Co-factor clearing and subgroup membership testing in pairing groups

Aurore Guillevic

Aarhus University and Inria Nancy

July 4, 2022

https://members.loria.fr/AGuillevic/files/talks/22-Aarhus-Crypto-Day.pdf

Outline

Introduction: GLV on elliptic curves

Subgroup membership testing with GLV on $\mathbf{G}_1$

Faster co-factor clearing

Ensuring correct subgroup membership testing in $\mathbf{G}_2$ and $\mathbf{G}_T$

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.

Outline

Introduction: GLV on elliptic curves

Subgroup membership testing with GLV on $\mathbf{G}_1$

Faster co-factor clearing

Ensuring correct subgroup membership testing in $\mathbf{G}_2$ and $\mathbf{G}_T$

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 𝒪
if m < 0 then
    m ← −m; P ← −P
write m in binary expansion m = Σ_{i=0}^{n−1} b_i 2^i, where b_i ∈ {0, 1}
R ← P
for i = n − 2 downto 0 do
    R ← [2]R
    if b_i = 1 then
        R ← 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 $m = \sum_{i=0}^{n-1} b_i 2^i$, $m' = \sum_{i=0}^{n'-1} b'_i 2^i$, where $b_i, b'_i \in \{0, 1\}$
$S \leftarrow P + Q$
if $n > n'$ **then** $R \leftarrow P$
else $R \leftarrow S$ $(n = n')$
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

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

An example: $j = 0$

Let $E\colon y^2 = x^3 + b$ defined over a prime field $\mathbb{F}_q$ where $q = 1 \bmod 3$.

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

ϕ is an **endomorphism** and $\phi^2 + \phi + 1 = 0$

ℓ-torsion points

Let $E\colon y^2 = x^3 + ax + b/\mathbb{F}_q$

$$E[\ell] = \{P \in E\colon [\ell]P = \mathcal{O}\}$$

and $\mathcal{O} \in E[\ell]$

ℓ-torsion points

Let $E\colon y^2 = x^3 + ax + b/\mathbb{F}_q$

$$E[\ell] = \{P \in E\colon [\ell]P = \mathcal{O}\}$$

and $\mathcal{O} \in E[\ell]$

Example

$\ell = 2$, $q \geq 5$: points of order 2 have $y = 0 \iff x^3 + ax + b = 0$.
Factor $x^3 + ax + b$ in $\mathbb{F}_q$:

- $x^3 + ax + b$ has no root in $\mathbb{F}_q$: $E(\mathbb{F}_q)[2] = \{\mathcal{O}\}$
- $(x - e_0)(x^2 + ux + v)$ over $\mathbb{F}_q$: $E(\mathbb{F}_q)[2] = \{(e_0, 0), \mathcal{O}\}$
- $(x - e_0)(x - e_1)(x - e_2)$ over $\mathbb{F}_q$: $E(\mathbb{F}_q)[2] = \{(e_0, 0), (e_1, 0), (e_2, 0), \mathcal{O}\}$

There exists an extension $\mathbb{F}_{q^i}$ such that $E(\mathbb{F}_{q^i})[2] = \{(x_0, 0), (x_1, 0), (x_2, 0), \mathcal{O}\}$

ℓ-torsion points

Let $E\colon y^2 = x^3 + ax + b/\mathbb{F}_q$

$$E[\ell] = \{P \in E\colon [\ell]P = \mathcal{O}\}$$

and $\mathcal{O} \in E[\ell]$

Example

$\ell = 2$, $q \geq 5$: points of order 2 have $y = 0 \iff x^3 + ax + b = 0$.
Factor $x^3 + ax + b$ in $\mathbb{F}_q$:

- $x^3 + ax + b$ has no root in $\mathbb{F}_q$: $E(\mathbb{F}_q)[2] = \{\mathcal{O}\}$
- $(x - e_0)(x^2 + ux + v)$ over $\mathbb{F}_q$: $E(\mathbb{F}_q)[2] = \{(e_0, 0), \mathcal{O}\}$
- $(x - e_0)(x - e_1)(x - e_2)$ over $\mathbb{F}_q$: $E(\mathbb{F}_q)[2] = \{(e_0, 0), (e_1, 0), (e_2, 0), \mathcal{O}\}$

There exists an extension $\mathbb{F}_{q^i}$ such that $E(\mathbb{F}_{q^i})[2] = \{(x_0, 0), (x_1, 0), (x_2, 0), \mathcal{O}\}$

$$\ell \text{ coprime to } q,\ \#E[\ell] = \ell^2$$

ℓ-torsion points

Let ℓ coprime to q, the structure of the points of ℓ-torsion is

$$E[\ell] = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$$

a $\mathbb{Z}/\ell\mathbb{Z}$ two-dimensional vector space.
$\rightarrow$ there exists a basis $\{P, Q\}$, with P, Q of order ℓ and "independent".

Endomorphism ϕ with basis $\{P, Q\}$

$\phi(P) = [a]P + [c]Q$
$\phi(Q) = [b]P + [d]Q$

$$\phi \leftrightarrow \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ w.r.t. basis } \{P, Q\}$$

Gallant–Lambert–Vanstone (GLV)

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

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

$$\implies \phi(P) = [\lambda]P$$

where λ mod ℓ is the **eigenvalue** of ϕ.

Gallant–Lambert–Vanstone (GLV)

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

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

$$\implies \phi(P) = [\lambda]P$$

where λ mod ℓ is the **eigenvalue** of ϕ.

To speed-up $[m]P$, decompose $m = m_0 + m_1\lambda$ with $|m_0|, |m_1| \approx \sqrt{\ell}$ 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

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

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

Outline

Introduction: GLV on elliptic curves

Subgroup membership testing with GLV on $\mathbb{G}_1$

Faster co-factor clearing

Ensuring correct subgroup membership testing in $\mathbb{G}_2$ and $\mathbb{G}_T$

Bilinear pairing

$(\mathbf{G}_1, +), (\mathbf{G}_2, +), (\mathbf{G}_T, \cdot)$ three cyclic groups of large prime order ℓ
Pairing: map $e : \mathbf{G}_1 \times \mathbf{G}_2 \to \mathbf{G}_T$

1. bilinear: $e(P_1 + P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$, $e(P, Q_1 + Q_2) = e(P, Q_1) \cdot e(P, Q_2)$
2. non-degenerate: $e(G_1, G_2) \neq 1$ for $\langle G_1 \rangle = \mathbf{G}_1$, $\langle G_2 \rangle = \mathbf{G}_2$
3. efficiently computable.

Most often used in practice:

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

Focus on $\mathbf{G}_1$: Endomorphism on an elliptic curve

$$E\colon y^2 = x^3 + b/\mathbb{F}_q,\ \ q = 1 \bmod 3,\ \ j(E) = 0$$

$$\mathbf{G}_1 \subset E(\mathbb{F}_q) \text{ subgroup of prime order}$$

- $r = \#\mathbf{G}_1$ is prime
- $r \mid \#E(\mathbb{F}_q)$
- $r^2 \nmid \#E(\mathbb{F}_q)$

$\implies$ ϕ acts as $[\lambda]$ in $\mathbf{G}_1$, and $\lambda^2 + \lambda + 1 = 0 \bmod r$

Given $m \in \mathbb{Z}/r\mathbb{Z}$, decompose $m = m_0 + m_1\lambda \bmod r$ with $|m_0|, |m_1| \approx \sqrt{r}$

Focus on $\mathbf{G}_1$: Endomorphism on an elliptic curve

$$E\colon y^2 = x^3 + b/\mathbb{F}_q,\ \ q = 1 \bmod 3,\ \ j(E) = 0$$

$$\mathbf{G}_1 \subset E(\mathbb{F}_q) \text{ subgroup of prime order}$$

- $r = \#\mathbf{G}_1$ is prime
- $r \mid \#E(\mathbb{F}_q)$
- $r^2 \nmid \#E(\mathbb{F}_q)$

$\implies$ ϕ acts as $[\lambda]$ in $\mathbf{G}_1$, and $\lambda^2 + \lambda + 1 = 0 \bmod r$

Given $m \in \mathbb{Z}/r\mathbb{Z}$, decompose $m = m_0 + m_1\lambda \bmod r$ with $|m_0|, |m_1| \approx \sqrt{r}$

No computable endomorphism on most of standard curves (NIST, Edwards 25519...)

Exception: Four-$\mathbb{Q}$, characteristic 2 $\mathbb{F}_{2^n}$ (next talk)

BLS12

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

$$E_{BLS}: \; y^2 = x^3 + b, \; q \equiv 1 \bmod 3, \; D = -3 \text{ (ordinary)}$$

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

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

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

GLV trick: write $r_0 + r_1\lambda = 0 \bmod r$
with λ the eigenvalue of ϕ mod r.

$$\lambda = -u^2,\ 1 + (1-u^2)\lambda = r = u^4 - u^2 + 1$$

Compute $P + [1-u^2]\phi(P) = ?\mathcal{O}$
Works because ϕ is a distorsion map on the cofactor subgroup

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

but no $\iff$ in the general case unless r prime and $\gcd(r, \#E(\mathbb{F}_q)/r) = 1$.

Outline

Introduction: GLV on elliptic curves

Subgroup membership testing with GLV on $\mathbf{G}_1$

Faster co-factor clearing

Ensuring correct subgroup membership testing in $\mathbf{G}_2$ and $\mathbf{G}_T$

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 $[c]P$ where $c = \#E(\mathbb{F}_q)/\#\mathbf{G}_1$

Wahby–Boneh, CHES'2019: $c = 3\ell^2$ but no point of order ℓ^2, only points of order dividing ℓ

$$\implies \text{compute only } [\ell]P$$

Luck or generic pattern?

Schoof's theorem 3.7 (1987), simplified

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

$$E[\ell] \subset E(\mathbb{F}_q) \iff \begin{cases} \ell^2 \mid \#E(\mathbb{F}_q) \\ \ell \mid q-1 \\ \ell \mid y \text{ where } t^2 - 4q = -Dy^2 \end{cases}$$

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

For all curves in the Taxonomy paper of Freeman, Scott, Teske,

- 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

Introduction: GLV on elliptic curves

Subgroup membership testing with GLV on $\mathbf{G}_1$

Faster co-factor clearing

Ensuring correct subgroup membership testing in $\mathbf{G}_2$ and $\mathbf{G}_T$

$\mathbf{G}_2$ technicalities

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

$$X^2 - tX + q$$

where t is the trace of E over $\mathbb{F}_q$.
GLV on $\mathbf{G}_1 \rightarrow$ GLS (Galbraith Lin Scott) on $\mathbf{G}_2$
A point $Q \in E'(\mathbb{F}_{q^i})$ has some eigenvalue μ under ψ is a *consequence* of Q having order r

- flaw in Scott's proof identified
- and fixed
- corner cases under control

$\rightarrow$ all safe as long as r is prime

$\mathbf{G}_T$ membership testing

$$\mathbf{G}_T = \mu_r = \{z \in \mathbb{F}_{q^k}^*, z^r = 1\}$$

Proposition

- $E\colon y^2 = x^3 + ax + b/\mathbb{F}_q$
- prime $r \mid \#E(\mathbb{F}_q)$, $r^2 \nmid \#E(\mathbb{F}_q)$
- $E[r] \subset E(\mathbb{F}_{q^k})$ and k is minimal $\iff \mathbf{G}_T \subset \mathbb{F}_{q^k}^*$

Let $z \in \mathbb{F}_{q^k}^*$.

$$z^{\Phi_k(q)} = 1 \text{ and } z^q = z^{t-1} \text{ and } \gcd(q+1-t, \Phi_k(q)) = r \implies z^r = 1 \ (z \in \mathbf{G}_T)$$

Future work

- fix the problem of $m_0 + m_1\lambda = h \cdot r$ and h is not coprime to the cofactor
  hint of the fix in ePrint 2022/348
- alternative def of $\mathbf{G}_2$: trace-zero subgroup, $\ker \xi \circ (1 + \pi_q + \pi_{q^2} + \ldots + \pi_{q^{k-1}}) \circ \xi^{-1}$
  early abort test?
- Apply to other curves, e.g. BW6 for 2-chain SNARKs