The isogeny cycle seminar

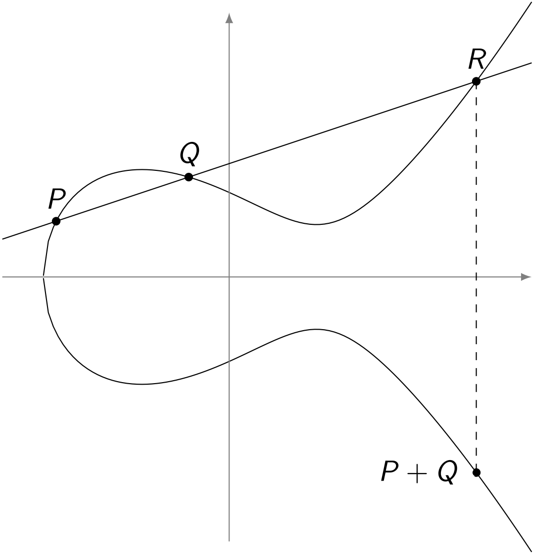
Luca De Feo

Université de Versailles & Inria Saclay

September 29, 2016, École Polytechnique Fédérale de Lausanne

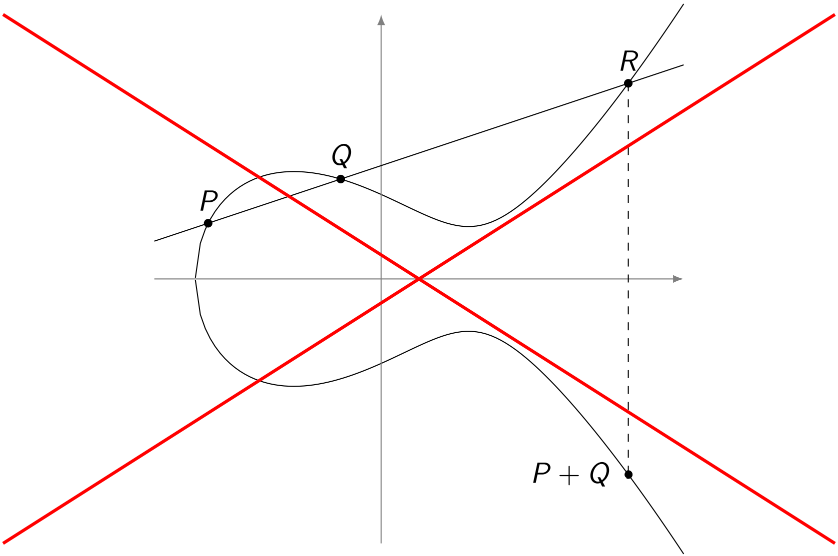
Elliptic curves

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve...

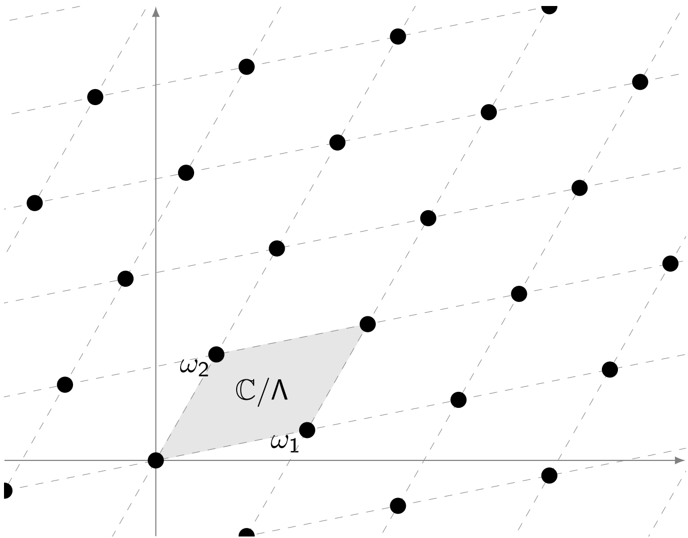


Elliptic curves

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve... forget it!



Elliptic curves

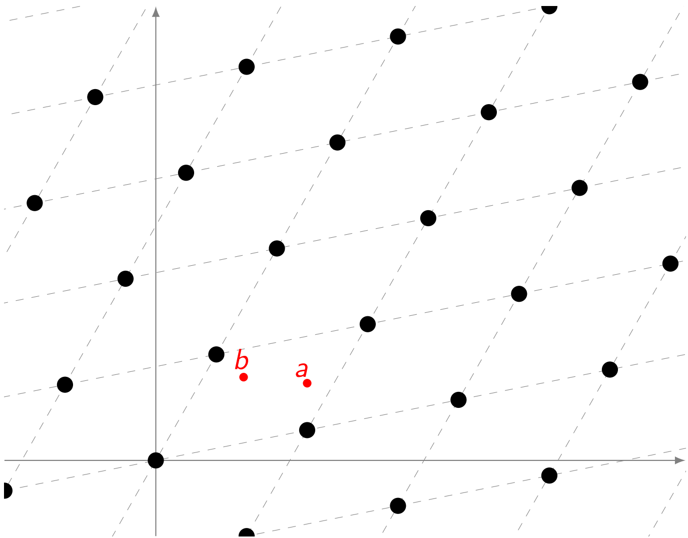


Let $\omega_1, \omega_2 \in \mathbb{C}$ be linearly independent complex numbers. Set

$$\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$$

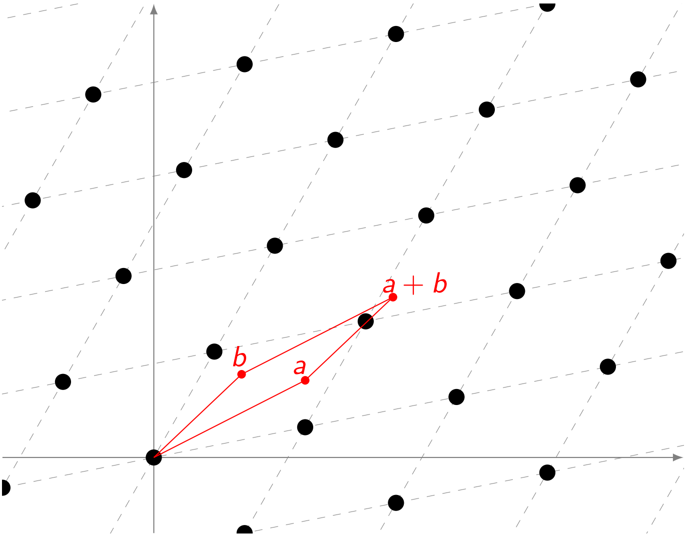
$\mathbb{C}/\Lambda$ is an elliptic curve.

Elliptic curves



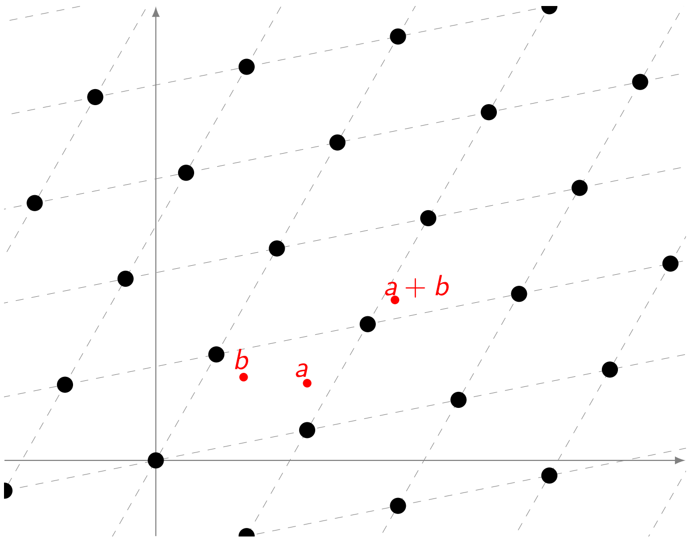
Addition law induced by addition on $\mathbb{C}$.

Elliptic curves



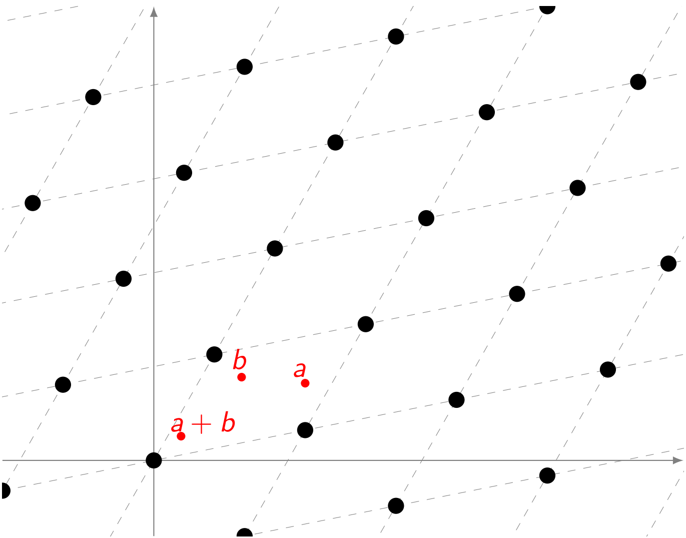
Addition law induced by addition on $\mathbb{C}$.

Elliptic curves



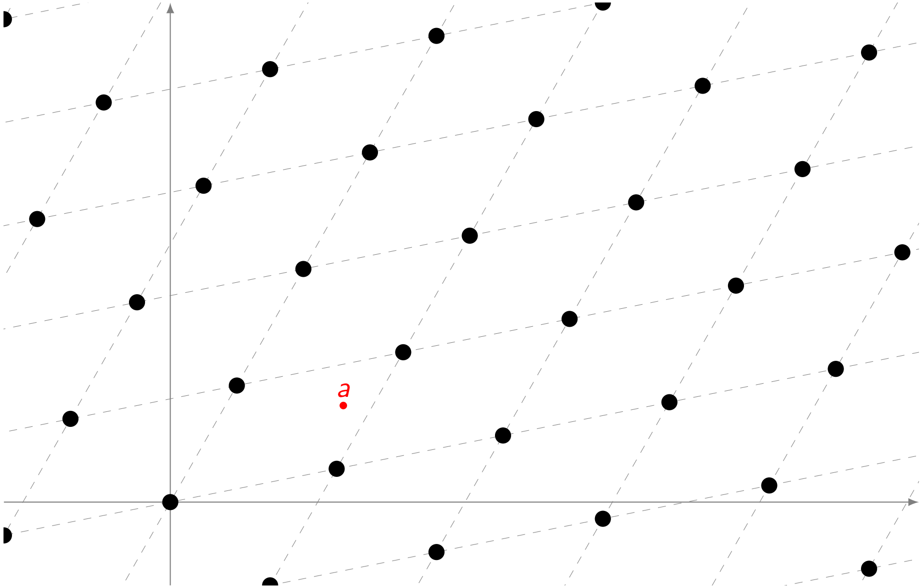
Addition law induced by addition on $\mathbb{C}$.

Elliptic curves

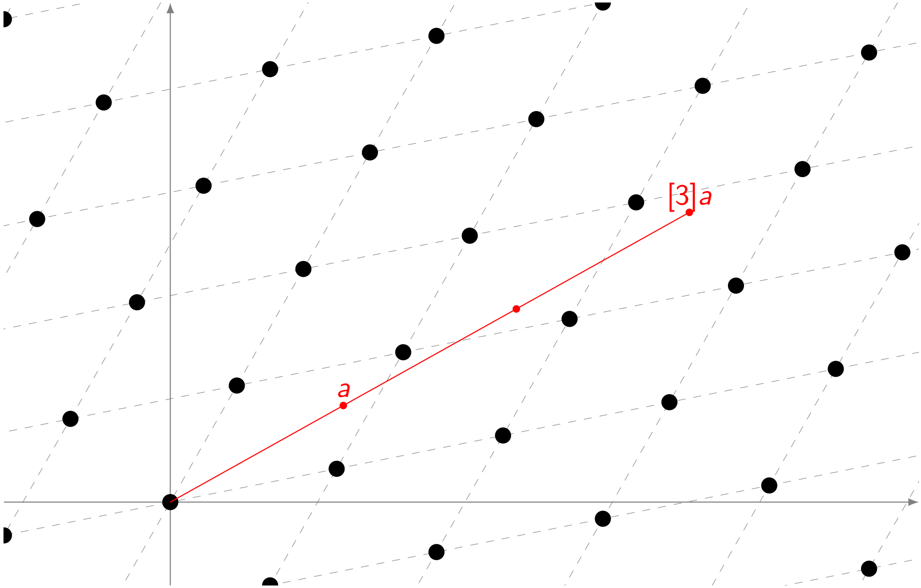


Addition law induced by addition on $\mathbb{C}$.

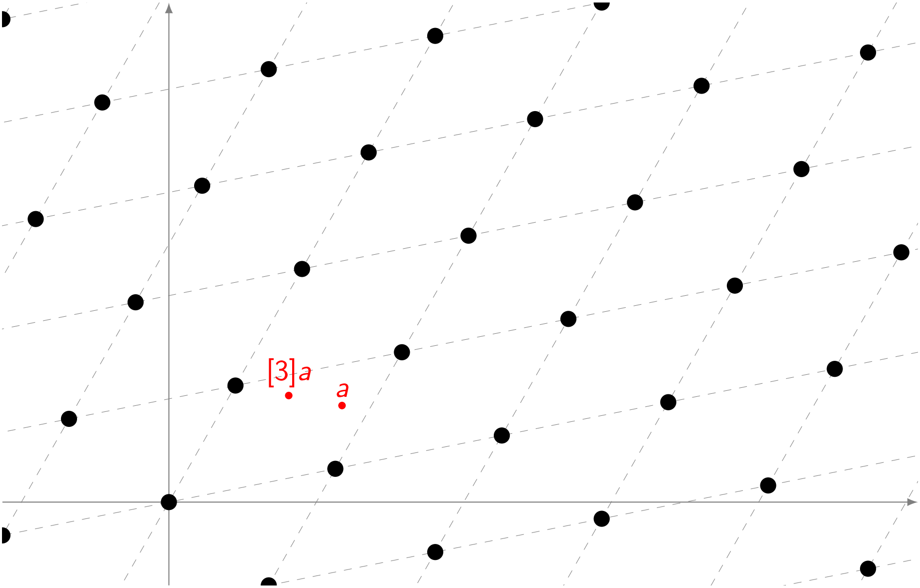
Multiplication



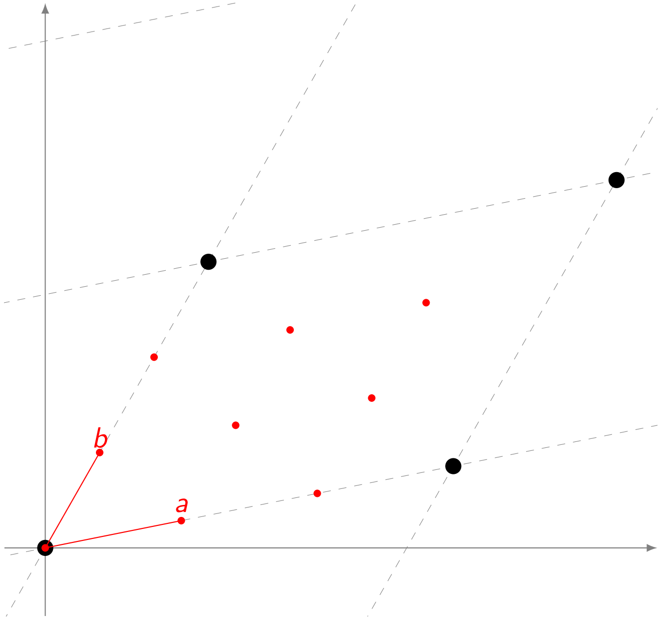
Multiplication



Multiplication



Torsion subgroups



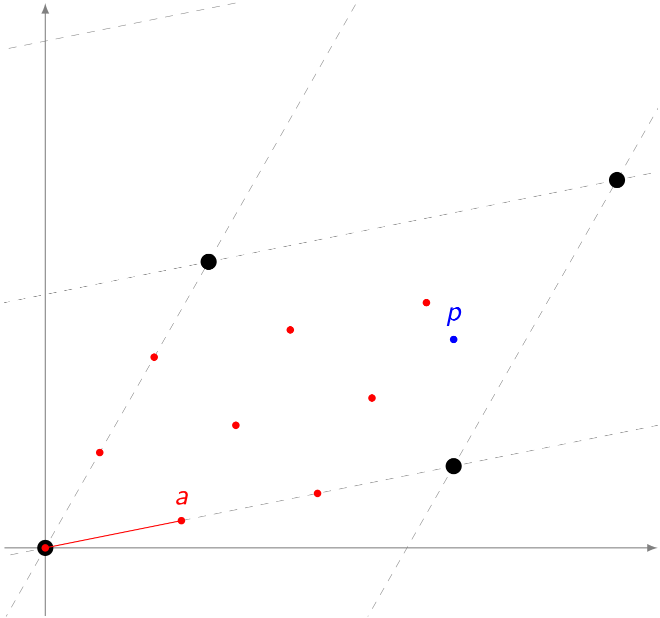
The ℓ-torsion subgroup is made up by the points

$$\left(\frac{i\omega_1}{\ell}, \frac{j\omega_2}{\ell}\right)$$

It is a group of rank two

$$E[\ell] = \langle a, b \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

Isogenies



Let $a \in \mathbb{C}/\Lambda_1$ be an ℓ-torsion point, and let

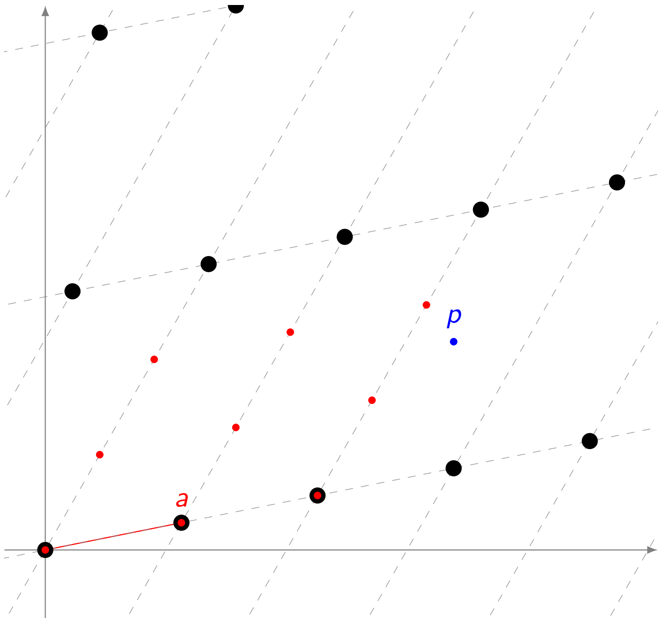
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

Then $\Lambda_1 \subset \Lambda_2$ and we define a degree ℓ cover

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

ϕ is a morphism of complex Lie groups and is called an isogeny.

Isogenies



Let $a \in \mathbb{C}/\Lambda_1$ be an ℓ-torsion point, and let

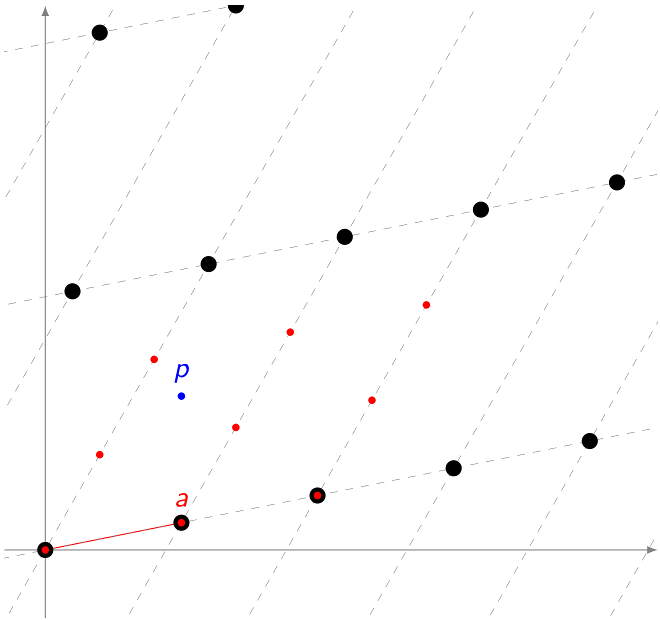
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

Then $\Lambda_1 \subset \Lambda_2$ and we define a degree ℓ cover

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

ϕ is a morphism of complex Lie groups and is called an isogeny.

Isogenies



Let $a \in \mathbb{C}/\Lambda_1$ be an ℓ-torsion point, and let

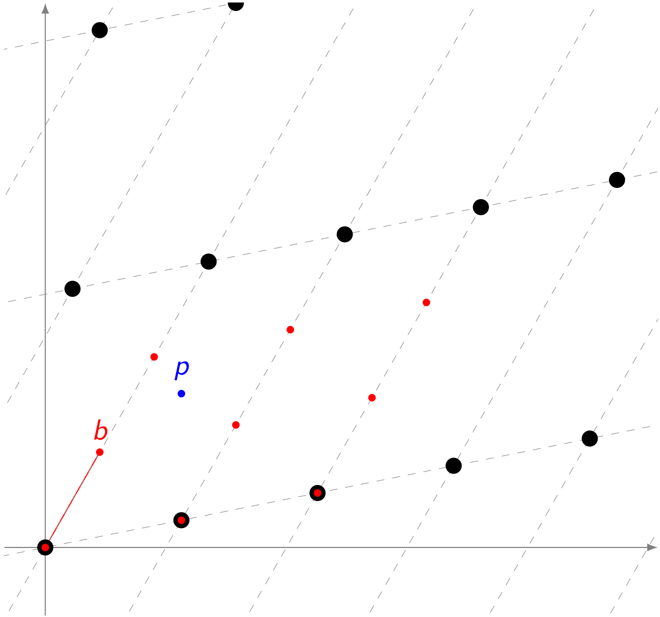
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

Then $\Lambda_1 \subset \Lambda_2$ and we define a degree ℓ cover

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

ϕ is a morphism of complex Lie groups and is called an isogeny.

Isogenies

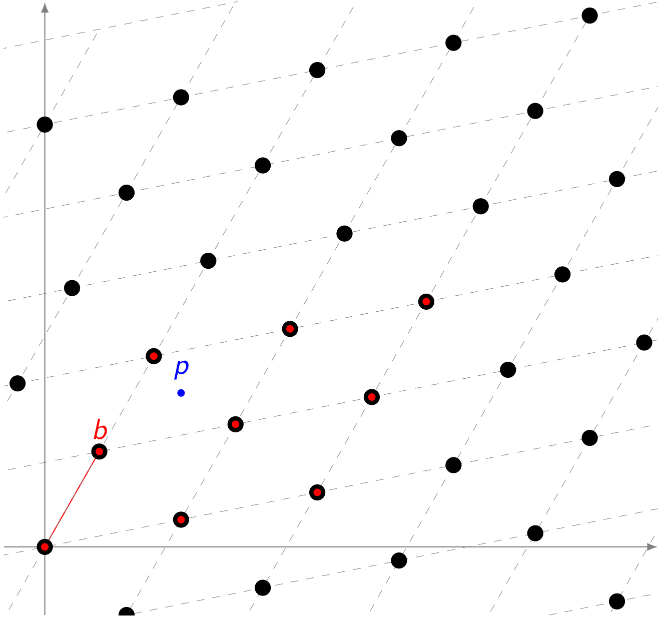


Taking a point b not in the kernel of ϕ, we obtain a new degree ℓ cover

$$\hat{\phi} : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_3$$

The composition $\hat{\phi} \circ \phi$ has degree ℓ^2 and is homothetic to the multiplication by ℓ map.
$\hat{\phi}$ is called the dual isogeny of ϕ.

Isogenies



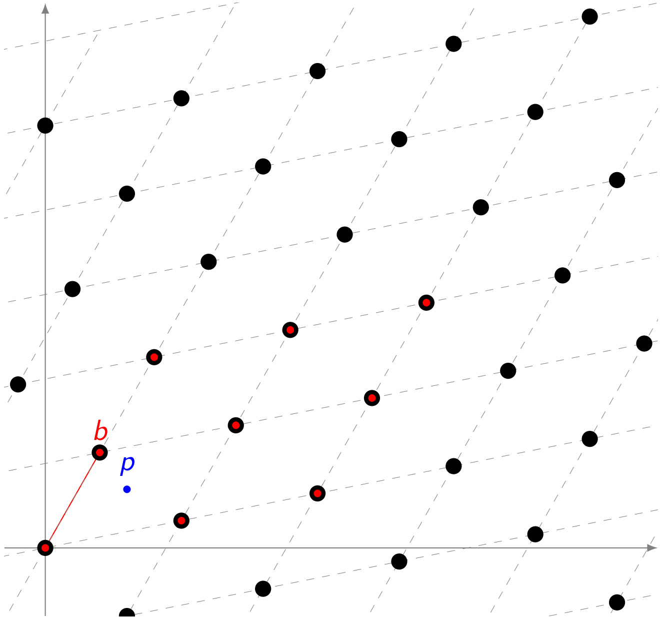
Taking a point b not in the kernel of ϕ, we obtain a new degree ℓ cover

$$\hat{\phi} : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_3$$

The composition $\hat{\phi} \circ \phi$ has degree ℓ^2 and is homothetic to the multiplication by ℓ map.

$\hat{\phi}$ is called the dual isogeny of ϕ.

Isogenies



Taking a point b not in the kernel of ϕ, we obtain a new degree ℓ cover

$$\hat{\phi} : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_3$$

The composition $\hat{\phi} \circ \phi$ has degree ℓ^2 and is homothetic to the multiplication by ℓ map.

$\hat{\phi}$ is called the dual isogeny of ϕ.

Isogenies over arbitrary fields

Isogenies are just the right notion of morphism for elliptic curves

- Surjective group morphisms.
- Algebraic maps (i.e., defined by polynomials).

(Separable) isogenies $\Leftrightarrow$ finite subgroups:

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

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.

The computational point of view

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 $P \in E(k)$.

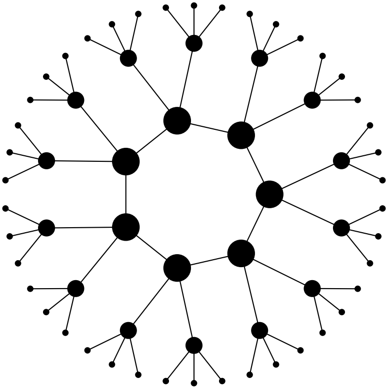
Output: The curve E/H and $\phi(P)$.

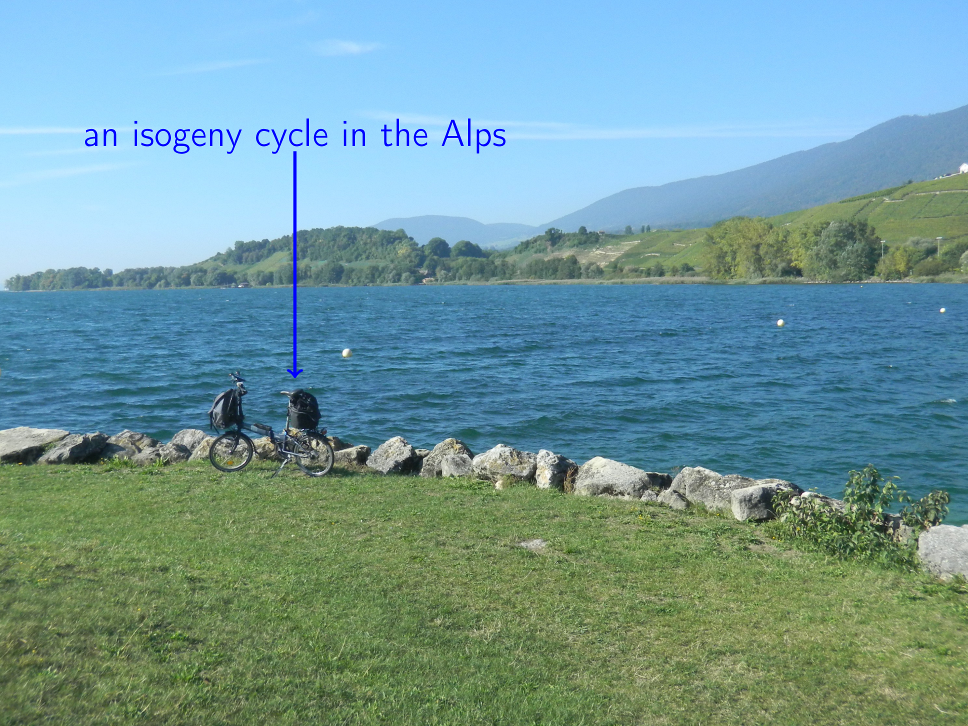
Isogeny graphs

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.




an isogeny cycle in the Alps

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.

Expander graphs

Let G be a finite undirected k-regular graph.

- k is the trivial eigenvalue of the adjacency matrix of G.
- G is called an expander if all non-trivial eigenvalues satisfy $|\lambda| \leq (1-\delta)k$.
- It is called a Ramanujan graph if $|\lambda| \leq 2\sqrt{k-1}$. This is optimal.

In practice, in an expander graph random walks of length $O(\frac{1}{\delta}\log|G|)$ land anywhere in the graph with probability distribution close to uniform.

Isogeny graphs and expansion

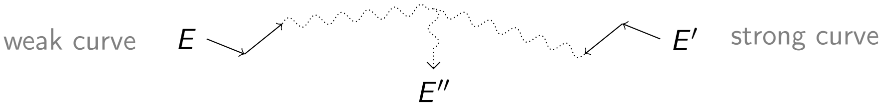
- The graph of ordinary isogenies of degree less than $(\log 4q)^B$ is an expander if $B > 2$.[a]
- The graph of supersingular isogenies of prime degree $\ell \neq p$ is Ramanujan.[b]

[a] Jao, Miller, and Venkatesan 2009.

[b] Pizer 1990, 1998.

Isogeny walks and cryptanalysis[3]

Recall: Having a weak DLP is not isogeny invariant.



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.

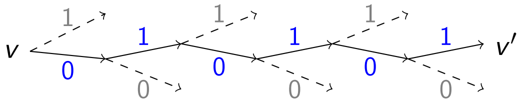
Note: Can be used to build trapdoor systems[2].

[2]Teske 2006.

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

Random walks and hash functions

Any expander graph gives rise to a hash function.



$H(010101) = v'$

- Fix a starting vertex v;
- The value to be hashed determines a random path to v';
- v' is the hash.

Provably secure hash functions

- Use the Ramanujan graph of supersingular 2-isogenies;[a]
- Collision resistance = hardness of finding cycles in the graph;
- Preimage resistance = hardness of finding a path from v to v'.

[a] Charles, K. E. Lauter, and Goren 2009.

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* char $k = 0$*),*

ordinary case (complex multiplication): *an imaginary quadratic field,*

supersingular case: *a quaternion algebra (only possible if* 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

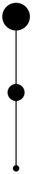
Theorem (Serre-Tate)

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

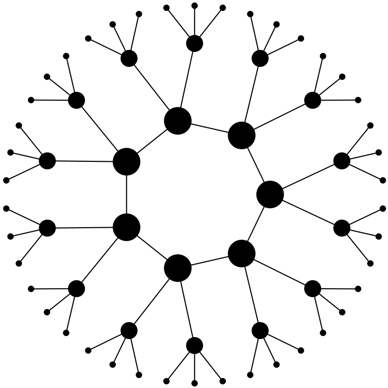
$$\mathbb{Q} \otimes \mathrm{End}(E) \simeq \mathbb{Q} \otimes \mathrm{End}(E').$$

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

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

- 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): The class group acts faithfully and transitively on the isogeny graph.

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

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.*

Post-Quantum cryptography

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.

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

DH using class groups[4]

Public data:

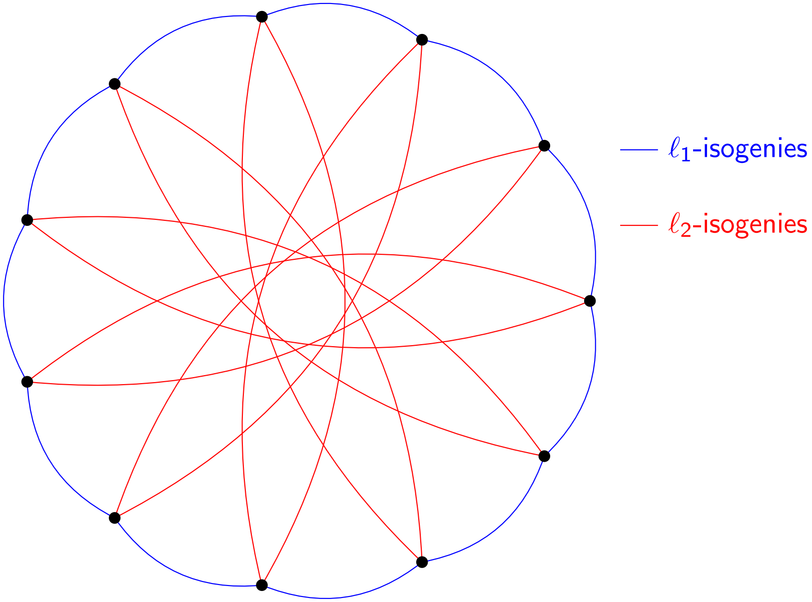
- $E/\mathbb{F}_p$ ordinary elliptic curve with complex multiplication field $\mathbb{K}$,
- primes ℓ_1,ℓ_2 not dividing $\mathrm{Disc}(E)$ and s.t. $\left(\frac{D_{\mathbb{K}}}{\ell_i}\right) = 1$.
- A *direction* on the isogeny graph (i.e. an element of the class group).

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

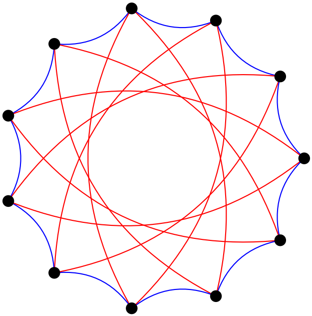
$$\begin{tikzcd}
 & E \arrow[dl, "\ell_1^{a_1}\ell_2^{a_2} = \mathcal{N}(\mathfrak{a})"'] \arrow[dr, "\mathcal{N}(\mathfrak{b}) = \ell_1^{b_1}\ell_2^{b_2}"] & \\
\mathfrak{a} * E \arrow[dr] & & \mathfrak{b} * E \arrow[dl] \\
 & \mathfrak{a}\mathfrak{b} * E = \mathfrak{b}\mathfrak{a} * E &
\end{tikzcd}$$

[4] Rostovtsev and Stolbunov 2006.

R&S key exchange



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[5]: HShP + isogeny evaluation
subexponential in the length of the walk.

[5] 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.
- 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.

R&S key exchange with supersingular curves

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 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 $\mathrm{poly}(e_A + e_B)$.

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

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

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

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

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

Our proposal: SIDH[6]

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:

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

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

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

[6] Jao and De Feo 2011.

Our proposal: SIDH[6]

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:

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

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

[6] Jao and De Feo 2011.

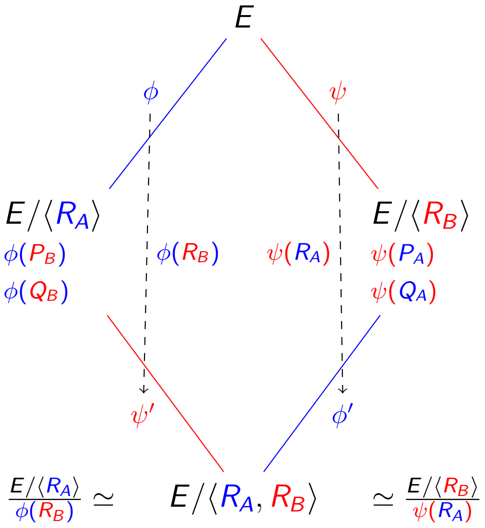
Our proposal: SIDH[6]

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:

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



[6] Jao and De Feo 2011.

Other protocols based on SIDH

Non-interactive protocols

- El-Gamal encryption.

Interactive protocols

- Zero-knowledge proofs of identity[a],
- Undeniable signatures[b],
- Strong designated verifier signatures[c],
- Authenticated encryption[d].

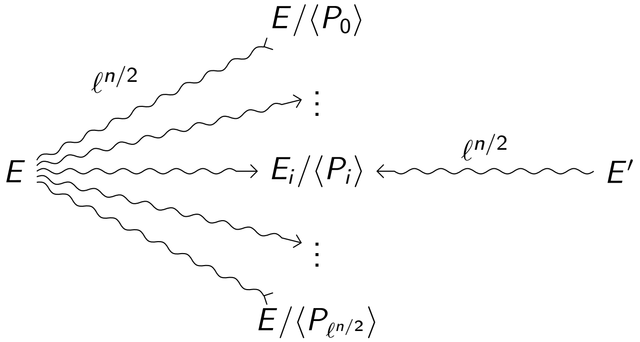
---

[a] De Feo, Jao, and Plût 2011.
[b] Jao and Soukharev 2014.
[c] Sun, Tian, and Wang 2012.
[d] Soukharev, Jao, and Seshadri 2016.

Missing: Classical signatures, ...

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[7] algorithm solves the problem in $O(\ell^{n/3})$.

[7] Tani 2008.

Other attacks

Ephemeral key recovery (total break)

Given E_0 and a public curve $E_0/\langle R\rangle$, find the kernel of the secret isogeny:

Subexponential $L_p(1/2, \sqrt{3}/2)$ when both curves are defined over $\mathbb{F}_p$.[a]

Polynomial isomorphic problem on quaternion algebras.[b]

Equivalent to computing the endomorphism rings of both E_0 and $E_0/\langle R_A\rangle$.[c]

---

[a] Biasse, Jao, and Sankar 2014.

[b] Kohel, K. Lauter, Petit, and Tignol 2014.

[c] Steven D Galbraith, Petit, Shani, and Ti 2016.

Other attacks

Other security models

Active attack against long term keys, learns the full key with (close to) optimal number of oracle queries. Countermeasures are relatively expensive.[a]

Side channel Constant-time implementation available.[b]

Attack on partially leaked keys.[a]

[a] Steven D Galbraith, Petit, Shani, and Ti 2016.
[b] Costello and Longa 2015.

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:

- Optimize arithmetic for $\mathbb{F}_p$.[a][b]
- -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: use Montgomery form.
- Avoid inversions by using *projective curve equations*.[a]
- Use $j = 0$ as starting curve.[a]

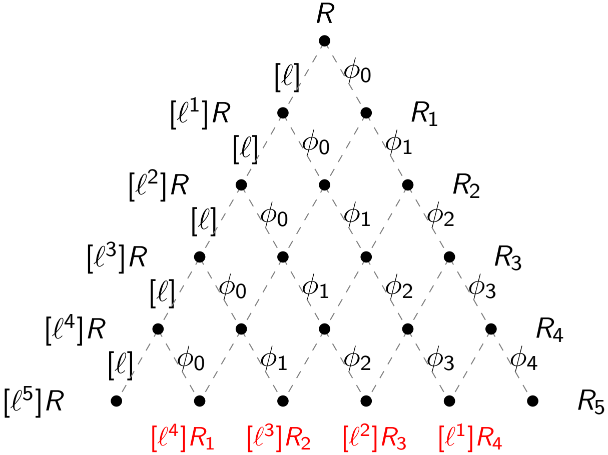
Fastest implementation[a]: 100Mcycles (Intel Haswell) @128bits quantum security level, 4512bits public key size.

[a] Costello and Longa 2015.

[b] Karmakar, Roy, Vercauteren, and Verbauwhede 2016.

Evaluating $\phi : E \to E/\langle R\rangle$ efficiently

$\mathrm{ord}(R) = \ell^a$ 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?

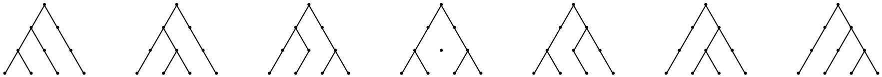


Figure: The seven well formed strategies for $e = 4$.

- 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.

A package to explore strategies:
`https://github.com/sidh-crypto/sidh-optimizer`.

References I

Kohel, David (1996).
"Endomorphism rings of elliptic curves over finite fields."
PhD thesis. University of California at Berkley.

Fouquet, Mireille and François Morain (2002).
"Isogeny Volcanoes and the SEA Algorithm."
In: Algorithmic Number Theory Symposium.
Ed. by Claus Fieker and David R. Kohel.
Vol. 2369.
Lecture Notes in Computer Science.
Berlin, Heidelberg: Springer Berlin / Heidelberg.
Chap. 23, pp. 47–62.

References II

Jao, David, Stephen D. Miller, and Ramarathnam Venkatesan (2009).
"Expander graphs based on GRH with an application to elliptic curve cryptography."
In: Journal of Number Theory 129.6,
Pp. 1491–1504.

Pizer, Arnold K. (1990).
"Ramanujan graphs and Hecke operators."
In: Bull. Amer. Math. Soc. (N.S.) 23.1.

— (1998).
"Ramanujan graphs."
In: Computational perspectives on number theory (Chicago, IL, 1995).
Vol. 7.
AMS/IP Stud. Adv. Math.
Providence, RI: Amer. Math. Soc.

References III

Teske, Edlyn (2006).
"An Elliptic Curve Trapdoor System."
In: Journal of Cryptology 19.1,
Pp. 115–133.

Galbraith, Steven D. (1999).
"Constructing Isogenies between Elliptic Curves Over Finite Fields."
In: LMS Journal of Computation and Mathematics 2,
Pp. 118–138.

Galbraith, Steven D., Florian Hess, and Nigel P. Smart (2002).
"Extending the GHS Weil descent attack."
In: Advances in cryptology—EUROCRYPT 2002 (Amsterdam).
Vol. 2332.
Lecture Notes in Comput. Sci.
Berlin: Springer,
Pp. 29–44.

References IV

Charles, Denis X., Kristin E. Lauter, and Eyal Z. Goren (2009).
"Cryptographic Hash Functions from Expander Graphs."
In: Journal of Cryptology 22.1,
Pp. 93–113.

Bisson, Gaetan and Andrew V. Sutherland (2011).
"A low-memory algorithm for finding short product representations in finite groups."
In: Designs, Codes and Cryptography 63.1,
Pp. 1–13.

Kuperberg, Greg (2005).
"A subexponential-time quantum algorithm for the dihedral hidden subgroup problem."
In: SIAM J. Comput. 35.1,
Pp. 170–188.
eprint: `quant-ph/0302112`.

References V

Regev, Oded (2004).
A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space.
arXiv: quant-ph/0406151.

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

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

References VI

Jao, David and Luca De Feo (2011).
"Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies."
In: Post-Quantum Cryptography.
Ed. by Bo-Yin Yang.
Vol. 7071.
Lecture Notes in Computer Science.
Taipei, Taiwan: Springer Berlin / Heidelberg.
Chap. 2, pp. 19–34.

De Feo, Luca, David Jao, and Jérôme Plût (2011).
Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.
URL: http://eprint.iacr.org/2011/506.

References VII

Jao, David and Vladimir Soukharev (2014).
"Isogeny-based quantum-resistant undeniable signatures."
In: International Workshop on Post-Quantum Cryptography.
Springer,
Pp. 160–179.

Sun, Xi, Haibo Tian, and Yumin Wang (2012).
"Toward quantum-resistant strong designated verifier signature from isogenies."
In: 2012 Fourth International Conference on Intelligent Networking and Collaborative Systems.

Soukharev, Vladimir, David Jao, and Srinath Seshadri (2016).
"Post-quantum security models for authenticated encryption."
In: International Workshop on Post-Quantum Cryptography.
Springer,
Pp. 64–78.

References VIII

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

Biasse, Jean-François, David Jao, and Anirudh Sankar (2014).
"A quantum algorithm for computing isogenies between supersingular elliptic curves."
In: International Conference in Cryptology in India.
Springer,
Pp. 428–442.

Kohel, David, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol (2014).
"On the quaternion-isogeny path problem."
In: LMS Journal of Computation and Mathematics 17.A,
Pp. 418–432.

References IX

Galbraith, Steven D, Christophe Petit, Barak Shani, and Yan Bo Ti (2016).
On the Security of Supersingular Isogeny Cryptosystems.
http://eprint.iacr.org/2016/859.
To appear at AsiaCrypt 2016.

Costello, Craig and Patrick Longa (2015).
"Four\ mathbb {Q}: Four-Dimensional Decompositions on a\ mathbb {Q}-curve over the Mersenne Prime."
In: International Conference on the Theory and Application of Cryptology and Information Security.
Springer,
Pp. 214–235.

References X

Karmakar, Angshuman, Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede (2016).
"Efficient Finite Field Multiplication for Isogeny Based Post Quantum Cryptography."
In: Proceedings of WAIFI 2016.