Cryptographie à base de courbes elliptiques : algorithmes et implémentation

Sorina Ionica

IMB, Université de Bordeaux
Public key cryptography

Sharing a common secret over an insecure channel
Public key cryptography and groups

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

\[
\begin{align*}
&\text{Alice} \quad P_A \quad \text{Bob} \\
&a, P_A = aP \quad b, P_B = bP \\
&K = aP_B \quad K = bP_B \\
&K = abP
\end{align*}
\]

Security: the Discrete Logarithm Problem (DLP) in \(G\)

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

\[
Q = \lambda P
\]
Elliptic Curve Cryptography

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

**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)
### Table: Complexity of generic attacks

<table>
<thead>
<tr>
<th>method</th>
<th>Fastest known attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>Number Field Sieve $\exp\left(\frac{1}{2}(\log N)^{\frac{1}{3}}(\log \log N)^{\frac{2}{3}}\right)$</td>
</tr>
<tr>
<td>ECC</td>
<td>Pollard-rho $\sqrt{r} = \exp\left(\frac{1}{2} \log r\right)$</td>
</tr>
</tbody>
</table>

### Table: Key sizes

<table>
<thead>
<tr>
<th>Security level</th>
<th>RSA</th>
<th>ECC</th>
</tr>
</thead>
<tbody>
<tr>
<td>80 bits</td>
<td>1024</td>
<td>160</td>
</tr>
<tr>
<td>128 bits</td>
<td>3072</td>
<td>256</td>
</tr>
<tr>
<td>256 bits</td>
<td>15360</td>
<td>512</td>
</tr>
</tbody>
</table>
ECC in the real world

key exchange, signatures, identification
Elliptic versus genus 2 curves

Genus 1 addition

\[ E(\mathbb{F}_q) : y^2 = x^3 - 3x + 1 \]

\[ \oplus R = P \oplus Q \]

\[ \#E(\mathbb{F}_q) \sim q \]

Genus 2 addition

\[ C_1(\mathbb{F}_q) : y^2 = x^5 - 3x^3 + x, \]

\[ \#J_C(\mathbb{F}_q) \sim q^2 \]
Scalar multiplication

- multiplication-by-$m$ map: $P \mapsto [m]P$ on $E(\mathbb{F}_q)$,
  $\mathcal{D} \mapsto [m]\mathcal{D}$ on $J_C(\mathbb{F}_q)$

- optimized binary double-and-add scalar multiplication:

1. write $m$ in binary rep. $m = \sum_{i=0}^{\log m - 1} m_i2^i$, $m_i \in \{0, 1\}$
2. $R \leftarrow P$
3. for $i$ from $\log m - 1$ to 0 do
   1. $R \leftarrow 2R$  \hspace{1cm} (Doubling)
   2. if $m_i = 1$ then $R \leftarrow R + P$  \hspace{1cm} (Addition)
4. return $R$

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

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

1. write \( m \leq \ell \) 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. \( R \leftarrow 2R \)
   2. if \( m_i = \ell_i = 1 \) then \( R \leftarrow R + T \)
   3. else if \( m_i = 1 \) and \( \ell_i = 0 \) then \( R \leftarrow R + P \)
   4. else if \( m_i = 0 \) and \( \ell_i = 1 \) then \( R \leftarrow R + Q \)
6. return \( R \)

- cost: \( \log \ell \) doublings + \( \sim \frac{3}{4} \log \ell \) additions in average
Assume there is an efficient (almost free) endomorphism

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

\(\lambda_\phi\) is large \(\to\) decompose \(m = m_0 + \lambda_\phi m_1 \mod r\) 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

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

- \[ q \equiv 1 \text{ mod } 4, \]
- let \[ i \in \mathbb{F}_q \text{ s.t. } i^2 = -1 \in \mathbb{F}_q \]
- \[ \phi : (x, y) \mapsto (-x, iy) \text{ is an endomorphism} \]
- \[ \phi \circ \phi(x, y) = (x, -y) \]
- \[ \phi^2 + \text{Id} = 0 \text{ on } E(\mathbb{F}_q) \]
- eigenvalue: \[ \lambda_\phi \equiv \sqrt{-1} \text{ mod } \#E(\mathbb{F}_q) \]
- this means for \( P \) of prime-order \( r \), \[ \phi(P) = [\lambda_\phi \mod r]P \]
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?
  - $E(\mathbb{F}_q)$: $y^2 = x^3 + a_4x + a_6$, $a_4, a_6 \in \mathbb{F}_q$
  - Not directly useful in this way. Used with twisted curves (Galbraith-Lin-Scott GLS curves)

- $j(E) = 1728, 8000, -3375 \leftrightarrow \phi = \sqrt{-1}, \sqrt{-2}, \frac{1+\sqrt{-7}}{2}$.
- $j(E) = 0, 54000, -32768 \leftrightarrow \phi = \frac{-1+\sqrt{-3}}{2}, \sqrt{-3}, \frac{1+\sqrt{-11}}{2}$.

Galbraith-Lin-Scott (GLS) curves (2009): defined over $\mathbb{F}_{q^2}$ instead of $\mathbb{F}_q$, $j \in \mathbb{F}_q$, one endomorphism $\phi: \phi^2 = -\text{Id}$ 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 modular arithmetic: special primes (ex. $p = 2^{127} - 1$)

Fast group law computation

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
Our contribution

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 over \( \mathbb{F}_{q^2} \), \( j \in \mathbb{F}_q \).
- 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 two families of curves over \( \mathbb{F}_{q^2} \), but \( j \in \mathbb{F}_q \).
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 over \(\mathbb{F}_{q^2}\), \(j \in \mathbb{F}_q\).
- 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
**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.
We would like a 4-dimensional decomposition of \( m \) when computing \( mP \)

- 2 endomorphisms \( \phi, \psi \) of eigenvalues \( \lambda_\phi, \lambda_\psi \)
- decompose \( m \equiv m_1 + m_2 \lambda_\phi + m_3 \lambda_\psi + m_4 \lambda_\phi \lambda_\psi \mod r \) 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 → Save \( \frac{3}{4} \log m \) doublings and \( \sim \frac{17}{32} \log m \) additions.
Curves are ordinary, i.e. endomorphisms form a lattice of dimension 2 $\Rightarrow [1, \phi]$

we need $\psi$ s.t. $\lambda_\psi \equiv \alpha + \beta \lambda_\phi \mod r$ and $\alpha, \beta > r^{1/4}$ to have a decomposition

How to construct $\psi$ efficiently computable?

**Longa-Sica curves (2012)**

Consider GLS curves with small $D \to 2$ endomorphisms

$\psi : \psi^2 + 1 = 0, \phi : \phi^2 + D = 0$ for points over $\mathbb{F}_{q^2}$. 
Satoh’s curves

\[ J_{C_1}(\mathbb{F}_{q^8}) \] \xrightarrow{\mathcal{I}} \ E_c \times E_c(\mathbb{F}_{q^8}) \]

\[ \hat{\mathcal{I}} \]

\[ J_{C_1}(\mathbb{F}_q) \]

\[ E_c \times E_c(\mathbb{F}_{q^2}) \]

\[ C_1: y^2 = x^5 + ax^3 + bx, \ a, b \in \mathbb{F}_q \]

\[ J_{C_1} \text{ is the Weil restriction of } \]

\[ E_c/\mathbb{F}_{q^2}: y^2 = x^3 + 27(3c - 10)x + 108(14 - 9c), \ c = a/\sqrt{b} \]
We start by computing a degree 2 isogeny (i.e. a map between curves) $\mathcal{I}_2$ from $E_c$. 

$D = 2D'$
We computed with Vélu’s formulas this 2-isogeny

\[ \mathcal{I}_2 : E_c \rightarrow E_{-c} \]

\[ (x, y) \mapsto \left( \frac{-x}{2} + \frac{162+81c}{-2(x-12)}, \frac{-y}{2\sqrt{-2}} \left( 1 - \frac{162+81c}{(x-12)^2} \right) \right) \]

\[ E_c \xrightarrow{\mathcal{I}_2} E_{-c} \]

- \( E_c / \mathbb{F}_{q^2} : y^2 = x^3 + 27(3c - 10)x + 108(14 - 9c) \)
- \( E_{-c} / \mathbb{F}_{q^2} : y^2 = x^3 + 27(-3c - 10)x + 108(14 + 9c) \)
We computed with Vélu’s formulas this 2-isogeny

\[ \mathcal{I}_2 : E_c \rightarrow E_{-c} \]

\[
(x, y) \mapsto \left( \frac{-x}{2} + \frac{162+81c}{-2(x-12)}, \frac{-y}{2\sqrt{-2}} \left( 1 - \frac{162+81c}{(x-12)^2} \right) \right)
\]

- \( E_c / \mathbb{F}_{q^2} : y^2 = x^3 + 27(3c - 10)x + 108(14 - 9c) \)
- \( E_{-c} / \mathbb{F}_{q^2} : y^2 = x^3 + 27(-3c - 10)x + 108(14 + 9c) \)
- \( \pi_{q^2}(c) = -c \)
- Go back from \( E_{-c} \) to \( E_c \) with the Frobenius map
We computed with Vélu’s formulas this 2-isogeny

\[\mathcal{I}_2 : E_c \rightarrow E_{-c}\]

\[(x, y) \mapsto \left(\frac{-x}{2} + \frac{162+81c}{-2(x-12)}, \frac{-y}{2\sqrt{-2}} \left(1 - \frac{162+81c}{(x-12)^2}\right)\right)\]

\[\pi_q \circ \mathcal{I}_2 = \phi_2 \equiv [\sqrt{\pm 2}]\]

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

\[ \mathcal{I}_2 : E_c \rightarrow E_{-c} \]
\[ (x, y) \mapsto \left( \frac{-x}{2} + \frac{162 + 81c}{-2(x-12)}, \frac{-y}{2\sqrt{-2}} \left( 1 - \frac{162 + 81c}{(x-12)^2} \right) \right) \]

\[ \pi_q \circ \mathcal{I}_2 = \phi_2 \equiv [\sqrt{\pm 2}] \]

- \( E_c / \mathbb{F}_{q^2} : y^2 = x^3 + 27(3c - 10)x + 108(14 - 9c) \)
- \( E_{-c} / \mathbb{F}_{q^2} : y^2 = x^3 + 27(-3c - 10)x + 108(14 + 9c) \)
- In \( \mathbb{F}_{q^2} \), \( \pi_q(c) = -c \)
- Go back from \( E_{-c} \) to \( E_c \) with the Frobenius map
- \( \phi_2 \) is different from the CM
We computed with Vélu’s formulas this 2-isogeny

\[ \mathcal{I}_2 : E_c \rightarrow E_{-c} \]

\[ (x, y) \mapsto \left( \frac{-x}{2} + \frac{162+81c}{-2(x-12)}, \frac{-y}{2\sqrt{-2}} \left( 1 - \frac{162+81c}{(x-12)^2} \right) \right) \]

\[ \pi_q \circ \mathcal{I}_2 = \phi_2 \equiv [\sqrt{\pm 2}] \]

- \( E_c/\mathbb{F}_{q^2} : y^2 = x^3 + 27(3c - 10)x + 108(14 - 9c) \)
- \( E_{-c}/\mathbb{F}_{q^2} : y^2 = x^3 + 27(-3c - 10)x + 108(14 + 9c) \)
- In \( \mathbb{F}_{q^2} \), \( \pi_q(c) = -c \)
- Go back from \( E_{-c} \) to \( E_c \) with the Frobenius map
- \( \phi_2 \) is different from the CM
- We can construct a second endomorphism from CM.
Efficient 4-dim. GLV on $E_c$

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

- 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.

\[
\begin{align*}
n &= 0x55d23edfa6a1f7e4 \\
m &= 0x549906b3eca27851 \\
t &= -0xfaca844b264dfaa353355300f9ce9d3a \\
q &= 0x9a2a8c914e2d05c3f2616cade9b911ad \\
r &= 0x1735ce0c4fbac46c2245c3ce9d8da0244f9059ae9ae4784d6b2f65b29c444309 \\
c^2 &= 0x40b634aec52905949ea0fe36099cb21a
\end{align*}
\]

with $q, r$ prime and $\#E_c(\mathbb{F}_{q^2}) = 4r$. 
## Operation count at the 128 bit security level

<table>
<thead>
<tr>
<th>Curve</th>
<th>Method</th>
<th>Operation count</th>
<th>Global estim.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E_c$</td>
<td>4-GLV, 16 pts.</td>
<td>$2748m+1668s$</td>
<td>$4416m$</td>
</tr>
<tr>
<td>$D = 4$ [LongaSica12]</td>
<td>4-GLV, 16 pts.</td>
<td>$1992m+2412s$</td>
<td>$4404m$</td>
</tr>
<tr>
<td>$E_c$</td>
<td>2-GLV, 4 pts.</td>
<td>$4704m+2976s$</td>
<td>$7680m$</td>
</tr>
<tr>
<td>$J_{C_1}$</td>
<td>4-GLV, 16 pts.</td>
<td>$4500m+ 816s$</td>
<td>$5316m$</td>
</tr>
<tr>
<td>$J_{C_1}$</td>
<td>2-GLV, 4 pts.</td>
<td>$7968m+1536s$</td>
<td>$9504m$</td>
</tr>
<tr>
<td>FKT [Bos et al. 13]</td>
<td>4-GLV, 16 pts.</td>
<td>$4500m+ 816s$</td>
<td>$5316m$</td>
</tr>
<tr>
<td>Kummer [Bos et al. 13]</td>
<td>–</td>
<td>$3328m+2048s$</td>
<td>$5376m$</td>
</tr>
</tbody>
</table>

**Table:** Benchmarks for scalar multiplication at 128 security level

<table>
<thead>
<tr>
<th>Curve</th>
<th>Method</th>
<th>Timing in ms.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E_{1,c}$ this work</td>
<td>4-GLV, 16 pts.</td>
<td>0.002202</td>
</tr>
<tr>
<td>$E_1$ Longa-Sica</td>
<td>4-GLV, 16 pts.</td>
<td>0.001882</td>
</tr>
<tr>
<td>$E_{1,c}$ GLV</td>
<td>2-GLV, 4pts.</td>
<td>0.004070</td>
</tr>
<tr>
<td>$J_{C_1}$ this work</td>
<td>4-GLV, 4 pts.</td>
<td>0.001831</td>
</tr>
</tbody>
</table>