q(x)})$ has a prime order so $c_1 = 1$. The cofactor on the sextic twist $E'(\mathbb{F}_{q^2})$ is $c = c_2$

$$c_2(x) = q(x) - 1 + t(x) = 36x^4 + 36x^3 + 30x^2 + 6x + 1\ .$$

On $\mathbb{G} = \mathbb{G}_2 = E'(\mathbb{F}_{q^2})[r]$, $\tilde{\phi} = \psi$ has a minimal polynomial $\tilde{\chi} = \chi$ and an eigenvalue $\tilde{\lambda} = \lambda$

$$\chi = X^2 - tX + q; \quad \lambda = 6X^2\ .$$

Applying the proposition (and taking care of exceptional cases),

Proposition

For the BN family, if $Q \in E'(\mathbb{F}_{q^2})$, $\psi(Q) = [u]Q \implies Q \in E'(\mathbb{F}_{q^2})[r]$.

Conclusion

- Many curve families have the $\mathbb{G}_1$ cofactor of the form $c_1 = 3\ell^2$. We show $P \mapsto [\ell]P$ is sufficient to clear the cofactor.
- For both $\mathbb{G}_1$ and $\mathbb{G}_2$, we give a common criterion that shows it is sufficient to verify the endomorphism to test membership $\tilde{\phi}(P) = \tilde{\lambda}P \iff P \in \mathbb{G}$
- Open-source implementation for different curves (BN, BLS12, BLS24) is available at

`https://github.com/ConsenSys/gnark-crypto`