# Post-Quantum Cryptography QIC 891

Javad Doliskani
Institute for Quantum Computing

# Isogenies

Let $E_1, E_2$ be elliptic curves over a finite field $\mathbb{F}_q$.

### Isogeny

An rational map

$$\phi : E_1 \to E_2$$

that preserves the group structure.

- a nonzero isogeny is surjective
- an isogeny is uniquely determined by its kernel

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

# Endomorphisms

- An *endomorphism* is an isogeny $\phi : E \to E$.

**Example**

- Multiplication by an integer

$$\begin{array}{rccc} [m]: & E & \longrightarrow & E \\ & P & \longmapsto & mP \end{array}$$

- Frobenius

$$\begin{array}{rccc} \pi: & E & \longrightarrow & E \\ & (x, y) & \longmapsto & (x^q, y^q) \end{array}$$

# The endomorphism ring

- The endomorphisms form a ring denoted $\mathrm{End}_k(E)$.
- We always have $\mathbb{Z} \subseteq \mathrm{End}_k(E)$.

## 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* $\mathcal{O} \subset \mathbb{Q} \otimes \mathrm{End}(E)$.

# Computing isogenies

An isogeny $\phi$ is represented as a rational function

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

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 $N/D$.

**The explicit isogeny evaluation problem**

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

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

# Computing isogenies (cryptanalysis)

**The implicit isogeny problem**

Input: Two isogenous curves $E_1, E_2$.

Output: An isogeny $E_1 \to E_2$.

**The implicit isogeny evaluation problem**

Input: Two isogenous curves $E_1, E_2$, and a point $P \in E_1(k)$,

Output: The image $\phi(P) \in E_2(k)$ under the isogeny.

# Isogeny graphs

Consider the graph $G_\ell(k) = (V, D)$ where

- $V$: the set of elliptic curves over a given field $k$
- $D$: the set of $\ell$-isogenies between elements of $V$

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

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

# Isogenies up to endomorphism

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

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

## Facts

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

# Dual isogenies

**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:

- $\phi(E[m]) = \ker \hat{\phi}$.
- Graphs of isogenies are undirected.

# Structure of the graph[1]

### 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*.

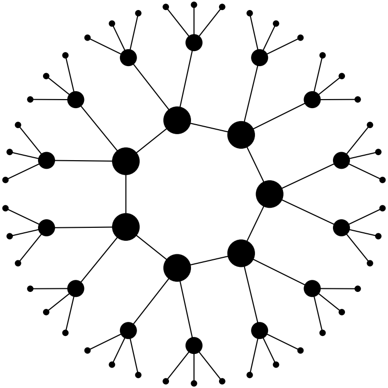
*Supersingular case*

- The graph is $(\ell + 1)$-regular.
- There is a unique connected component made of all supersingular curves with the same number of points.

[1] Kohel 1996; Fouquet and Morain 2002.

# Isogeny graphs (ordinary curves)

*Example:* Finite field, graph of 3-isogenies.



# Isogeny graphs (ordinary curves)

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

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

- 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.*

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

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

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

# DH using class groups[2]

*Public data:*

- $E/\mathbb{F}_p$ ordinary elliptic curve with complex multiplication field $\mathbb{K}$,
- primes $\ell_1$,$\ell_2$ not dividing $\mathrm{Disc}(E)$ and s.t. $\left(\frac{D_{\mathbb{K}}}{\ell_i}\right) = 1$.
- A *direction* on the isogeny graph (a Frobenius eigenvalue).

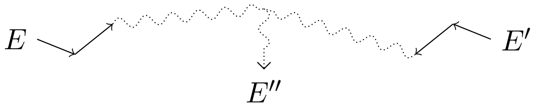
*Secret data:* Random walks $\mathfrak{a}, \mathfrak{b}$ in the $\ell_i$-isogeny graphs.

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

[2] Rostovtsev and Stolbunov 2006.

# Isogeny walks and cryptanalysis

Classic meet in the middle attack[3]




## Fourth root attacks

- Start two random walks from the two curves and wait for a collision.
- Over $\mathbb{F}_q$, the average size of an isogeny class is $h_\Delta \sim \sqrt{q}$.
- A collision is expected after $O(\sqrt{h_\Delta}) = O(q^{\frac{1}{4}})$ steps.

[3] Galbraith 1999; Galbraith, Hess, and Smart 2002; Charles, Lauter, and Goren 2009; Bisson and Sutherland 2011.

# Hidden Subgroup Problem (quantum)

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**

*If $G$ is abelian, then*

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

# Hidden Subgroup Problem (quantum)

## Known reductions

- Discrete Log on $G$ of size $p \to$ HSP on $(\mathbb{Z}/p\mathbb{Z})^2$,
- hence DH, ECDH, etc. are broken by quantum computers.
- Semigroup-DH on $G \to$ HSP on the dihedral group $G \ltimes \mathbb{Z}/2\mathbb{Z}$.

## Quantum algorithms for dihedral HSP

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

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

---

[a] Kuperberg 2005.
[b] Regev 2004.

# 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, exponential in the length.

Quantum[4]: HSP + isogeny evaluation
subexponential in the length of the walk.

[4] Childs, Jao, and Soukharev 2010.

# Supersingular curves

$\mathbb{Q} \otimes \mathrm{End}(E)$ 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, and overly simplifying!).
- There are $g(X_0(p)) + 1 \sim \frac{p+1}{12}$ supersingular curves up to isomorphism.
- There is a unique isogeny class of supersingular curves over $\bar{\mathbb{F}}_p$ (there are two over any finite field).
- The graph of $\ell$-isogenies is $\ell + 1$-regular.

# R&S key exchange with supersingular curves

- there is no action of a commutative class group.
- 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.

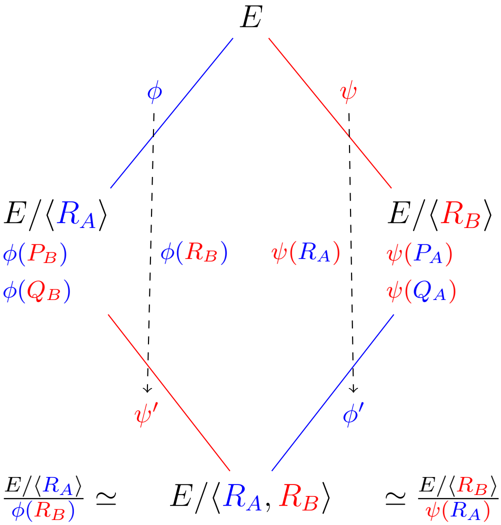
# The SIDH System[5]

*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:*

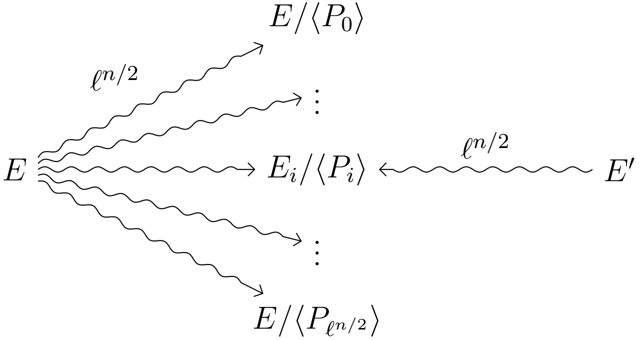
- $R_A = m_A P_A + n_A Q_A$,
- $R_B = m_B P_B + n_B Q_B$,




[5] Jao and De Feo 2011.

# Generic attacks

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




- With high probability $\phi$ is the unique collision (or *claw*).
- A *quantum claw finding*[6] algorithm solves the problem in $O(\ell^{n/3})$.

[6] Tani 2008.

# References I

Kohel, David (1996).
"Endomorphism rings of elliptic curves over finite fields".

Fouquet, Mireille and François Morain (2002).
"Isogeny Volcanoes and the SEA Algorithm".

Rostovtsev, Alexander and Anton Stolbunov (2006).
*Public-key cryptosystem based on isogenies.*

Galbraith, Steven D. (1999).
"Constructing Isogenies between Elliptic Curves Over Finite Fields".

Galbraith, Steven D., Florian Hess, and Nigel P. Smart (2002).
"Extending the GHS Weil descent attack".

Charles, Denis X., Kristin E. Lauter, and Eyal Z. Goren (2009).
"Cryptographic Hash Functions from Expander Graphs".

Bisson, Gaetan and Andrew V. Sutherland (2011).
"A low-memory algorithm for finding short product representations in finite groups".

# References II


Kuperberg, Greg (2005).
"A subexponential-time quantum algorithm for the dihedral hidden subgroup problem".

Regev, Oded (2004).
*A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space.*

Childs, Andrew M., David Jao, and Vladimir Soukharev (2010).
"Constructing elliptic curve isogenies in quantum subexponential time".

Jao, David and Luca De Feo (2011).
"Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies".

Tani, Seiichiro (2008).
"Claw Finding Algorithms Using Quantum Walk".