UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

FUN WITH ISOGENIES AND TREES

Luca De Feo[1]
joint work with David Jao[2] and Jérôme Plût[3]
[1]Université de Versailles – Saint-Quentin-en-Yvelines,
[2]University of Waterloo,
[3]ANSI

October 30, 2012, Séminaire LFANT,
projet LFANT, Université de Bordeaux

As long as we are concerned in this talk, elliptic curves are

- Algebraic groups defined over a (finite) field.
- Their group law is easy to compute (say, in constant time).
- Any curve E is (almost) uniquely determined by its j-invariant $j(E)$ up to isomorphism (i.e. a change of coordinates).

$$E : y^2 = x^3 + ax + b \qquad a, b \in k$$

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

Isogenies are just the right notion of morphism for elliptic curves

- Surjective group morphism.
- Algebraic map (i.e., defined by polynomials).
- Rational (coefficients in the base field k).

$$0 \to H \to E \xrightarrow{\phi} E' \to 0$$

The kernel H determines the image curve E' up to isomorphism

$$E/H \stackrel{\text{def}}{=} E'.$$

Isogeny degree

Neither of these definitions is quite correct, but they *nearly* are:

- The degree of ϕ is the cardinality of $\ker \phi$.
- (Bisson) the degree of ϕ is the time needed to compute it.

Isogenies: an example

Define the multiplication-by-m map $[m] : E \to E$

$$[m]P = \underbrace{P + \cdots + P}_{m \text{ times}}$$

$[m]$ is an isogeny:

- $\deg[m] = m^2$;
- In general $\ker[m] = E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$.

Remark: This is, indeed, an endomorphism.

COMPUTATIONAL ISOGENIES

In practice: an isogeny ϕ is just a rational fraction (or maybe two)

$$\frac{N(x)}{D(x)} = \frac{x^n + \cdots + n_1 x + n_0}{x^{n-1} + \cdots + d_1 x + d_0} \in k(x), \qquad \text{with } n = \deg \phi,$$

and $D(x)$ vanishes on $\ker \phi$.

THE EXPLICIT ISOGENY PROBLEM

INPUT: A *description* of the isogeny (e.g, its kernel).

OUTPUT: The curve E/H and the rational fraction N/D.

LOWER BOUND: $\Omega(n)$.

THE ISOGENY EVALUATION PROBLEM

INPUT: A *description* of the isogeny ϕ, a point $P \in E(k)$.

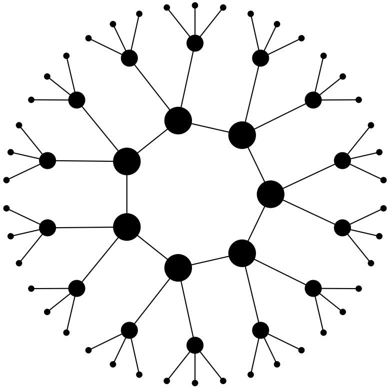
OUTPUT: The curve E/H and $\phi(P)$.

Isogeny graphs

We want to study the graph of elliptic curves with isogenies up to isomorphism. We say two isogenies ϕ, ϕ' are isomorphic if:

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[dr, "\phi'"'] & E' \arrow[d, leftrightarrow, "\wr"] \\ & E' \end{tikzcd}$$

Example: Finite field, ordinary case, graph of isogenies of degree 3.



Structure of the graph

Theorem (Serre-Tate)

Two curves are isogenous over a finite field k if and only if they have the same number of points on k.

The graph of isogenies of prime degree $\ell \neq p$

Ordinary case

- Nodes can have degree $0, 1, 2$ or $\ell + 1$.
- Connected components form so called volcanoes.

Supersingular case

- The graph is $\ell + 1$-regular.
- There is an unique connected component made of all supersingular curves with the same number of points.
- The graph has the Ramanujan property (for cryptographers like me: sufficiently long random walks land anywhere with probability distribution close to uniform).

Isogenies up to endomorphism

$$\begin{tikzcd} E \arrow[r, bend left, "\phi'"] \arrow[r, bend right, "\phi"'] & E' \end{tikzcd}$$

In some cases we want to identify edges between the same vertices. We say two isogenies ϕ, ϕ' are in the same class if there exist endomorphisms a and b of E and E' such that:

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[d, "a"'] & E' \arrow[d, "b"] \\ E \arrow[r, "\phi'"'] & E' \end{tikzcd}$$

Facts

- This is an equivalence relation.
- Two isogenies are in the same class if and only if they have the same domain and codomain.

The dual isogeny theorem

Theorem: for any isogeny $\phi : E \to E'$ there exists $\hat{\phi}$

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[d, "{[m]}"'] & E' \arrow[dl, "\hat{\phi}"] \\ E & \end{tikzcd}$$

- $\hat{\phi}$ is called the dual isogeny, $\deg \phi = \deg \hat{\phi} = m$.
- $\hat{\hat{\phi}} = \phi$.

Obvious corollaries:

- $\phi(E[m]) = \ker \hat{\phi}$ (dual isogenies are “easy” to compute).
- Graphs of isogenies are undirected.

THE ENDOMORPHISM RING

- An endomorphism is an isogeny $\phi : E \to E$.
- The endomorphisms form a ring denoted $\mathrm{End}_k(E)$.

THEOREM

$\mathbb{Q} \otimes \mathrm{End}_{\bar{k}}(E)$ is isomorphic to one of the following

ORDINARY CASE: $\mathbb{Q}$ *(only possible if* $\mathrm{char}\, k = 0$*),*

ORDINARY CASE (COMPLEX MULTIPLICATION): *an imaginary quadratic field,*

SUPERSINGULAR CASE: *a quaternion algebra (only possible if* $\mathrm{char}\, k \neq 0$*).*

COROLLARY

$\mathrm{End}(E)$ is isomorphic to an order $\mathcal{O} \subset \mathbb{Q} \otimes \mathrm{End}(E)$.

Isogenies and endomorphisms

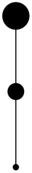
Theorem (Serre-Tate)

Two elliptic curves E, E' are isogenous if and only if

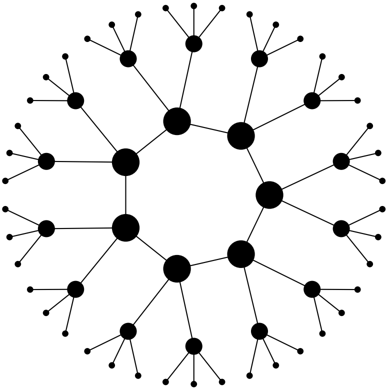
$$\mathbb{Q} \otimes \mathrm{End}(E) \simeq \mathbb{Q} \otimes \mathrm{End}(E').$$

Example: Finite field, ordinary case, 3-isogeny graph.

$\mathrm{End}(E)$



bigger node $=$ bigger $\mathrm{End}(E)$



The ordinary case

Let $\mathrm{End}(E) = \mathcal{O} \subset \mathbb{Q}(\sqrt{d})$ be the endomorphism ring of E. Define

- $\mathcal{I}(\mathcal{O})$, the group of invertible fractional ideals,
- $\mathcal{P}(\mathcal{O})$, the group of principal ideals,

Definition (The class group)

The class group of $\mathcal{O}$ is

$$\mathrm{Cl}(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O}).$$

- It is a finite abelian group.
- It arises as the Galois group of an abelian extension of $\mathbb{Q}(\sqrt{d})$.

Isogeny (classes) = ideal (classes)

Definition

Let

- $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$;
- $E[\mathfrak{a}]$ be the the subgroup of $E(\bar{k})$ annihilated by $\mathfrak{a}$;
- $\phi : E \to E/E[\mathfrak{a}]$.

Then $\deg \phi = \mathcal{N}(\mathfrak{a})$. We denote by $*$ the action on the set of elliptic curves.

$$\mathfrak{a} * j(E) = j(E/E[\mathfrak{a}]).$$

Theorem

The action $*$ *factors through* $\mathrm{Cl}(\mathcal{O})$. *It is faithful and transitive.*

Example: principal ideals

Let $\mathfrak{a} = m\mathcal{O}$, the ideal corresponding to multiplication by m. Then

- $\deg\phi = \mathcal{N}(m\mathcal{O}) = m^2$,
- $E[\mathfrak{a}] = E[m]$,
- $m\mathcal{O} \in \mathcal{P}(\mathcal{O})$,
- $m\mathcal{O} \equiv 1 \in \mathrm{Cl}(\mathcal{O})$.
- $\mathfrak{a} * j(E) = j(E)$.

Example: the dual isogeny

Let ϕ be an isogeny and $\hat\phi$ its dual. Let $\mathfrak{a}$ and $\hat{\mathfrak{a}}$ their associated ideals. Then

- $\hat{\mathfrak{a}}\mathfrak{a} = \mathfrak{a}\hat{\mathfrak{a}} = m\mathcal{O} \in \mathcal{P}(\mathcal{O})$,
- $\deg\phi = \mathcal{N}(\mathfrak{a}) = \mathcal{N}(\hat{\mathfrak{a}}) = \deg\hat\phi$,
- $\hat{\mathfrak{a}} \equiv \mathfrak{a}^{-1} \in \mathrm{Cl}(\mathcal{O})$.

Diffie-Hellman key exchange

Let $G = \langle g \rangle$ be a cyclic group of prime order p.

$$\begin{tikzcd}
 & g \arrow[dl, "a"'] \arrow[dr, "b"] & \\
g^{a} \arrow[dr, "b"'] & & g^{b} \arrow[dl, "a"] \\
 & g^{ab} &
\end{tikzcd}$$

Group action: $\mathbb{Z}/p\mathbb{Z}$ over G.

DH-like key exchange based on (semi)-group actions

Let G be an abelian group acting (faithfully and transitively) on a set X.

$$\begin{tikzcd} & x_0 \arrow[dl, "g"'] \arrow[dr, "h"] & \\ g \cdot x_0 \arrow[dr, "h"'] & & h \cdot x_0 \arrow[dl, "g"] \\ & gh \cdot x_0 = hg \cdot x_0 & \end{tikzcd}$$

Hidden Subgroup Problem

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

Let G be a group, X a set and $f : G \to X$. We say that f hides a subgroup $H \subset G$ if

$$f(g_1) = f(g_2) \Leftrightarrow g_1 H = g_2 H.$$

Definition (Hidden Subgroup Problem (HSP))

INPUT: G, X as above, an oracle computing f.

OUTPUT: generators of H.

Theorem (Schorr, Josza)

If G is abelian, then

- $HSP \in poly_{BQP}(\log|G|)$,
- *using* $poly(\log|G|)$ *queries to the oracle.*

DISCRETE LOGARITHM → HSP

Let $G = \langle g \rangle$ of order p, and let $h = g^s$. Define

$$\begin{aligned} f : (\mathbb{Z}/p\mathbb{Z})^2 &\to G \\ (a, b) &\mapsto g^a h^b = g^{a+sb} \end{aligned}$$

Remark: A collision in f uncovers the secret s, like in Pollard's Rho.

THE REDUCTION

- f is a group morphism;
- $\ker f = \langle (s, -1) \rangle \simeq \mathbb{Z}/p\mathbb{Z}$.

Hence f hides the secret $\langle (s, -1) \rangle$.

Consequence: Diffie-Hellman is broken by quantum computers

The security of DH-like schemes based on group actions depends on

DEFINITION ((SEMI)GROUP ACTION PROBLEM (SAP))

INPUT: A (semi)group G, a set X, elements $x, y \in X$.

OUTPUT: Find $s \in G$ such that $y = s \cdot x$.

DEFINITION (HIDDEN SHIFT PROBLEM (HSHP))

INPUT: $f_0, f_1 : G \to X$ two oracles such that $f_1(g) = f_0(gs)$.

OUTPU: The secret $s \in G$.

The Hidden Shift Problem

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

Reductions

- SAP $\to$ HShP (evident).
- HShP $\to$ non-abelian HSP for the dihedral group $G \ltimes \mathbb{Z}/2\mathbb{Z}$.

Quantum algorithms:

Kuperberg: $2^{O(\sqrt{\log |G|})}$ quantum time and space and query complexity.

Regev: $L_{|G|}(\frac{1}{2}, \sqrt{2})$ quantum time and query complexity,
poly(log($|G|$)) quantum space.

Remark (Regev): certain lattice-based cryptosystems are also vulnerable to the HSP for dihedral groups.

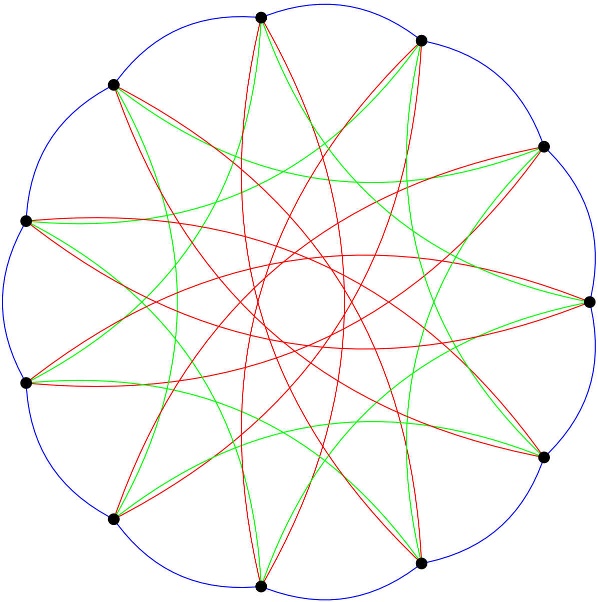
Rostovstev and Stolbunov's key exchange

Public data:

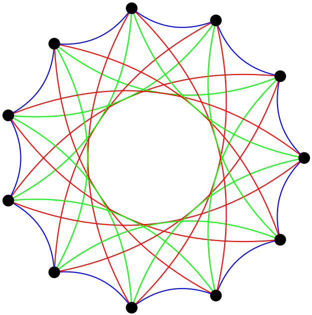
- $E/\mathbb{F}_p$ ordinary elliptic curve with complex multiplication field $\mathbb{K}$,
- primes ℓ_1,ℓ_2, ℓ_3, … not dividing $\mathrm{Disc}(E)$ and s.t. $\left(\frac{D_{\mathbb{K}}}{\ell_i}\right) = 1$.
- A *direction* on each ℓ_i-isogeny graph (a Frobenius eigenvalue).

Secret data: Random walks $\mathfrak{a}, \mathfrak{b}$ in the ℓ_i-isogeny graphs.

$$\begin{tikzcd}
 & E \arrow[dl, "\ell_1^{a_1}\ell_2^{a_2}\ell_3^{a_3}\cdots = \mathcal{N}(\mathfrak{a})"'] \arrow[dr, "\mathcal{N}(\mathfrak{b}) = \ell_1^{b_1}\ell_2^{b_2}\ell_3^{b_3}\cdots"] & \\
\mathfrak{a} * E \arrow[dr] & & \mathfrak{b} * E \arrow[dl] \\
 & \mathfrak{ab} * E = \mathfrak{ba} * E &
\end{tikzcd}$$


ℓ_1-isogenies
ℓ_2-isogenies
ℓ_3-isogenies

R&S KEY EXCHANGE



KEY GENERATION: compose small degree isogenies
polynomial in the lenght of the random walk.

ATTACK: find an isogeny between two curves
polynomial in the degree.

QUANTUM (CHILDS-JAO-SOUKHAREV): HShP + isogeny evaluation
subexponential in the length of the walk.

$\mathbb{Q} \otimes \mathrm{End}(E)$ is a quaternion algebra (non-commutative)

Facts

- Every supersingular curve is defined over $\mathbb{F}_{p^2}$.
- $E(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2$ (up to twist).
- There are $g(X_0(p)) + 1 \sim \frac{p+1}{12}$ supersingular curves up to isomorphism.
- For every maximal order type of the quaternion algebra $\mathbb{Q}_{p,\infty}$ there are 1 or 2 curves over $\mathbb{F}_{p^2}$ having endomorphism ring isomorphic to it.
- There is a unique isogeny class of supersingular curves over $\bar{\mathbb{F}}_p$ (there are two over any finite field).
- The graph of ℓ-isogenies is $\ell + 1$-regular.

Good and bad news

Good news: there is no action of a commutative class group.

Bad news: there is no action of a commutative class group.

However: left ideals of $\mathrm{End}(E)$ still act on the isogeny graph:

$$\begin{tikzcd} E \arrow[r, "\mathfrak{a}"] \arrow[d, "\mathfrak{b}"'] & E' \arrow[d, "\mathfrak{b}_{\mathfrak{a}}"] \\ E'' \arrow[r, "\mathfrak{a}_{\mathfrak{b}}"'] & E''' \end{tikzcd}$$

- The action factors through the right-isomorphism equivalence of ideals.
- Ideal classes form a groupoid (in other words, an undirected multigraph...).

From ideals back to isogenies

In practice, computations with ideals are hard. We fix, instead:

- Small primes ℓ_A, ℓ_B;
- A large prime p such that $p+1 = \ell_A^{e_A}\ell_B^{e_B}$;
- A supersingular curve E over $\mathbb{F}_{p^2}$, such that

$$E \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2 = (\mathbb{Z}/\ell_A^{e_A}\mathbb{Z})^2 \oplus (\mathbb{Z}/\ell_B^{e_B}\mathbb{Z})^2,$$

- We use isogenies of degrees $\ell_A^{e_A}$ and $\ell_B^{e_B}$ with cyclic rational kernels;
- The diagram below can be constructed in time poly($e_A + e_B$).

$$\ker\phi = \langle P\rangle \subset E[\ell_A^{e_A}]$$

$$\ker\psi = \langle Q\rangle \subset E[\ell_B^{e_B}]$$

$$\ker\phi' = \langle \psi(P)\rangle$$

$$\ker\psi' = \langle \phi(Q)\rangle$$

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[d, "\psi"'] & E/\langle P\rangle \arrow[d, "\psi'"] \\ E/\langle Q\rangle \arrow[r, "\phi'"'] & E/\langle P, Q\rangle \end{tikzcd}$$

A ZK PROOF OF KNOWLEDGE

Secret: knowledge of the kernel of a degree $\ell_A^{e_A}$ isogeny from E to $E/\langle S\rangle$.

$$E \overset{\phi}{\text{———}} E/\langle S\rangle$$

A ZK proof of knowledge

Secret: knowledge of the kernel of a degree $\ell_A^{e_A}$ isogeny from E to $E/\langle S\rangle$.

$$\begin{tikzcd}
E \arrow[rr, dash, "\phi"] \arrow[d, dash, "?"'] & & E/\langle S\rangle \arrow[d, dash, "?"] \\
E/\langle P\rangle \arrow[rr, dash, "?"'] & & E/\langle P, S\rangle
\end{tikzcd}$$

1. Choose a random point $P \in E[\ell_B^{e_B}]$, compute the diagram;
2. Publish the curves $E/\langle P\rangle$ and $E/\langle P, S\rangle$;

A ZK proof of knowledge

Secret: knowledge of the kernel of a degree $\ell_A^{e_A}$ isogeny from E to $E/\langle S\rangle$.

$$
\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash, "\psi"'] & E/\langle S\rangle \arrow[d, dash, "\psi'"] \\
E/\langle P\rangle \arrow[r, dash, "?"'] & E/\langle P, S\rangle
\end{tikzcd}
$$

1. Choose a random point $P \in E[\ell_B^{e_B}]$, compute the diagram;
2. Publish the curves $E/\langle P\rangle$ and $E/\langle P, S\rangle$;
3. The verifier asks one of the two questions:
   - Reveal the degree $\ell_B^{e_B}$ isogenies;

A ZK proof of knowledge

Secret: knowledge of the kernel of a degree $\ell_A^{e_A}$ isogeny from E to $E/\langle S\rangle$.

$$\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash, "?"'] & E/\langle S\rangle \arrow[d, dash, "?"] \\
E/\langle P\rangle \arrow[r, dash, "\phi'"'] & E/\langle P, S\rangle
\end{tikzcd}$$

1. Choose a random point $P \in E[\ell_B^{e_B}]$, compute the diagram;
2. Publish the curves $E/\langle P\rangle$ and $E/\langle P, S\rangle$;
3. The verifier asks one of the two questions:
   - Reveal the degree $\ell_B^{e_B}$ isogenies;
   - Reveal the bottom isogeny.

SECURITY

$$\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash, "?"'] & E/\langle S \rangle \arrow[d, dash, "?"] \\
E/\langle P \rangle \arrow[r, dash, "\phi'"'] & E/\langle P, S \rangle
\end{tikzcd}$$

What information does ϕ' give on ϕ?

- We prove that the protocol is zero-knowledge if distinguishing a pair (ϕ, ϕ') from a random pair (ϕ, χ) is hard.
- We conjecture this problem is hard, even using ideal classes.

Security

$$\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash, "\psi"'] & E/\langle S \rangle \arrow[d, dash, "\psi'"] \\
E/\langle P \rangle \arrow[r, dash, "?"'] & E/\langle P, S \rangle
\end{tikzcd}$$

What information do ψ and ψ' give on ϕ?

- On the first round, we learn $(P, \phi(P))$,

SECURITY

$$\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash, "\psi"'] & E/\langle S\rangle \arrow[d, dash, "\psi'"] \\
E/\langle Q\rangle \arrow[r, dash, "?"'] & E/\langle Q, S\rangle
\end{tikzcd}$$

What information do ψ and ψ' give on ϕ?

- On the first round, we learn $(P, \phi(P))$,
- On the second round, we learn $(Q, \phi(Q))$,
- $\ldots$

SECURITY

$$\begin{tikzcd}[column sep=huge, row sep=huge]
E \arrow[r, dash, "\phi"] \arrow[d, dash, "\psi"'] & E/\langle S\rangle \arrow[d, dash, "\psi'"] \\
E/\langle Q\rangle \arrow[r, dash, "?"'] & E/\langle Q, S\rangle
\end{tikzcd}$$

What information do ψ and ψ' give on ϕ?

- On the first round, we learn $(P, \phi(P))$,
- On the second round, we learn $(Q, \phi(Q))$,
- $\dots$
- With high probabilty, $\langle P, Q\rangle = E[\ell_B^{e_B}]$, and we learn $\phi(E[\ell_B^{e_B}])$.
- We make $\phi(E[\ell_B^{e_B}])$ part of the public data, and we conjecture that this is secure.

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

The idea: Alice chooses ϕ, Bob chooses ψ.

$$\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash, "\psi"'] & E/\langle P\rangle \arrow[d, dash, "\psi'"] \\
E/\langle Q\rangle \arrow[r, dash, "\phi'"'] & E/\langle P, Q\rangle
\end{tikzcd}$$

Problem:

- How does Alice know the kernel of ϕ'?
- How does Bob know the kernel of ψ'?

GOING DIFFIE-HELLMAN

The idea: Alice chooses ϕ, Bob chooses ψ.

$$\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash, "\psi"'] & E/\langle P\rangle \arrow[d, dash, "\psi'"] \\
E/\langle Q\rangle \arrow[r, dash, "\phi'"'] & E/\langle P, Q\rangle
\end{tikzcd}$$

Problem:

- How does Alice know the kernel of ϕ'?
- How does Bob know the kernel of ψ'?

Our solution:

- It is not so dangerous to publish $\phi(E[\ell_B^{e_B}])$.
- It is not so dangerous to publish $\psi(E[\ell_A^{e_A}])$.

Our proposal

Public data:

- Prime p such that $p + 1 = \ell_A^a \ell_B^b$;
- Supersingular curve $E \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2$;
- $E[\ell_A^a] = \langle P_A, Q_A \rangle$;
- $E[\ell_B^b] = \langle P_B, Q_B \rangle$.

Secret data:

- $R_A = m_A P_A + n_A Q_A$,
- $R_B = m_B P_B + n_B Q_B$,

$$
\begin{tikzcd}
 & E \arrow[dl, "\phi"'] \arrow[dr, "\psi"] & \\
E/\langle R_A \rangle \arrow[dr, "\psi'"'] & & E/\langle R_B \rangle \arrow[dl, "\phi'"] \\
\frac{E/\langle R_A \rangle}{\phi(R_B)} \simeq & E/\langle R_A, R_B \rangle & \simeq \frac{E/\langle R_B \rangle}{\psi(R_A)}
\end{tikzcd}
$$

Our proposal

Public data:

- Prime p such that $p+1=\ell_A^a\ell_B^b$;
- Supersingular curve $E\simeq(\mathbb{Z}/(p+1)\mathbb{Z})^2$;
- $E[\ell_A^a]=\langle P_A,Q_A\rangle$;
- $E[\ell_B^b]=\langle P_B,Q_B\rangle$.

Secret data:

- $R_A=m_AP_A+n_AQ_A$,
- $R_B=m_BP_B+n_BQ_B$,

$$\begin{tikzcd}
 & E \arrow[dl, "\phi"'] \arrow[dr, "\psi"] & \\
E/\langle R_A\rangle \arrow[dr, "\psi'"'] & & E/\langle R_B\rangle \arrow[dl, "\phi'"] \\
 & E/\langle R_A,R_B\rangle &
\end{tikzcd}$$

$\phi(P_B)$, $\phi(Q_B)$

$\psi(P_A)$, $\psi(Q_A)$

$$\frac{E/\langle R_A\rangle}{\phi(R_B)}\simeq E/\langle R_A,R_B\rangle\simeq\frac{E/\langle R_B\rangle}{\psi(R_A)}$$

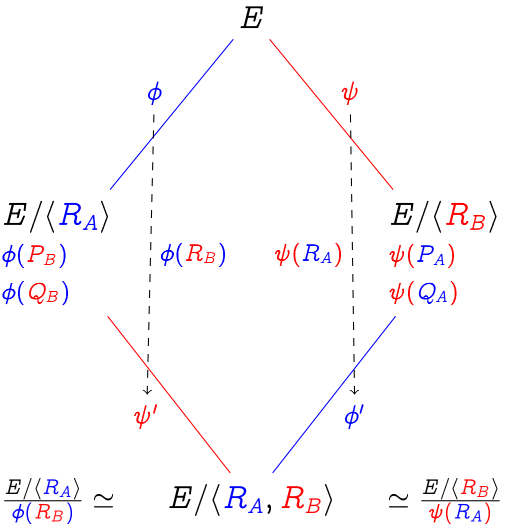
Our proposal

Public data:

- Prime p such that $p+1 = \ell_A^a \ell_B^b$;
- Supersingular curve $E \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2$;
- $E[\ell_A^a] = \langle P_A, Q_A \rangle$;
- $E[\ell_B^b] = \langle P_B, Q_B \rangle$.

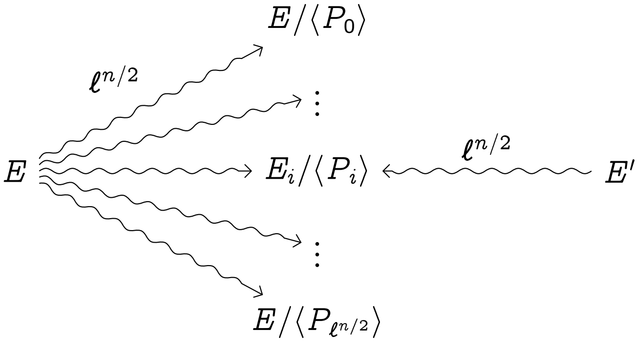
Secret data:

- $R_A = m_A P_A + n_A Q_A$,
- $R_B = m_B P_B + n_B Q_B$,



Generic attacks

Problem: Given E, E', isogenous of degree ℓ^n, find $\phi : E \to E'$.



- With high probability ϕ is the unique collision (or *claw*).
- A quantum claw finding algorithm solves the problem in $O(\ell^{n/3})$ (Tani).

Our recommended parameters

- For efficiency chose p such that $p+1 = 2^a 3^b$.
- For classical n-bit security, choose $2^a \sim 3^b \sim 2^{2n}$, hence $p \sim 2^{4n}$.
- For quantum n-bit security, choose $2^a \sim 3^b \sim 2^{3n}$, hence $p \sim 2^{6n}$.

Practical optimizations:

- -1 is a quadratic non-residue: $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[X]/(X^2+1)$.
- E (or its twist) has a 4-torsion point: it has an Edwards and a Montgomery form.
- Other optimizations in the next slides.

Analysis of the key exchange

Round 1

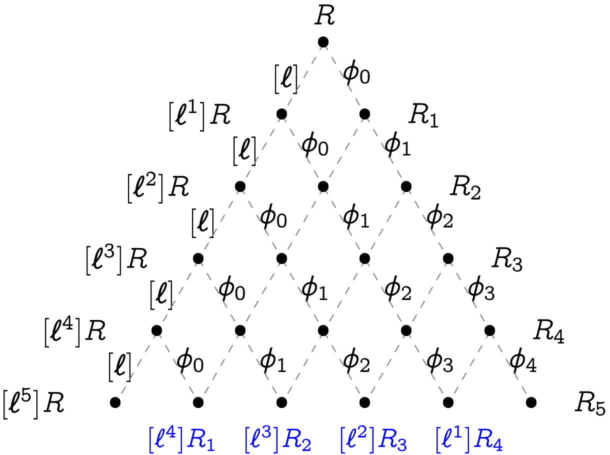
- Pick random $m, n \in \mathbb{Z}$;
- Compute $R = mP + nQ$;
- Compute $\phi : E \to E/\langle R \rangle$;
- Evaluate $\phi(S), \phi(T)$ for some points S, T.

Round 2

- Compute $R' = mP' + nQ'$;
- Compute $\psi : E \to E/\langle R' \rangle$;

EVALUATING COMPOSITE ISOGENIES

$\mathrm{ord}(R) = \ell^a$ and $\phi = \phi_0 \circ \phi_1 \circ \cdots \circ \phi_{a-1}$, each of degree ℓ



For each i, one needs to compute $[\ell^{e-i}]R_i$ in order to compute ϕ_i.

WHAT'S THE BEST STRATEGY?

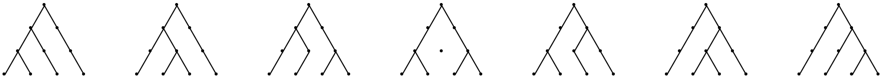


FIGURE: The seven well formed strategies for $e = 4$.

- Right edges are ℓ-isogeny evaluation;
- Left edges are multiplications by ℓ (about twice as expensive);

The best strategy can be precomputed offline and hardcoded in an embedded system.

Funny fact: strategies are in one-to-one correspondence with certain instances of Gelfand-Tsetlin patterns [OEIS, Sequence A130715].

Example

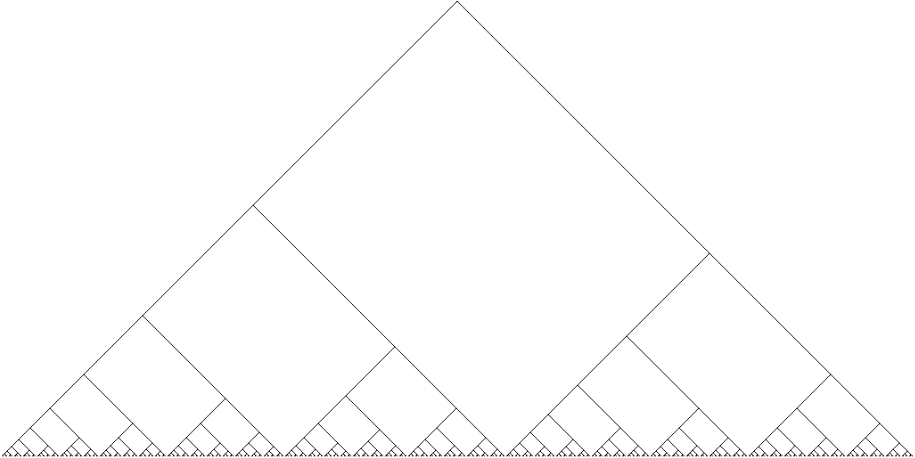
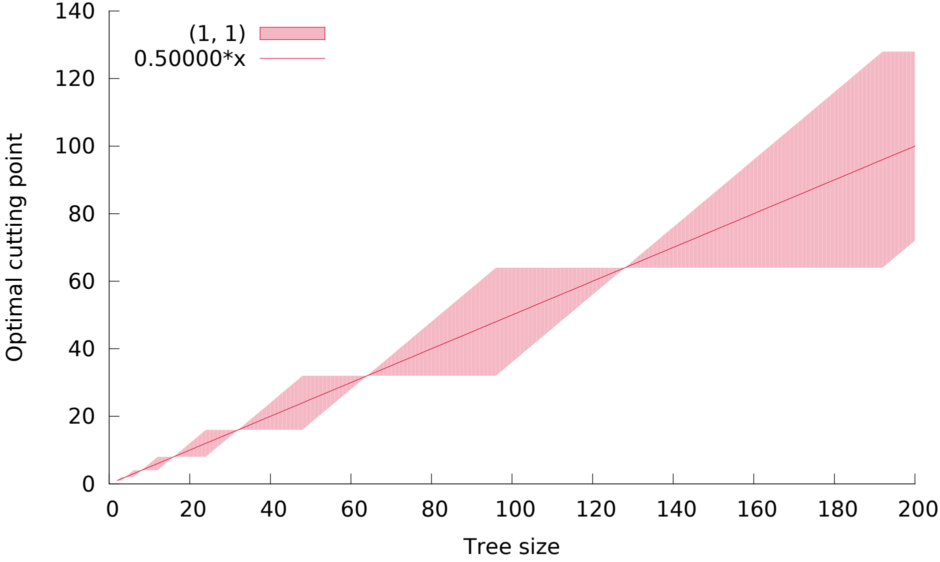
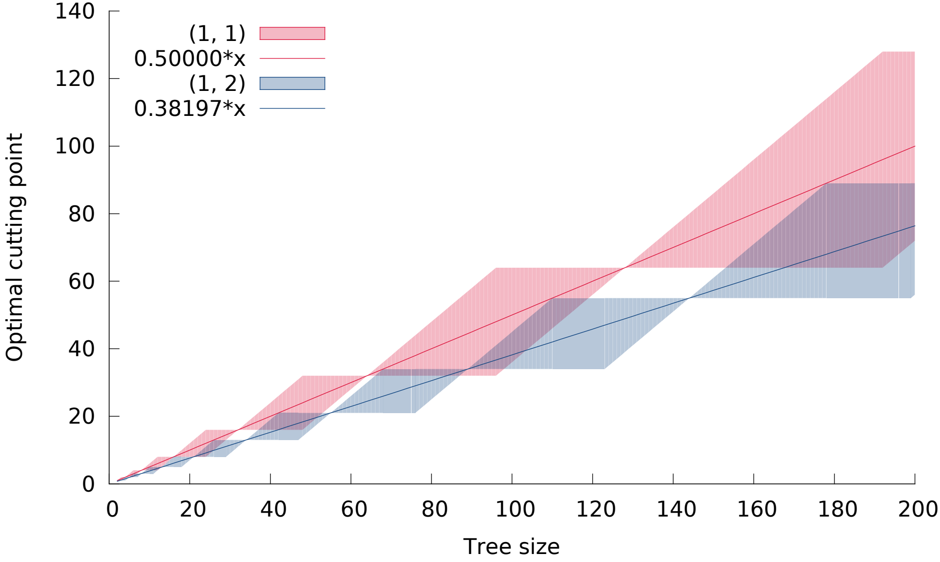


Figure: Optimal strategy for $e = 512$, $\ell = 2$.

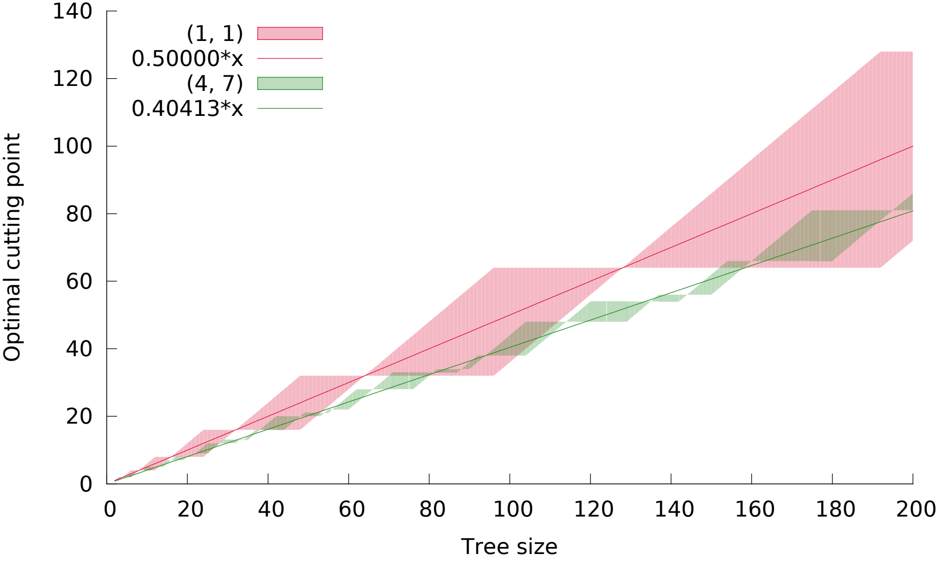
Many optimal strategies



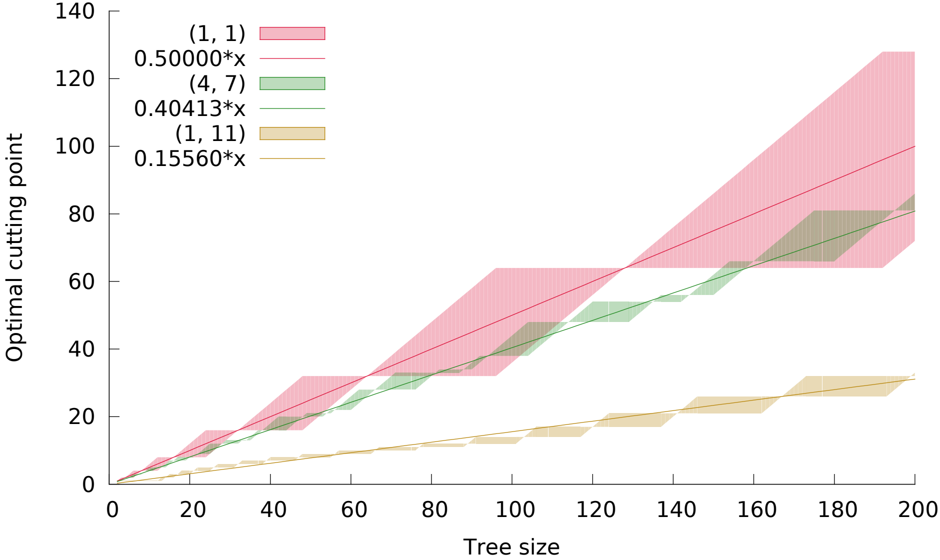
Many optimal strategies



Many optimal strategies



Many optimal strategies



Timings

Reference implementation

Available at http://www.prism.uvsq.fr/~dfl/

- C + GMP implementation of $\mathbb{F}_{p^2}$;
- C implementation of the key exchange;
- Cython interface to the key exchange and implementation of elliptic curves;
- Python + Sage script for parameter generation and strategy computation.

	tuned $(2,1)$			balanced $(1,1)$	
	512 bits	768 bits	1024 bits	768 bits	1024 bits
Alice round 1	28.1 ms	65.7 ms	122 ms	66.8 ms	123 ms
Alice round 2	23.3 ms	54.3 ms	101 ms	55.5 ms	102 ms
Bob round 1	28.0 ms	65.6 ms	125 ms	67.1 ms	128 ms
Bob round 2	22.7 ms	53.7 ms	102 ms	55.1 ms	105 ms

Conclusion

We have proposed a new candidate primitive for post-quantum cryptography.

- It is based on a new group theoretic construction that does not seem to have been used before.
- It is based on well known objects for which a lot of good software already exists.
- It has a simple Zero Knowledge proof with no analogue in classic discrete log based and group action based constructions.
- It is reasonably fast:
  - More than 1000 times faster than Rostovstev and Stolbunov's system at the same (classical) security level.
  - Running times comparable to pairing-based protocols.
- Because of its novelty, more scrutiny is required to assess its security. In particular, it is not clear what mathematical assumptions are needed to prove its security.