Scalar decomposition on elliptic curves
GLV, GLS, and beyond

Benjamin Smith

Laboratoire d'Informatique de l'École polytechnique (LIX)
and **INRIA Saclay–Île-de-France**

BAC
May 24, 2013

Schnorr Signatures

For an example: consider the Schnorr signature scheme based on our finite cyclic group $\mathcal{G} = \langle P \rangle$ of order N.

We will need to fix a cryptographic hash function

$$H : \{0, 1\}^* \longrightarrow [0..N - 1]$$

(arbitrary length strings of bits $\longrightarrow$ values in $\mathbb{Z}/N\mathbb{Z}$)

Schnorr: Key Generation algorithm

System parameters $\mathcal{G} = \langle P \rangle$ of order N, hash $H : \{0,1\}^* \to \mathbb{Z}/N\mathbb{Z}$

Output A public/private-key pair $(Q, x) \in \mathcal{G} \times \mathbb{Z}/N\mathbb{Z}$;
Q is the public key, while x is the private key.

1 Set $x := \textbf{random}(\mathbb{Z}/N\mathbb{Z})$;

2 Set $Q := [x]P$;

3 Return (Q, x).

Schnorr: Sign algorithm

System parameters $\mathcal{G} = \langle P \rangle$ of order N, hash $H : \{0,1\}^* \to \mathbb{Z}/N\mathbb{Z}$

Input A message $m \in \{0,1\}^*$ and
a private key $x \in \mathbb{Z}/N\mathbb{Z}$.

Output A Schnorr signature $(s, e) \in (\mathbb{Z}/N\mathbb{Z})^2$.

1 Set $k := \mathbf{random}(\mathbb{Z}/N\mathbb{Z})$;

2 Set $R := [k]P$;

3 Set $e := H(m||R)$; *(Here || is concatenation of bitstrings)*

4 Let $s := k - xe \pmod{N}$;

5 Return (s, e).

Schnorr: Verify algorithm

System parameters $\mathcal{G} = \langle P \rangle$ of order N, hash $H : \{0,1\}^* \to \mathbb{Z}/N\mathbb{Z}$

Input A signature $(s, e) \in (\mathbb{Z}/N\mathbb{Z})^2$,
a message $m \in \{0,1\}^*$, and
a public key $Q \in \mathcal{G}$.

Output **True** if (s, e) is a valid Schnorr signature on the message m for the user with public key Q, otherwise **False**.

1 Let $R' := [s]P \oplus [e]Q$;

2 Let $e' := H(m||R')$;

3 **If** $e' = e$, **then**
  Return **True**;
else
  Return **False**.

Scalar multiplication

Scalar multiplication is fundamental in each part of the signature scheme.

We need to compute $[m]P$ for arbitrary $m \in [0, N-1]$ and P in $\mathcal{G}$
as fast as possible.

- Generally, $m \sim N$ (ie, $\log m = \log N$): really big!
- Measure algorithmic performance in terms of $\log_2 N$
  (since this governs the input and output size)
- Computing $[m]P$ by iterating the group law m times over?
  Exponentially slow!

Scalar multiplication: binary exponentiation

We can always compute $[m]P$ in $O(\log N)$ $\mathcal{G}$-operations.

Input m in $[0..N-1]$, P in $\mathcal{G}$

Output $[m]P$

1. Let $n := \lceil \log_2 N \rceil$;
2. Compute the binary representation $m = \sum_{i=0}^{n-1} m_i 2^i$ (with $m_i \in \{0,1\}$); *Note: normally this is for free*
3. Set $R := 0_{\mathcal{G}}$;
4. For i in $n-1$ down to 0,
   - 4a Set $R := [2]R$;
   - 4b Set $R := R \oplus [m_i]P$;
     Note: $[m_i]P = 0$ *or* P
5. Return R.

...$\log_2 m$ doublings, $\leq \log_2 m$ addings; worst/general case $\log m = \log N$

Scalar multiplication: multiexponentation

Here's something cute:
We can compute $[a]P \oplus [b]Q$ using only $\log_2 \max(|a|, |b|)$ doublings

Input a and b in $[0..N-1]$, P and Q in $\mathcal{G}$

Output $[a]P \oplus [b]Q$

1 Let $n = \lceil \log_2 \max(a, b) \rceil$;

2 Compute binary representations $a = \sum_{i=0}^{n-1} a_i 2^i$ and $b = \sum_{i=0}^{n-1} b_i 2^i$ (with $a_i, b_i \in \{0, 1\}$) *Normally: for free*

3 Set $R := 0_{\mathcal{G}}$;

4 For $i = n-1$ down to 0,

  4a Set $R := [2]R$;

  4b Set $R := R \oplus ([a_i]P \oplus [b_i]Q)$;
  Note: $[a_i]P \oplus [b_i]Q) = 0, P, Q,$ *or* $P \oplus Q$

5 Return R.

Abstract groups: the gold standard

...But in the "real" world, we don't have abstract groups: everything has some concrete representation.

The ideal $\mathcal{G}$ should *approximate* an abstract/black-box $\mathcal{G}$:

- Elements should take $\log_2 N$ bits to store
  ...so we don't waste memory or bandwidth
- Group operations should require a small-poly($\log_2 N$) bit operations
  ...so that the cryptosystem will work as fast as possible
- Discrete Logarithm Problems should require $O(\sqrt{N})$ $\mathcal{G}$-operations
  ...to be as secure as possible

From the abstract to the concrete

State of the art: $\mathcal{G} \subseteq \mathcal{E}(\mathbb{F}_q)$, $q = p, p^2,$ or 2^{prime}

- Elements? Only need to store the x-coordinate plus the "sign" of y.
  $\implies \log_q +1$ bits
  Almost perfect if $\mathcal{G}$ is most of $\mathcal{E}(\mathbb{F}_q)$
  - *ie,* $\#\mathcal{E}(\mathbb{F}_q) = Nh$, *with* h *tiny (eg.* $h = 1$*);*
  - want n-bit prime-order $\mathcal{G}$? Use an n-bit q
  - lots of choices of $\mathcal{E}/\mathbb{F}_q$ (compared to unique $\mathbb{F}_q^\times$)
- Group operations? low-degree polynomials over $\mathbb{F}_q$
  OK
- DLP?
  ? ...So far, generic curves: $O(\sqrt{N}) \implies (\frac{1}{2}\log_2 q)$-bit security

Geometry: Use It or Lose It

So: Elliptic curves are a source of concrete groups that perform essentially as well as black-box groups...

BUT

..there's nothing black-box about a smooth plane cubic

Problems:

Destructive Exploit the geometry to solve DLPs faster (reduce security)

Constructive Exploit the geometry to make cryptosystems more efficient

Let's be constructive

When we study an algebraic object, we always look at its endomorphisms (homomorphisms back into itself).

We work with $\mathcal{G} \cong \mathbb{Z}/N\mathbb{Z}$, embedded in $\mathcal{E}$.

$$\begin{aligned} &\mathrm{End}(\mathcal{G}) = \mathbb{Z}/N\mathbb{Z} \\ &\mathrm{End}(\mathcal{E}) \supseteq \mathbb{Z}[\pi], \quad \text{where } \pi : (x, y) \longmapsto (x^q, y^q) \text{ (Frobenius)} \end{aligned}$$

If $\psi \in \mathrm{End}_{\mathbb{F}_q}(\mathcal{E})$ restricts to an endomorphism of $\mathcal{G}$ (that is, $\psi(\mathcal{G}) \subseteq \mathcal{G}$) —and this happens pretty much all the time—then

$$\psi(P) = [\lambda_\psi]P \qquad \text{for all } P \in \mathcal{G}$$

We call λ_ψ the *eigenvalue* of ψ on $\mathcal{G}$. *Note:* $-N/2 < \lambda_\psi < N/2$.

Scalar multiplication with an endomorphism

Consider scalar multiplication: we want to compute $[m]P$.
Abstractly, we can do this with $\log_2 m$ doubles.

Suppose $\psi \in \mathrm{End}(\mathcal{E})$ has eigenvalue λ_ψ in $\mathbb{Z}/N\mathbb{Z}$.
If

$$m \equiv a + b\lambda_\psi \pmod{N},$$

then

$$[m]P = [a]P \oplus [b]\psi(P)$$

—and we can compute the RHS using multiexponentation.
Hence

- if ψ can be evaluated fast *(time/space $<$ few doubles)*, and
- if we can find a and b significantly shorter than m,

then we can compute $[m]P$ significantly faster.

Scalar multiplication with an endomorphism

Lemma

If $|\lambda_\psi| > N^{1/2}$, then we can find a and b such that

$$a + b\lambda_\psi \equiv m \pmod{N}$$

with

$$a \text{ and } b \text{ in } O(\sqrt{N}).$$

(Even better: can compute a and b easily)

Great! Now all we need is a source of good $\mathcal{E}$ equipped with fast ψ...
...and this turns out to be highly nontrivial.

Note: integer multiplications and Frobenius do not make good ψ.

GLV Curves (Gallant–Lambert–Vanstone, CRYPTO 2001)

Start with an explicit CM curve over $\overline{\mathbb{Q}}$ and reduce mod p.

Example (CM by $\sqrt{-1}$)

Let $p \equiv 1 \pmod 4$; let i be a square root of -1 in $\mathbb{F}_p$. Then the curves

$$\mathcal{E}_a : y^2 = x^3 + ax$$

have an explicit (and extremely efficient) endomorphism

$$\psi : (x, y) \longmapsto (-x, iy).$$

Good scalar decompositions: this $\lambda_\psi = \sqrt{-1}$. *Weak point: curve rarity.*

Limitations of GLV

The curves $\mathcal{E}_a/\mathbb{F}_p : y^2 = x^3 + ax$ look perfect...
...but we are not always free to choose our own prime p.

Example

The 256-bit prime $p = 2^{255} - 19$ offers very fast field arithmetic.
The $\mathbb{F}_p$-isomorphism classes of $\mathcal{E}_a/\mathbb{F}_p$ are represented by $a = 1, 2, 4, 8$.

$$\text{Largest prime factor of } \#\mathcal{E}_a(\mathbb{F}_p) = \begin{cases} 199 \text{ bits} & \text{if } a = 1 \\ 239 \text{ bits} & \text{if } a = 2 \\ 175 \text{ bits} & \text{if } a = 4 \\ 173 \text{ bits} & \text{if } a = 8 \end{cases}$$

So we pay for fast arithmetic with at least 17 (/256) bits of group order, which is about 9 (/128) bits of security.

Other GLV curves

We can try other explicit CM curves... But there are hardly any of them!

- ψ fast (generally) implies deg ϕ very small
- deg ϕ small, $\phi \notin \mathbb{Z} \implies \mathbb{Z}[\phi]$ has small discriminant Δ
- curves with CM by discriminant Δ have j-invariant classified by Hilbert polynomials H_Δ
- H_Δ has very small degree, typically 1 for tiny Δ
- $\implies$ only one j-invariant per Δ
- Only 2, 4, or 6 twists (curves) per j-invariant
- $\implies$ a handful of suitable curves, none of which might have (almost)-prime reduction mod p

Only 18 GLV curves with endomorphisms faster than doubling.
No guarantee *any* of them have good cryptographic group orders mod p.

GLS Curves (Galbraith–Lin–Scott, EUROCRYPT 2009)

Start with any curve over $\mathbb{F}_p$, extend to $\mathbb{F}_{p^2}$, and use p-th powering on the quadratic twist.

Example

Let $p \equiv 5 \pmod 8$, take A, B, in $\mathbb{F}_p$, take μ in $\mathbb{F}_{p^2}$ with μ nonsquare:

$$\mathcal{E}/\mathbb{F}_{p^2} : y^2 = x^3 + \mu^2 Ax + \mu^3 B$$

has an efficient endomorphism

$$\psi : (x, y) \longmapsto (-x^p, iy^p) \quad \text{where } i^2 = -1.$$

p-th powering in $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{D})$ almost free: $(a_0 + a_1\sqrt{D})^p = a_0 - a_q\sqrt{D}$

Good scalar decompositions: $\lambda_\psi = \sqrt{-1}$. *Weak point: twist insecurity.*

New endomorphisms

Example

Consider a general elliptic curve $\mathcal{E} : y^2 = x^3 + Ax + B$ over $\mathbb{F}_{p^2}$.
No obvious endomorphisms, apart from

- $[m]$ for $m \in \mathbb{Z}$ *(eigenvalue m, too slow for big m !)*
- Frobenius $\pi : (x, y) \to (x^{p^2}, y^{p^2})$ *(fixes $\mathbb{F}_{p^2}$-points: eigenvalue 1)*, and
- Linear combinations: too slow!

We would like to use the sub-Frobenius

$$\pi_0 : (x, y) \longmapsto (x^p, y^p),$$

but it's **not an endomorphism**: it is an **isogeny** mapping us onto the curve

$${}^{(p)}\mathcal{E} : y^2 = x^3 + A^p x + B^p$$

—which, over $\mathbb{F}_{p^2}$, coincides with the Galois conjugate of $\mathcal{E}$.

New endomorphisms

We've mapped onto the wrong curve! We need to get back to $\mathcal{E}$.

We have another p-powering isogeny ${}^{(p)}\pi_0 : {}^{(p)}\mathcal{E} \to \mathcal{E}$,
but the composition ${}^{(p)}\pi_0\pi_0$ is π (Frobenius), no use!

Idea: What if $\mathcal{E}$ was the reduction mod p of a **quadratic** $\mathbb{Q}$**-curve**?

That is, a curve $\widetilde{\mathcal{E}}/\mathbb{Q}(\sqrt{D})$ such that there is an isogeny $\widetilde{\phi} : \widetilde{\mathcal{E}} \to {}^{\sigma}\widetilde{\mathcal{E}}$?

Then $\widetilde{\phi}$ would reduce to an isogeny $\phi : \mathcal{E} \to {}^{(p)}\mathcal{E}$, and
the composition ${}^{(p)}\pi_0\phi$ would be a new endomorphism.

New endomorphisms

Example

Consider the universal quadratic $\mathbb{Q}$-curve of degree 2 (Hasegawa):

Let D be any squarefree discriminant, $t \in \mathbb{Q}$ a free parameter, and

$$\widetilde{\mathcal{E}}/\mathbb{Q}(\sqrt{D}) : y^2 = (x-4)(x^2 + 4x + 18\sqrt{D}t - 14)$$
$${}^{\sigma}\widetilde{\mathcal{E}}/\mathbb{Q}(\sqrt{D}) : y^2 = (x-4)(x^2 + 4x - 18\sqrt{D}t - 14)$$

There exists a 2-isogeny $\widetilde{\phi} : \widetilde{\mathcal{E}} \to {}^{\sigma}\widetilde{\mathcal{E}}$, defined by

$$\widetilde{\phi} : (x, y) \longmapsto \left(f(x), \frac{y}{\sqrt{-2}} f'(x) \right) \text{ where } f(x) = \frac{x^2 - 4x + 18\sqrt{D}t + 18}{-2(x-4)}$$

New endomorphisms (S., 2013)

Example

For any $p > 3$ and any $t \in \mathbb{F}_p$, the curve

$$\mathcal{E}_t/\mathbb{F}_{p^2} : y^2 = (x-4)(x^2 + 4x + 18\sqrt{D}t - 14)$$

has a *fast* endomorphism ψ defined by

$$\psi : (x, y) \longmapsto \left(\frac{-f(x^p)}{2}, \frac{y^p f'(x^p)}{2\sqrt{-2}} \right) \text{ where } f(x^p) = x^p + \frac{18(1 + t\sqrt{D})}{(x^p - 4)}$$

For example: $p = 2^{127} - 1$, $D = -1$, $s = 1229\ldots107$;
Get $\#\mathcal{E}_{2,s}(\mathbb{F}_p(\sqrt{D})) = 2 \cdot (\text{255-bit prime})$ *twist secure!*

So, what was the point again?

Use the geometry of the curve for faster ECC.

The critical operation is scalar multiplication.

With fast endomorphisms on elliptic curves:
scalar multiplication becomes half-length multiexponentiation.