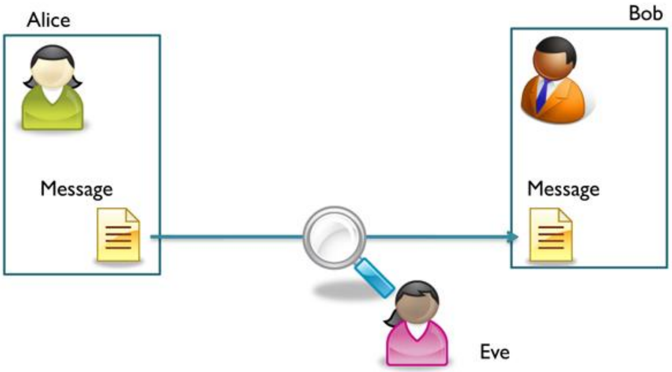
Cryptographie à base de courbes elliptiques : algorithmes et implémentation

Sorina Ionica

IMB, Université de Bordeaux



Sharing a common secret over an insecure channel

Public key cryptography and groups

- Diffie-Hellman Key Exchange : $(G, +, P)$ public

$$\begin{array}{ccc} \text{Alice} & \xrightarrow{P_A} & \text{Bob} \\ a, P_A = aP & \xleftarrow[P_B]{} & b, P_B = bP \\ K = aP_B & & K = bP_B \\ & K = abP & \end{array}$$

Security: the Discrete Logarithm Problem (DLP) in G

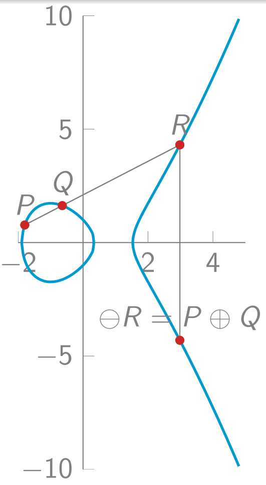
- Given $P, Q \in G$ find (if it exists) λ such that

$$Q = \lambda P$$

Consider $\mathbb{F}_q$, $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$

Weierstrass form

$$y^2 = x^3 + ax + b$$



- Secure implementation : DLP is hard if $r = \#G$ is a large prime number.
- Shorter keys (compared to RSA, group cryptography over finite fields)

Security

Table : Complexity of generic attacks

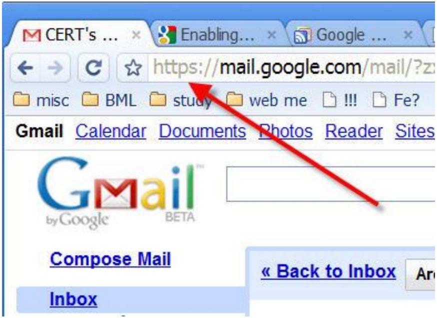
method	Fastest known attack
RSA	Number Field Sieve $exp(\frac{1}{2}(logN)^{\frac{1}{3}}(log \log N)^{\frac{2}{3}})$
ECC	Pollard-rho $\sqrt{r} = exp(\frac{1}{2}\log r)$

Table : Key sizes

Security level	RSA	ECC
80 bits	1024	160
128 bits	3072	256
256 bits	15360	512

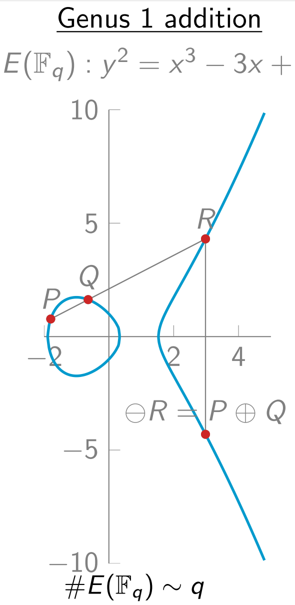
ECC in the real world

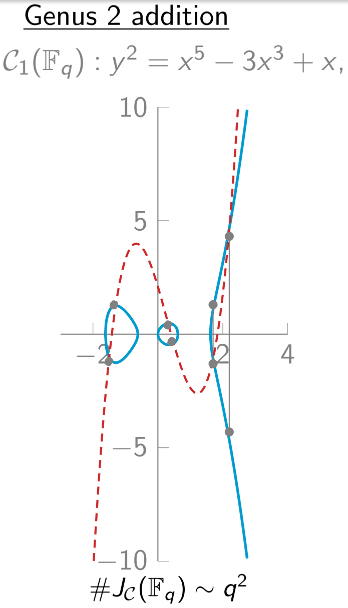
key exchange, signatures, identification



bitcoin

Elliptic versus genus 2 curves





Scalar multiplication

- multiplication-by-m map: $P \mapsto [m]P$ on $E(\mathbb{F}_q)$,
  $\mathcal{D} \mapsto [m]\mathcal{D}$ on $J_{\mathcal{C}}(\mathbb{F}_q)$
- optimized binary double-and-add scalar multiplication:

---

1. write m in binary rep. $m = \sum_{i=0}^{\log m-1} m_i 2^i$, $m_i \in \{0,1\}$
2. $R \leftarrow P$
3. for i from $\log m - 1$ to 0 do
    1. $R \leftarrow 2R$ (Doubling)
    2. if $m_i = 1$ then $R \leftarrow R + P$ (Addition)
4. return R

- cost: $\log m$ doublings $+ \sim \frac{1}{2} \log m$ additions in average

Multi-scalar multiplication

$$[m]P + [\ell]Q \in \mathbf{G} \subset E(\mathbb{F}_q)$$

---

1. write $m \leqslant \ell$ in binary rep. $m = \sum_{i=0}^{\log m - 1} m_i 2^i$, $\ell = \sum_{i=0}^{\log \ell - 1} \ell_i 2^i$, $m_i, \ell_i \in \{0, 1\}$
2. precompute $T = P + Q$
3. if $\log \ell > \log m$ then $R \leftarrow Q$
4. else $R \leftarrow T$
5. for i from $\log \ell - 1$ to 0 do
    1. $R \leftarrow 2R$ (Doubling)
    2. if $m_i = \ell_i = 1$ then $R \leftarrow R + T$ (Addition)
    3. else if $m_i = 1$ and $\ell_i = 0$ then $R \leftarrow R + P$ (Addition)
    4. else if $m_i = 0$ and $\ell_i = 1$ then $R \leftarrow R + Q$ (Addition)
6. return R

- cost: $\log \ell$ doublings $+ \sim \frac{3}{4} \log \ell$ additions in average

Algorithme GLV pour la multiplication scalaire

Assume there is an efficient (almost free) endomorphism

$$\phi : G \to G, \quad \phi(P) = \lambda_\phi P$$

λ_ϕ is large $\to$ decompose $m = m_0 + \lambda_\phi m_1 \bmod r$ with $\log m_0 \sim \log m_1 \sim \log m/2$

Multi-exponentiation

Compute $mP = m_0 P + m_1 \phi(P)$ in $(\log m)/2$ operations.

Save half doublings for a cost of a quarter of additions.

Endomorphisms: an example

$$E_\alpha(\mathbb{F}_q) : y^2 = x^3 + \alpha x, \quad j(E_\alpha) = 1728 \ (i.e. \text{ CM by } \sqrt{-1}, \ D = 4)$$

- $q \equiv 1 \bmod 4$,
- let $i \in \mathbb{F}_q$ s.t. $i^2 = -1 \in \mathbb{F}_q$
- $\phi : (x, y) \mapsto (-x, iy)$ is an endomorphism
- $\phi \circ \phi(x, y) = (x, -y)$
- $\phi^2 + \mathrm{Id} = 0$ on $E(\mathbb{F}_q)$
- eigenvalue: $\lambda_\phi \equiv \sqrt{-1} \bmod \#E(\mathbb{F}_q)$
- this means for P of prime-order r, $\phi(P) = [\lambda_\phi \bmod r]P$

Endomorphism: Frobenius map

- Frobenius map, $E(\mathbb{F}_q)$, $(x,y) \in E(\mathbb{F}_{q^n}) \mapsto (x^q, y^q) \in E(\mathbb{F}_{q^n})$. Why ?
  - $E(\mathbb{F}_q) : y^2 = x^3 + a_4 x + a_6,\ a_4, a_6 \in \mathbb{F}_q$
  - Not directly useful in this way. Used with twisted curves (Galbraith-Lin-Scott GLS curves)
- $j(E) = 1728, 8000, -3375 \longleftrightarrow \phi = \sqrt{-1}, \sqrt{-2}, \frac{1+\sqrt{-7}}{2}$.
- $j(E) = 0, 54000, -32768 \longleftrightarrow \phi = \frac{-1+\sqrt{-3}}{2}, \sqrt{-3}, \frac{1+\sqrt{-11}}{2}$.
- Galbraith-Lin-Scott (GLS) curves (2009): defined over $\mathbb{F}_{q^2}$ instead of $\mathbb{F}_q$, $j \in \mathbb{F}_q$, one endomorphism $\phi : \phi^2 = -\mathrm{Id}$ on $E(\mathbb{F}_{q^2})$.
  - but still $j \in \mathbb{F}_q$
- These are all available *fast* endomorphisms.

Implementation

Fast algorithms for scalar multiplication: GLV

Fast group law computation

Fast modular arithmetic : special primes (ex. $p = 2^{127} - 1$)

Example: No curve $E/\mathbb{F}_{q^2}$ with $p = 2^{127} - 1$ and GLV of dimension 4.

Challenge: the fastest implementation for a given security level

Four dimensional GLV via the Weil restriction

joint work with Aurore Guillevic

GLV friendly curve zoo

Genus 1

- GLV 2001 : complex multiplication by $\sqrt{-1}, \sqrt{-2}, \frac{1+\sqrt{-7}}{2}, \sqrt{-3}, \frac{1+\sqrt{-11}}{2}$.
- Galbraith-Lin-Scott 2009: curves$/\mathbb{F}_{q^2}$, $j \in \mathbb{F}_q$.
- Longa-Sica 2012: 4-dim GLV+GLS

Genus 2

- Mestre, Kohel-Smith, Takashima : explicit real multiplication by $\sqrt{2}$, $\sqrt{5}$
- 4-dim. : Buhler-Koblitz, Furukawa-Takahashi curves

GLV friendly curve zoo

Genus 1

- GLV 2001 : complex multiplication by $\sqrt{-1}$, $\sqrt{-2}$, $\frac{1+\sqrt{-7}}{2}$, $\sqrt{-3}$, $\frac{1+\sqrt{-11}}{2}$.
- Galbraith-Lin-Scott 2009: curves$/\mathbb{F}_{q^2}$, $j \in \mathbb{F}_q$.
- Longa-Sica 2012: 4-dim GLV+GLS

Genus 2

- Mestre, Kohel-Smith, Takashima : explicit real multiplication by $\sqrt{2}$, $\sqrt{5}$
- 4-dim. : Buhler-Koblitz, Furukawa-Takahashi curves
- This work: 4-dim.-GLV on Satoh/Satoh-Freeman curves 2009

GLV friendly curve zoo

Genus 1

- GLV 2001 : complex multiplication by $\sqrt{-1}, \sqrt{-2}, \frac{1+\sqrt{-7}}{2}$, $\sqrt{-3}, \frac{1+\sqrt{-11}}{2}$.
- Galbraith-Lin-Scott 2009: curves$/\mathbb{F}_{q^2}$, $j \in \mathbb{F}_q$.
- Longa-Sica 2012: 4-dim GLV+GLS
- This work: 4 dim.-GLV on two families of curves$/\mathbb{F}_{q^2}$, but $j \in \mathbb{F}_{q^2}$.

Genus 2

- Mestre, Kohel-Smith, Takashima : explicit real multiplication by $\sqrt{2}$, $\sqrt{5}$
- 4-dim. : Buhler-Koblitz, Furukawa-Takahashi curves
- This work: 4-dim.-GLV on Satoh/Satoh-Freeman curves 2009

4-GLV, ..., 2^i-GLV: time-memory trade-off

- We would like a 4-dimensional decomposition of m when computing mP
- 2 endomophisms ϕ, ψ of eigenvalues $\lambda_\phi, \lambda_\psi$
- decompose $m \equiv m_1 + m_2\lambda_\phi + m_3\lambda_\psi + m_4\lambda_\phi\lambda_\psi \bmod r$ with $\log m_i \sim \frac{1}{4}\log m$
- Store $P, \phi(P), \psi(P), \phi\psi(P), \ldots \Rightarrow$ 16 points
- 4-dim. multiexponentiation $\rightarrow$ Save $\frac{3}{4}\log m$ doublings and $\sim \frac{17}{32}\log m$ additions.

Dimension 4 - Longa and Sica 2012

- Curves are ordinary, i.e. endomorphisms form a lattice of dimension 2 $\Rightarrow [1, \phi]$
- we need ψ s.t. $\lambda_\psi \equiv \alpha + \beta\lambda_\phi \bmod r$ and $\alpha, \beta > r^{1/4}$ to have a decomposition

How to construct ψ efficiently computable?

Longa-Sica curves (2012)

Consider GLS curves with small $D \rightarrow 2$ endomorphisms $\psi: \ \psi^2 + 1 = 0$, $\phi: \ \phi^2 + D = 0$ for points over $\mathbb{F}_{q^2}$.

Satoh's curves

$$
\begin{tikzcd}
J_{\mathcal{C}_1}(\mathbb{F}_{q^8}) \arrow[r, bend left, "\mathcal{I}"] & E_c \times E_c(\mathbb{F}_{q^8}) \arrow[l, bend left, "\hat{\mathcal{I}}"] \\
 & E_c \times E_c(\mathbb{F}_{q^2}) \arrow[u] \\
J_{\mathcal{C}_1}(\mathbb{F}_q) \arrow[uu] &
\end{tikzcd}
$$

$$\mathcal{C}_1\colon\ y^2 = x^5 + ax^3 + bx,\ a, b \in \mathbb{F}_q$$

$J_{\mathcal{C}_1}$ is the Weil restriction of

$$E_c/\mathbb{F}_{q^2} : y^2 = x^3 + 27(3c - 10)x + 108(14 - 9c), \quad c = a/\sqrt{b}$$

$$\begin{tikzcd}
J_{\mathcal{C}_1}(\mathbb{F}_{q^8}) \arrow[r, bend left, "\mathcal{I}"] & E_c \times E_c(\mathbb{F}_{q^8}) \arrow[l, bend left, "\hat{\mathcal{I}}"] \\
 & E_c \times E_c(\mathbb{F}_{q^2}) \arrow[u] \\
J_{\mathcal{C}_1}(\mathbb{F}_q) \arrow[uu] &
\end{tikzcd}$$

$$D = 2D' \qquad \longrightarrow \qquad E_c \overset{\mathcal{I}_2}{\dashrightarrow} ?$$

We start by computing a degree 2 isogeny (i.e. a map between curves) $\mathcal{I}_2$ from E_c.

4-dim GLV on elliptic curves

We computed with Vélu's formulas this 2-isogeny

$$\begin{array}{rcl} \mathcal{I}_2 : E_c & \rightarrow & E_{-c} \\ (x,y) & \mapsto & \left(\frac{-x}{2} + \frac{162+81c}{-2(x-12)}, \frac{-y}{2\sqrt{-2}} \left(1 - \frac{162+81c}{(x-12)^2} \right) \right) \end{array}$$

$$\begin{tikzcd} E_c \arrow[rr, bend left, "\mathcal{I}_2"] & & E_{-c} \end{tikzcd}$$

- $E_c/\mathbb{F}_{q^2} : y^2 = x^3 + 27(3c-10)x + 108(14-9c)$
- $E_{-c}/\mathbb{F}_{q^2} : y^2 = x^3 + 27(-3c-10)x + 108(14+9c)$

4-dim GLV on elliptic curves

We computed with Vélu's formulas this 2-isogeny

$$\begin{array}{rcl} \mathcal{I}_2 : E_c & \rightarrow & E_{-c} \\ (x,y) & \mapsto & \left(\frac{-x}{2} + \frac{162+81c}{-2(x-12)}, \frac{-y}{2\sqrt{-2}}\left(1 - \frac{162+81c}{(x-12)^2}\right)\right) \end{array}$$

$$\begin{tikzcd} E_c \arrow[r, bend left, "\mathcal{I}_2"] & E_{-c} \end{tikzcd}$$

- $E_c/\mathbb{F}_{q^2} : y^2 = x^3 + 27(3c-10)x + 108(14-9c)$
- $E_{-c}/\mathbb{F}_{q^2} : y^2 = x^3 + 27(-3c-10)x + 108(14+9c)$
- In $\mathbb{F}_{q^2}$, $\pi_q(c) = -c$
- Go back from E_{-c} to E_c with the Frobenius map

We computed with Vélu's formulas this 2-isogeny

$$
\begin{array}{rcl}
\mathcal{I}_2 : E_c & \to & E_{-c} \\
(x,y) & \mapsto & \left(\frac{-x}{2} + \frac{162+81c}{-2(x-12)}, \frac{-y}{2\sqrt{-2}} \left(1 - \frac{162+81c}{(x-12)^2}\right)\right)
\end{array}
$$

$$
\begin{array}{l}
\pi_q \circ \mathcal{I}_2 \\
= \phi_2 \\
\equiv [\sqrt{\pm 2}]
\end{array}
\quad
\begin{tikzcd}
E_c \arrow[loop left] \arrow[rr, bend left, "\mathcal{I}_2"] & & E_{-c} \arrow[ll, "\pi_q"]
\end{tikzcd}
$$

- $E_c/\mathbb{F}_{q^2} : y^2 = x^3 + 27(3c-10)x + 108(14-9c)$
- $E_{-c}/\mathbb{F}_{q^2} : y^2 = x^3 + 27(-3c-10)x + 108(14+9c)$
- In $\mathbb{F}_{q^2}$, $\pi_q(c) = -c$
- Go back from E_{-c} to E_c with the Frobenius map

4-dim GLV on elliptic curves

We computed with Vélu's formulas this 2-isogeny

$$\begin{array}{rcl} \mathcal{I}_2 : E_c & \to & E_{-c} \\ (x, y) & \mapsto & \left(\frac{-x}{2} + \frac{162+81c}{-2(x-12)}, \frac{-y}{2\sqrt{-2}} \left(1 - \frac{162+81c}{(x-12)^2} \right) \right) \end{array}$$

$$\begin{tikzcd} E_c \arrow[loop left, "{\pi_q \circ \mathcal{I}_2 = \phi_2 \equiv [\sqrt{\pm 2}]}"] \arrow[rr, bend left, "\mathcal{I}_2"] & & E_{-c} \arrow[ll, "\pi_q"] \end{tikzcd}$$

- $E_c/\mathbb{F}_{q^2} : y^2 = x^3 + 27(3c - 10)x + 108(14 - 9c)$
- $E_{-c}/\mathbb{F}_{q^2} : y^2 = x^3 + 27(-3c - 10)x + 108(14 + 9c)$
- In $\mathbb{F}_{q^2}$, $\pi_q(c) = -c$
- Go back from E_{-c} to E_c with the Frobenius map
- ϕ_2 is different from the CM

4-dim GLV on elliptic curves

We computed with Vélu's formulas this 2-isogeny

$$
\begin{array}{rcl}
\mathcal{I}_2 : E_c & \to & E_{-c} \\
(x,y) & \mapsto & \left(\frac{-x}{2} + \frac{162+81c}{-2(x-12)}, \frac{-y}{2\sqrt{-2}} \left(1 - \frac{162+81c}{(x-12)^2}\right)\right)
\end{array}
$$

$$
\begin{array}{l}
\pi_q \circ \mathcal{I}_2 \\
= \phi_2 \\
\equiv [\sqrt{\pm 2}]
\end{array}
\quad
\begin{tikzcd}
E_c \arrow[loop left] \arrow[rr, bend left, "\mathcal{I}_2"] \arrow[rr, dashed, bend right, "\mathcal{I}_{D'}"'] & & E_{-c} \arrow[ll, "\pi_q"']
\end{tikzcd}
$$

- $E_c/\mathbb{F}_{q^2} : y^2 = x^3 + 27(3c-10)x + 108(14-9c)$
- $E_{-c}/\mathbb{F}_{q^2} : y^2 = x^3 + 27(-3c-10)x + 108(14+9c)$
- In $\mathbb{F}_{q^2}$, $\pi_q(c) = -c$
- Go back from E_{-c} to E_c with the Frobenius map
- ϕ_2 is different from the CM
- We can construct a second endomorphism from CM.

Efficient 4-dim. GLV on E_c

$$\pi_q \circ \mathcal{I}_2 = \phi_2 \equiv [\sqrt{\pm 2}]$$
$$\pi_q \circ \mathcal{I}_{D'} = \phi_{D'} \equiv [\sqrt{\mp D'}]$$

$$\begin{tikzcd}
E_c(\mathbb{F}_{q^2}) \arrow[loop left] \arrow[rr, bend left, "\mathcal{I}_2"] \arrow[rr, bend right, "\mathcal{I}_{D'}"'] & & E_{-c}(\mathbb{F}_{q^2}) \arrow[ll, "\pi_q"']
\end{tikzcd}$$

- second isogeny $\mathcal{I}_{D'}$ computed with Velu's formulas
- 4-dimensional decomposition using proper values of $1, \phi_2$, $\phi_{D'}$, $\phi_2 \circ \phi_{D'}$.
- $\phi_2^2 \pm 2 = 0$, $\phi_{D'}^2 \mp D' = 0$ for points defined over $\mathbb{F}_{q^2}$.

Example with $D = 40$

- $D = 40 = 4 \cdot (2 \cdot 5)$
- $\#E_c(\mathbb{F}_{q^2})$ of the form $(-2n^2 - 20m^2 + 4)/4$, $4 \mid \#E_c(\mathbb{F}_{q^2})$
- search for m, n s.t. q is prime and $\#E_c(\mathbb{F}_{q^2})$ is almost prime.

$$
\begin{aligned}
n &= \text{0x55d23edfa6a1f7e4} \\
m &= \text{0x549906b3eca27851} \\
t &= \text{- 0xfaca844b264dfaa353355300f9ce9d3a} \\
q &= \text{0x9a2a8c914e2d05c3f2616cade9b911ad} \\
r &= \text{0x1735ce0c4fbac46c2245c3ce9d8da0244f9059ae9ae4784d6b2f65b29c444309} \\
c^2 &= \text{0x40b634aec52905949ea0fe36099cb21a}
\end{aligned}
$$

with q, r prime and $\#E_c(\mathbb{F}_{q^2}) = 4r$.

Operation count at the 128 bit security level

Curve	Method	Operation count	Global estim.
E_c	4-GLV, 16 pts.	$2748m+1668s$	$4416m$
$D=4$ [LongaSica12]	4-GLV, 16 pts.	$1992m+2412s$	$4404m$
E_c	2-GLV, 4 pts.	$4704m+2976s$	$7680m$
$J_{\mathcal{C}_1}$	4-GLV, 16 pts.	$4500m+\ 816s$	$5316m$
$J_{\mathcal{C}_1}$	2-GLV, 4 pts.	$7968m+1536s$	$9504m$
FKT [Bos et al. 13]	4-GLV, 16 pts.	$4500m+\ 816s$	$5316m$
Kummer [Bos et al. 13]	–	$3328m+2048s$	$5376m$

Table : Benchmarks for scalar multiplication at 128 security level

Curve	Method	Timing in ms.
$E_{1,c}$ this work	4-GLV, 16 pts.	0.002202
E_1 Longa-Sica	4-GLV, 16 pts.	0.001882
$E_{1,c}$ GLV	2-GLV, 4pts.	0.004070
$J_{\mathcal{C}_1}$ this work	4-GLV, 4 pts.	0.001831