Four-dimensional GLV via the Weil restriction

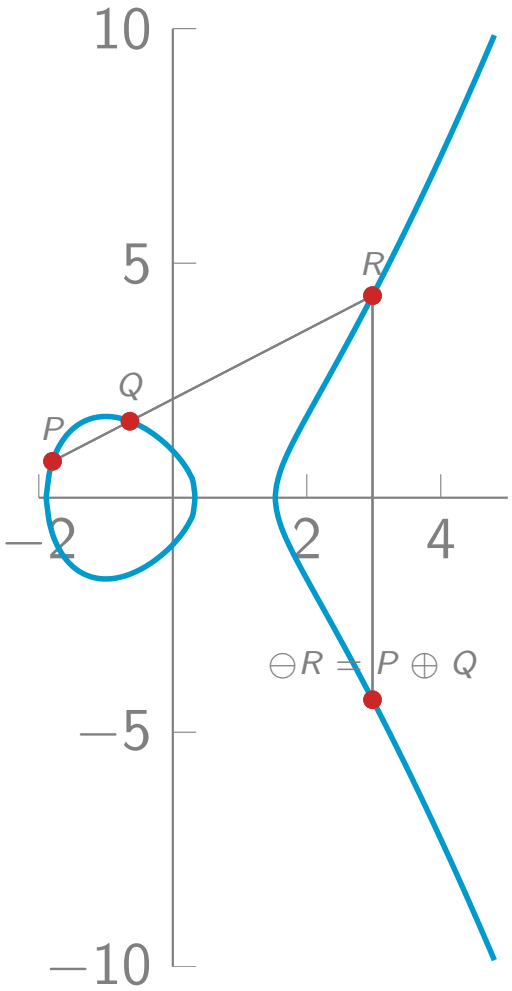
Aurore Guillevic[1,2] and Sorina Ionica[1]

[1]École Normale Supérieure Paris and [2]Thales Communications

Asiacrypt 2013

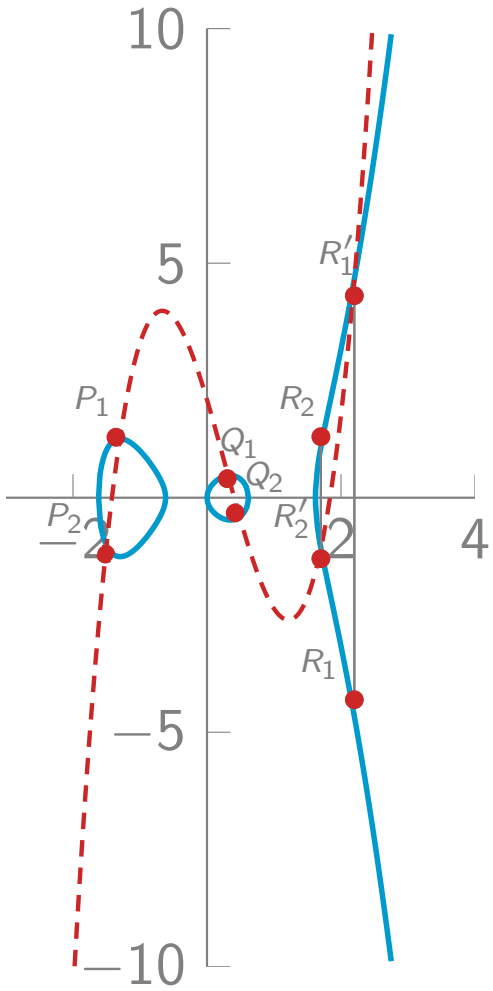
Elliptic versus genus 2 curves

Genus 1 addition



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

Genus 2 addition



$\#J_{\mathcal{C}}(\mathbb{F}_q) \sim q^2$

How fast...?

Scalar multiplication: given G of prime order r, $m \in \mathbb{Z}/r\mathbb{Z}$, $P \in G$:

$$(P, m) \to mP.$$

- Assume there is an efficient (almost free) endomorphism

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

$\to$ Gallant-Lambert-Vanstone Crypto 2001.

- if λ_ϕ is large, decompose $m = m_0 + \lambda_\phi m_1 \bmod r$ (Extended Euclid), with $\log m_0 \sim \log m_1 \sim \log m/2$
- compute $mP = m_0 P + m_1 \phi(P)$ with a multiexponentiation algorithm

- For a scalar multiplication $mP \in E(\mathbb{F}_q)$ speed-up of up to 50 % via a multiexponentiation algorithm!

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.

Computing 4-dim. decompositions

Consider the lattice
$L = \{(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 | x_1 + x_2\lambda_\phi + x_3\lambda_\psi + x_4\lambda_\phi\lambda_\psi = 0 \pmod{r}\}$

Consider a "good" basis (v_i) with $\max_i |v_i| \leq Cr^{1/4}$, C tiny.

Write $(m, 0, 0, 0) = \sum_{j=1}^{4} \beta_j v_j$, with $\beta_j \in \mathbb{Q}$.

$v = \sum_{j=1}^{4} \lfloor \beta_j \rceil v_j \Rightarrow u = (m, 0, 0, 0) - v = (m_1, m_2, m_3, m_4)$.

Hence $mP = m_1 P + m_2\lambda_\phi P + m_3\lambda_\psi P + m_4\lambda_\psi\lambda_\phi P$ with $|m_i| \leq 2Cr^{1/4}$.

Dimension 4 - Longa and Sica 2012

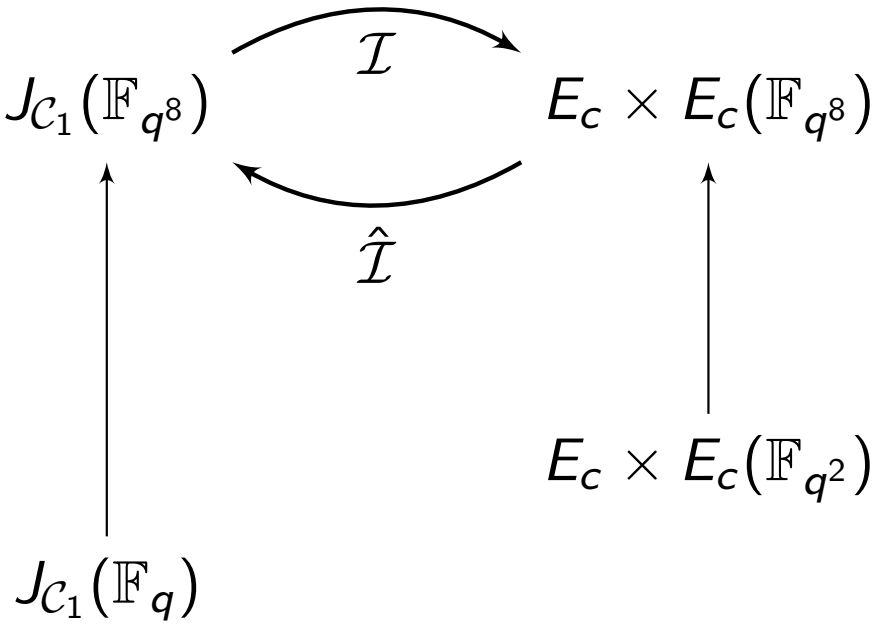
- Curves are ordinary, i.e. endomorphisms form a lattice of dimension 2 $\Rightarrow [1, \phi]$
- we need ψ s.t. $\lambda_\psi \equiv \alpha + \beta\lambda_\phi \bmod r$ and $\alpha, \beta > r^{1/4}$ to have a good lattice reduction

How to construct ψ 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

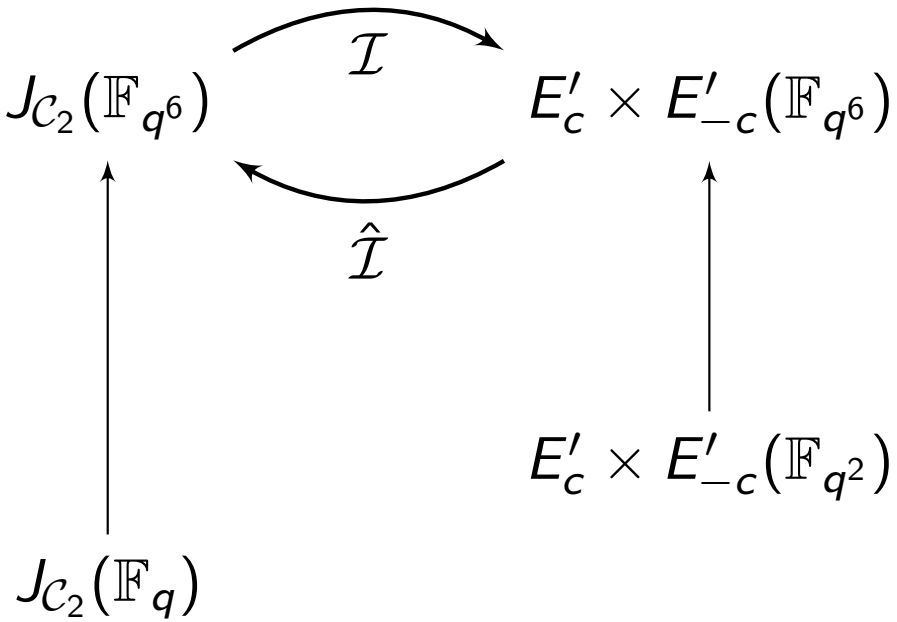


$$\mathcal{C}_1 \colon\ y^2 = x^5 + ax^3 + bx,\ a, b \in \mathbb{F}_q$$

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

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

Freeman-Satoh curves

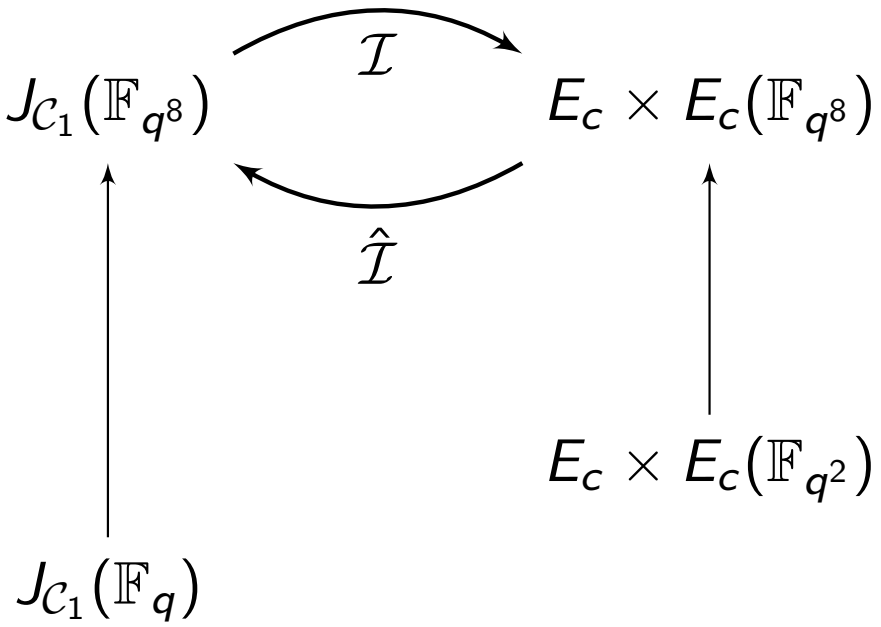


$$\mathcal{C}_2 : y^2 = x^6 + ax^3 + b,\ a, b \in \mathbb{F}_q$$

$J_{\mathcal{C}_2}$ is the Weil restriction of

$$E'_c/\mathbb{F}_{q^2} : y^2 = x^3 + 3(2c-5)x + c^2 - 14c + 22 \text{ with } c = a/\sqrt{b}.$$

Satoh's Jacobians



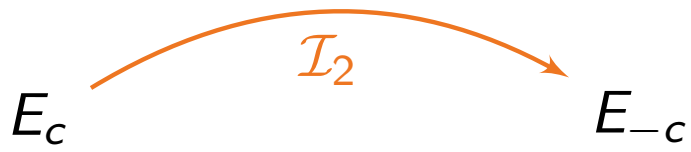
$$D = 2D' \longrightarrow E_c \overset{\mathcal{I}_2}{\dashrightarrow} ?$$

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

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

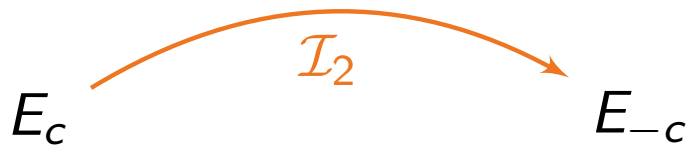


- $E_c/\mathbb{F}_{q^2} : y^2 = x^3 + 27(3c-10)x + 108(14-9c)$
- $E_{-c}/\mathbb{F}_{q^2} : y^2 = x^3 + 27(-3c-10)x + 108(14+9c)$

4-dim GLV on elliptic curves

We computed with Vélu's formulas this 2-isogeny

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



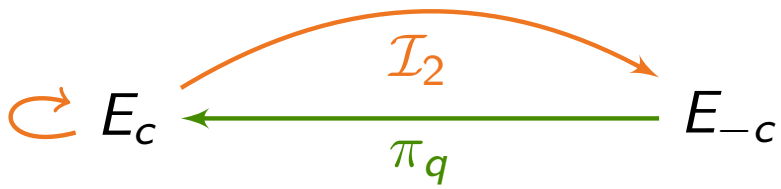
- $E_c/\mathbb{F}_{q^2} : y^2 = x^3 + 27(3c-10)x + 108(14-9c)$
- $E_{-c}/\mathbb{F}_{q^2} : y^2 = x^3 + 27(-3c-10)x + 108(14+9c)$
- In $\mathbb{F}_{q^2}$, $\pi_q(c) = -c$
- Go back from E_{-c} to E_c with the Frobenius map
- Similar to Smith's construction on reductions of $\mathbb{Q}$-curves.

4-dim GLV on elliptic curves

We computed with Vélu's formulas this 2-isogeny

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

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



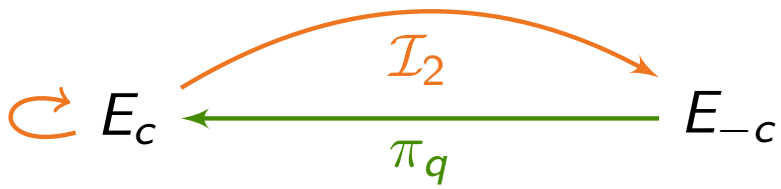
- $E_c/\mathbb{F}_{q^2} : y^2 = x^3 + 27(3c - 10)x + 108(14 - 9c)$
- $E_{-c}/\mathbb{F}_{q^2} : y^2 = x^3 + 27(-3c - 10)x + 108(14 + 9c)$
- In $\mathbb{F}_{q^2}$, $\pi_q(c) = -c$
- Go back from E_{-c} to E_c with the Frobenius map
- Similar to Smith's construction on reductions of $\mathbb{Q}$-curves.

4-dim GLV on elliptic curves

We computed with Vélu's formulas this 2-isogeny

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

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



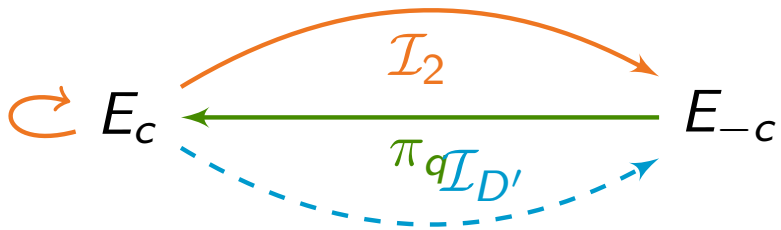
- $E_c/\mathbb{F}_{q^2} : y^2 = x^3 + 27(3c-10)x + 108(14-9c)$
- $E_{-c}/\mathbb{F}_{q^2} : y^2 = x^3 + 27(-3c-10)x + 108(14+9c)$
- In $\mathbb{F}_{q^2}$, $\pi_q(c) = -c$
- Go back from E_{-c} to E_c with the Frobenius map
- Similar to Smith's construction on reductions of $\mathbb{Q}$-curves.
- ϕ_2 is different from the CM

4-dim GLV on elliptic curves

We computed with Vélu's formulas this 2-isogeny

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

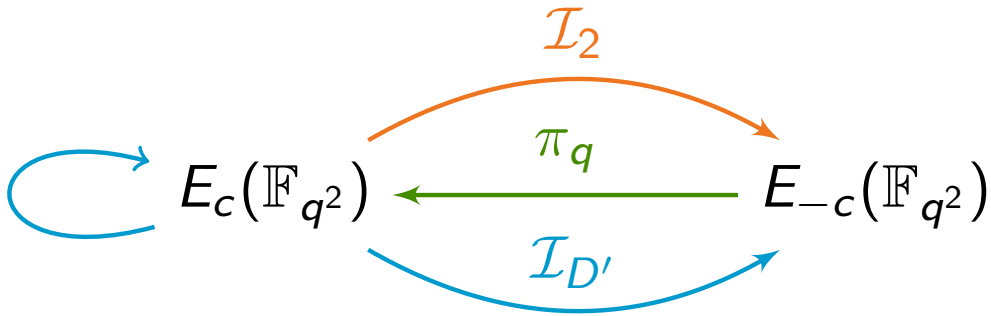
$\pi_q \circ \mathcal{I}_2 = \phi_2 \equiv [\sqrt{\pm 2}]$



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

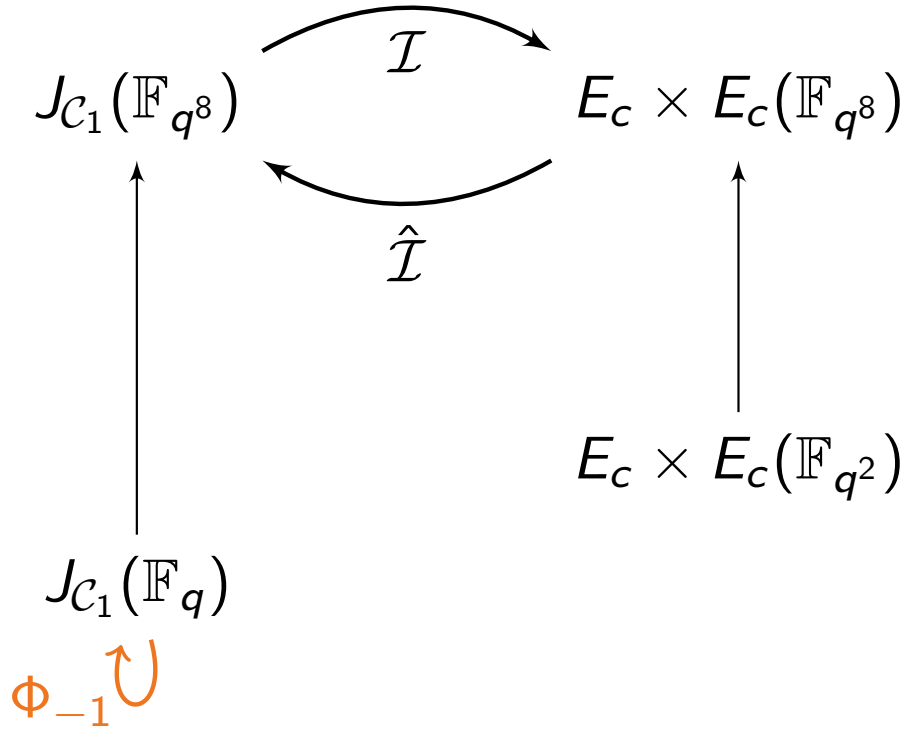
Efficient 4-dim. GLV on E_c

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



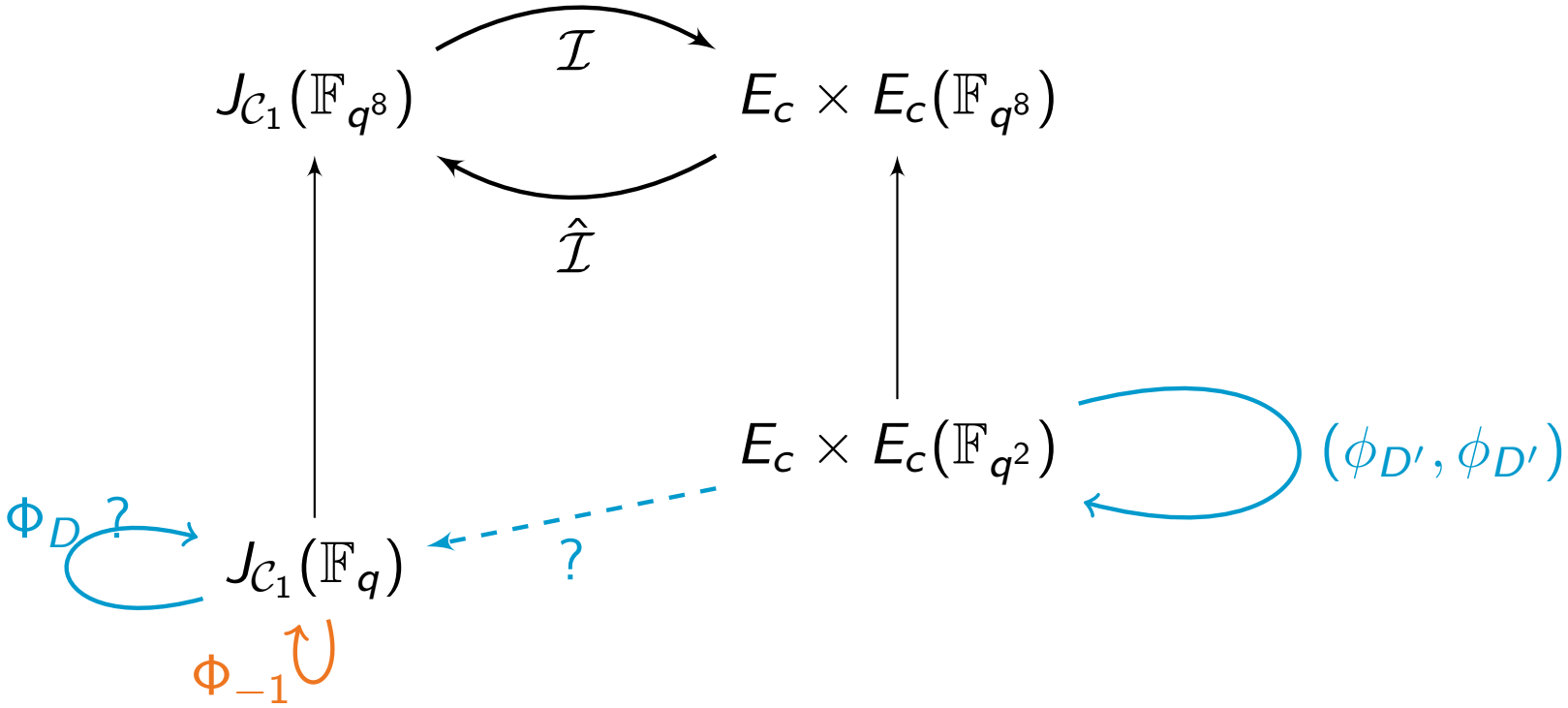
- second isogeny $\mathcal{I}_{D'}$ computed with Velu's formulas
- 4-dimensional decomposition using proper values of $1, \phi_2, \phi_{D'}, \phi_2 \circ \phi_{D'}$.
- $\phi_2^2 \pm 2 = 0$, $\phi_{D'}^2 \mp D' = 0$ for points defined over $\mathbb{F}_{q^2}$.

Satoh's genus 2 curves



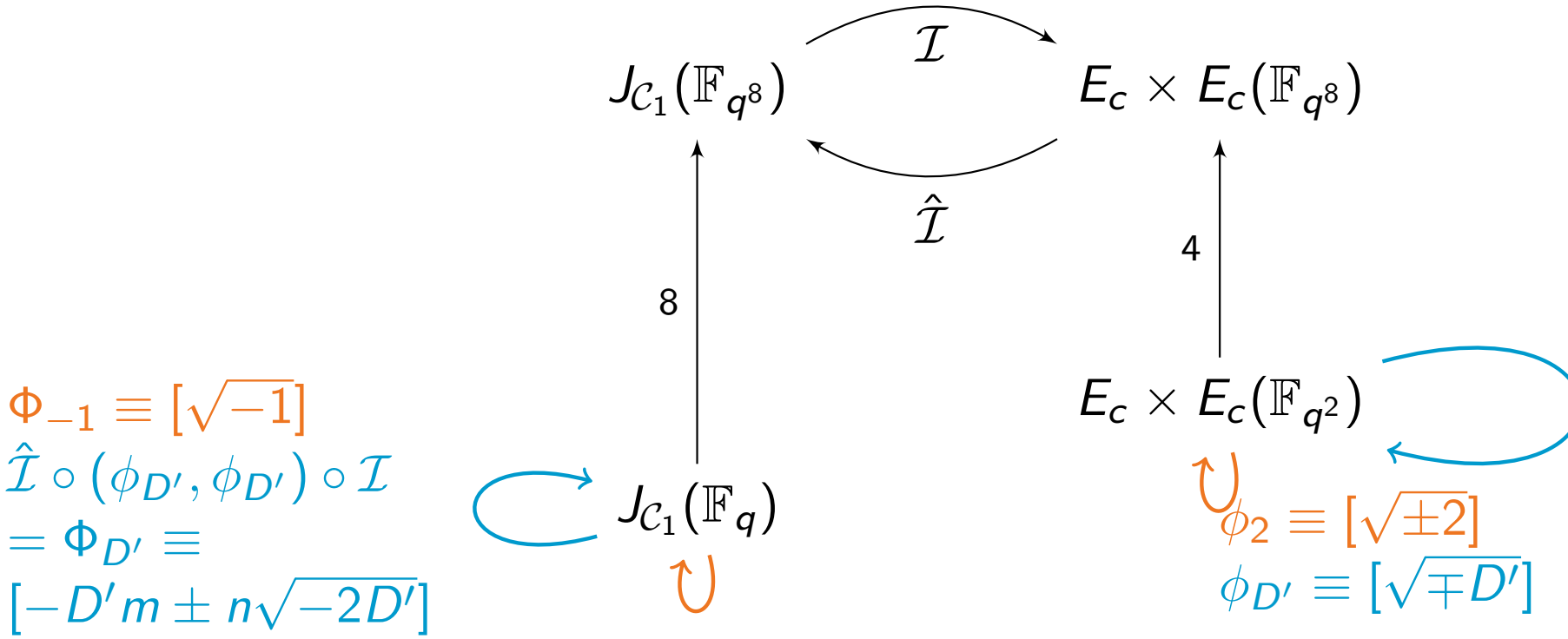
- we already have Φ_{-1} on $J_{\mathcal{C}_1}$:
  $\mathcal{D} : (u_1, u_0, v_1, v_0) \mapsto (-u_1, u_0, -iv_1, iv_0)$

Satoh's genus 2 curves



- we already have Φ_{-1} on $J_{\mathcal{C}_1}$:
  $\mathcal{D} : (u_1, u_0, v_1, v_0) \mapsto (-u_1, u_0, -iv_1, iv_0)$
- construct an endomorphism from CM on $E_c \times E_c$
- bring it back to $J_{\mathcal{C}_1}$ via the isogeny
- optimized isogeny computation $\rightarrow$ roughly an addition of elements in the Jacobian over $\mathbb{F}_{q^2}$.

4-dim. GLV on $J_{\mathcal{C}_1}$



- 2 endomorphisms on $J_{\mathcal{C}_1}(\mathbb{F}_q)$: Φ_{-1}, $\Phi_{D'}$
- Φ_{-1} is s.t. $\Phi_{-1}^2 + 1 = 0$ on $J_{\mathcal{C}_1}$
- $\Phi_{D'}$ is s.t. $\Phi_{D'}^2 + 2D'm\Phi_{D'} + 4D'p = 0$.

Constructing curves using the CM method

- Pick a discriminant $D = 2D'$, with D' small.
- Search for q such that $4q = 2n^2 + D'm^2$.
- Take the Hilbert polynomial and get roots in $\mathbb{F}_{q^2} \rightarrow j(E_c)$
- Solve $j(E_c) = 2^6 \frac{(3c-10)^3}{(c-2)(c+2)^2}$ and find $c \in \mathbb{F}_{q^2}$ such that $c^2 \in \mathbb{F}_q$.
- We may choose the value of $r | \#E(\mathbb{F}_{q^2})$ as an input of our algorithm.

  $\rightarrow$ prevent from attacks on the q-DH assumption.

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.

$$
\begin{aligned}
n &= 0\text{x}55\text{d}23\text{edfa}6\text{a}1\text{f}7\text{e}4 \\
m &= 0\text{x}549906\text{b}3\text{eca}27851 \\
t &= -\ 0\text{xfaca}844\text{b}264\text{dfaa}353355300\text{f}9\text{ce}9\text{d}3\text{a} \\
q &= 0\text{x}9\text{a}2\text{a}8\text{c}914\text{e}2\text{d}05\text{c}3\text{f}2616\text{cade}9\text{b}911\text{ad} \\
r &= 0\text{x}1735\text{ce}0\text{c}4\text{fbac}46\text{c}2245\text{c}3\text{ce}9\text{d}8\text{da}0244\text{f}9059\text{ae}9\text{ae}4784\text{d}6\text{b}2\text{f}65\text{b}29\text{c}444309 \\
c^2 &= 0\text{x}40\text{b}634\text{aec}52905949\text{ea}0\text{fe}36099\text{cb}21\text{a}
\end{aligned}
$$

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]	–	$3328m+2048s$	$5376m$

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]	–	$3328m+2048s$	$5376m$

Thank you for your attention!

Thanks to Aurore for part of the slides!