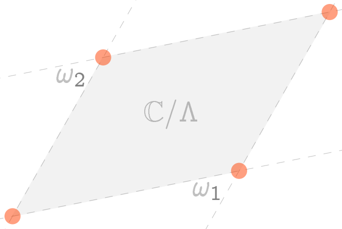
# Open problems in isogeny-based cryptography


**Luca De Feo**

**Université de Versailles & Inria, Université Paris-Saclay**

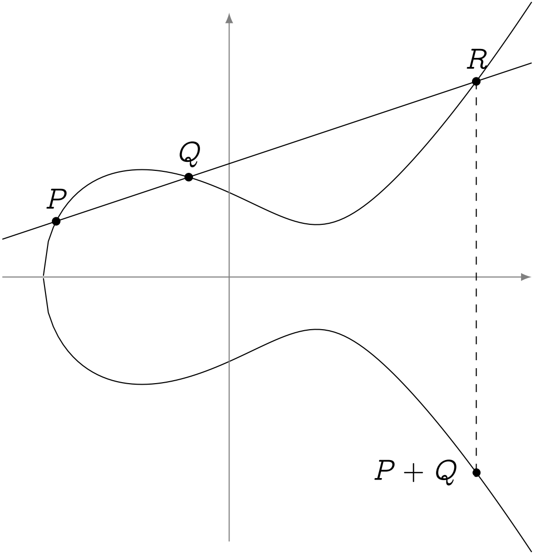

**September 11, 2017, Arithmétique en Plat Pays, Lille**



# Overview

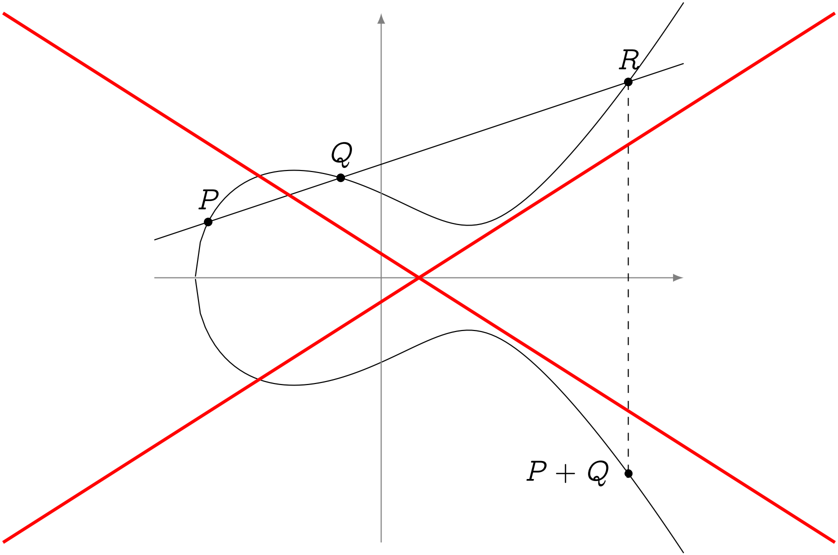
# Elliptic curves

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

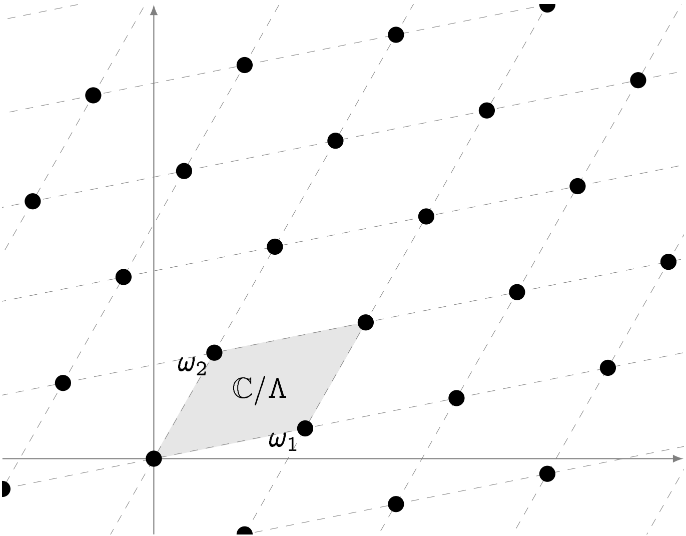


# Elliptic curves

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



# Elliptic curves

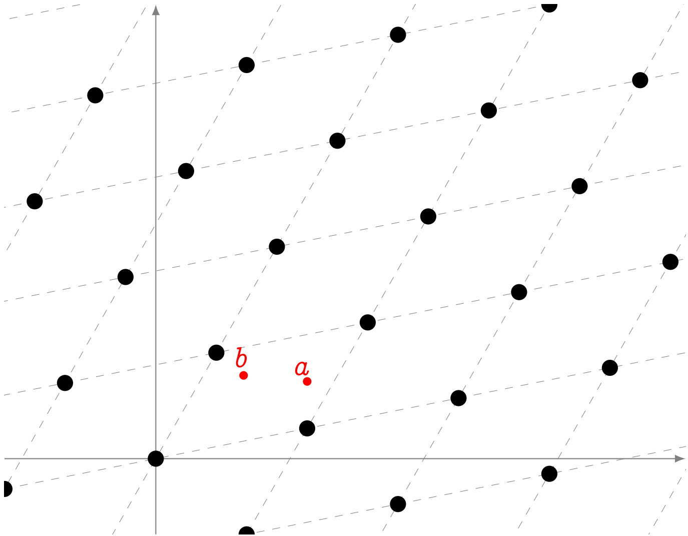



Let $\omega_1, \omega_2 \in \mathbb{C}$ be linearly independent complex numbers. Set

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

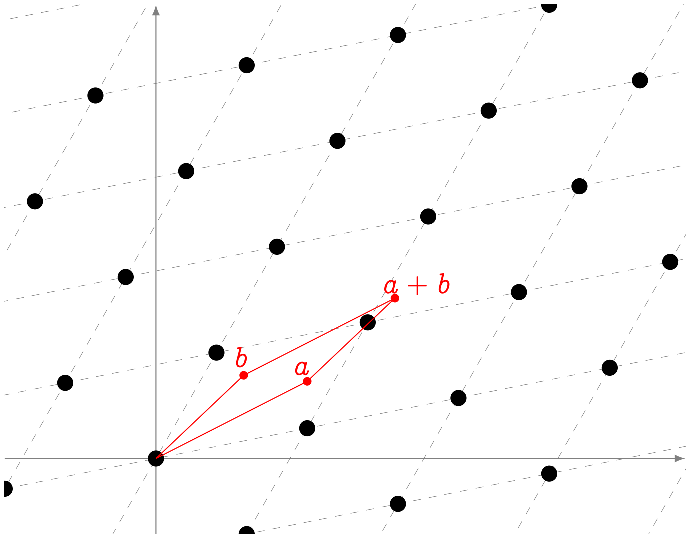
$\mathbb{C}/\Lambda$ is an elliptic curve.

# Elliptic curves



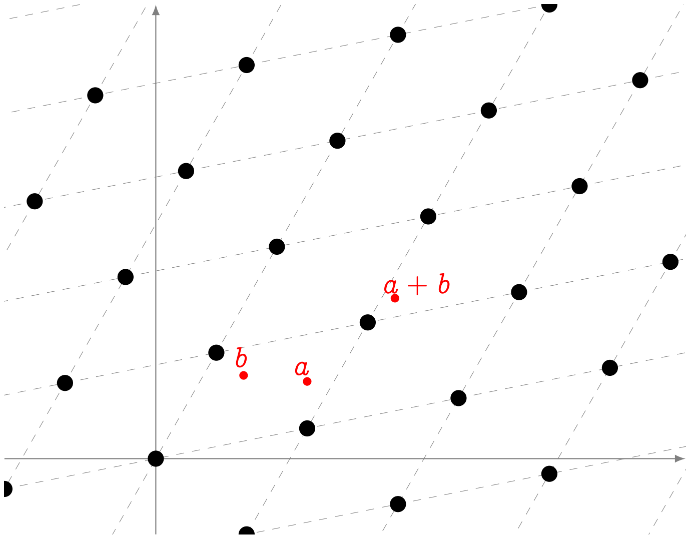

Addition law induced by addition on $\mathbb{C}$.

# Elliptic curves



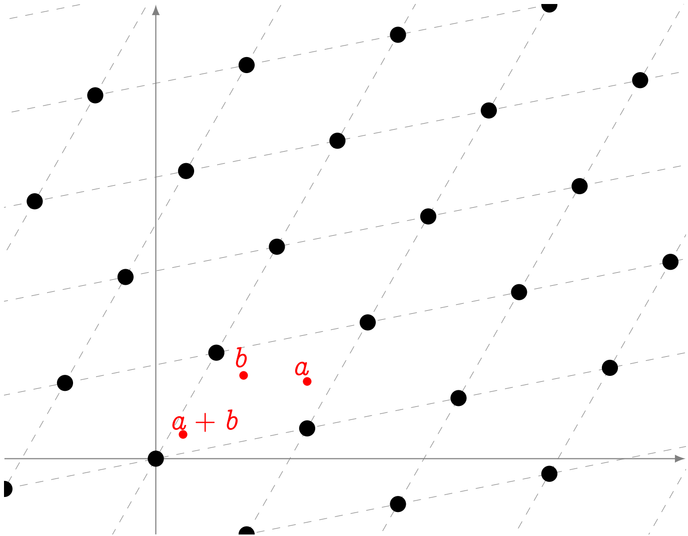

Addition law induced by addition on $\mathbb{C}$.

# Elliptic curves



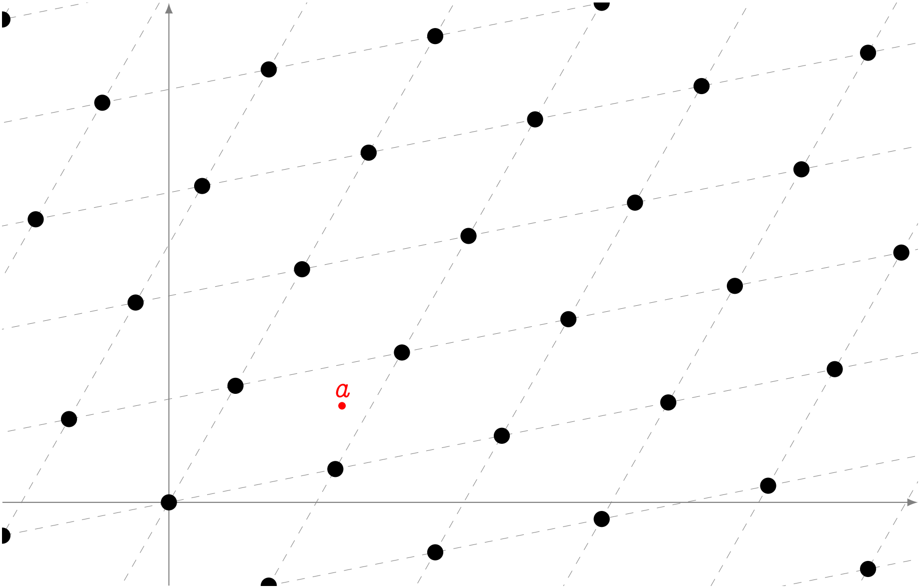

Addition law induced by addition on $\mathbb{C}$.

# Elliptic curves

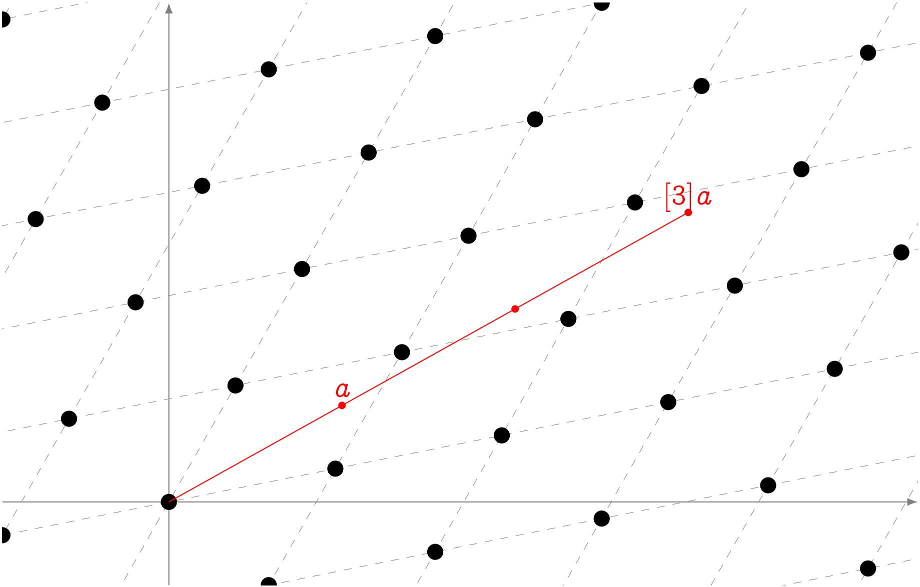



Addition law induced by addition on $\mathbb{C}$.

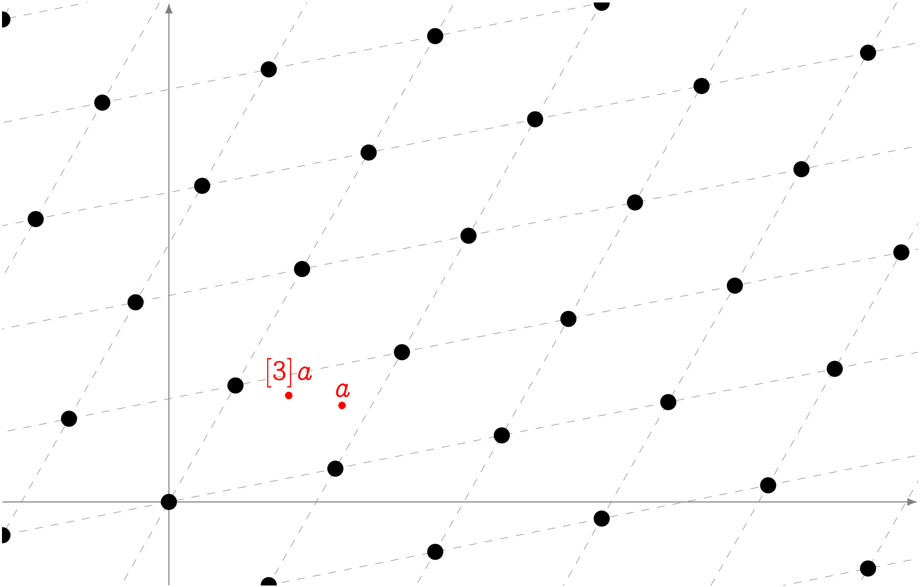
# Multiplication



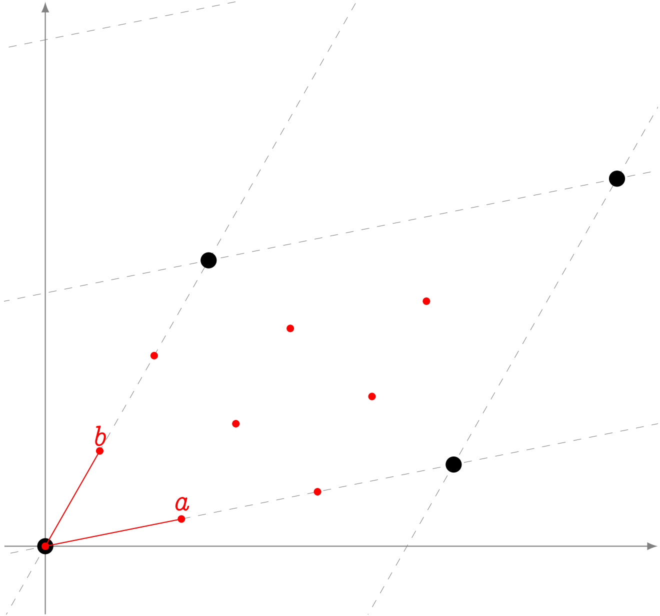
# Multiplication



# Multiplication



# Torsion subgroups



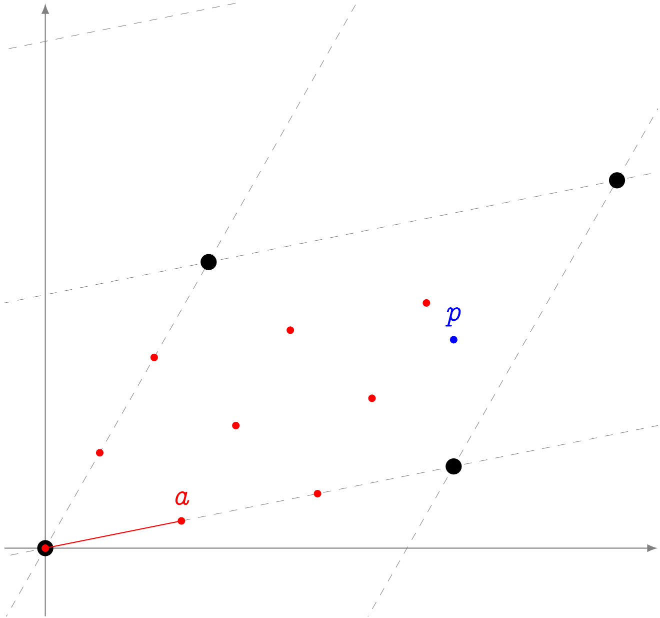

The $\ell$-torsion subgroup is made up by the points

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

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 $\ell$-torsion point, and let

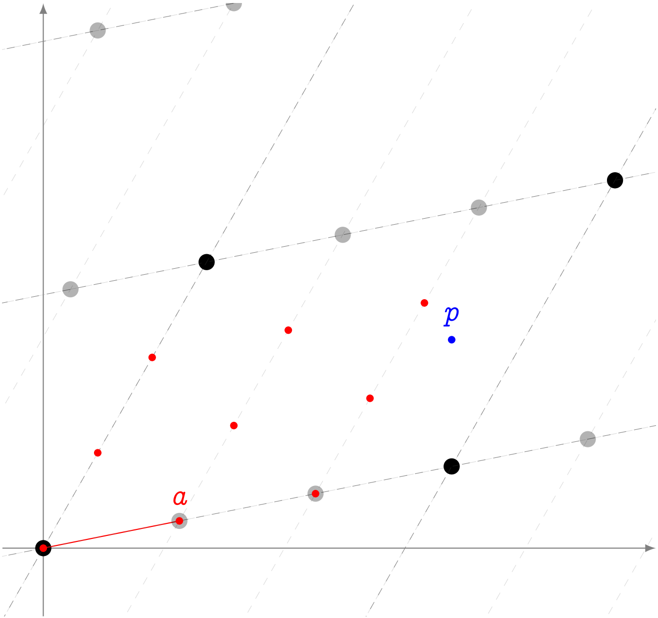
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

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

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

$\phi$ is a morphism of complex Lie groups and is called an isogeny.

# Isogenies




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

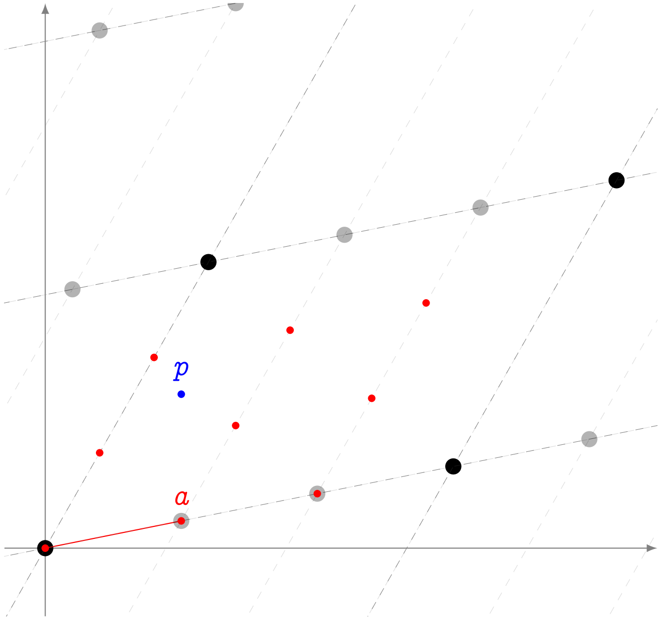
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

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

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

$\phi$ is a morphism of complex Lie groups and is called an isogeny.

# Isogenies




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

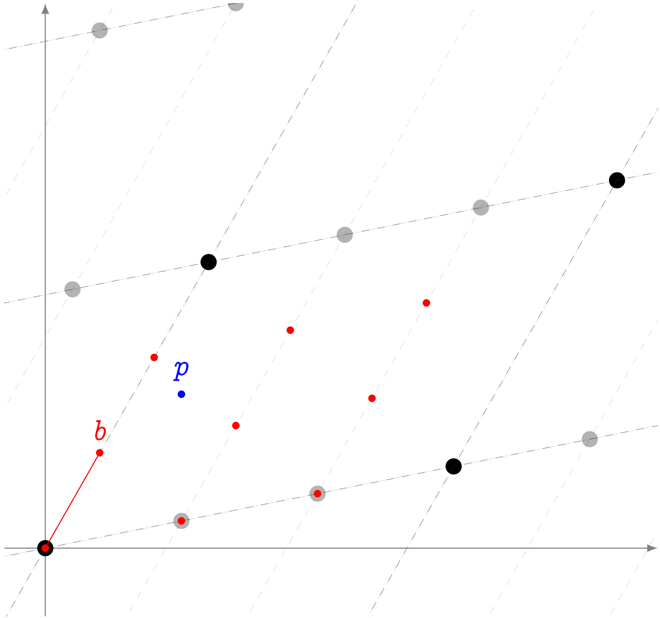
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

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

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

$\phi$ is a morphism of complex Lie groups and is called an isogeny.

# Isogenies



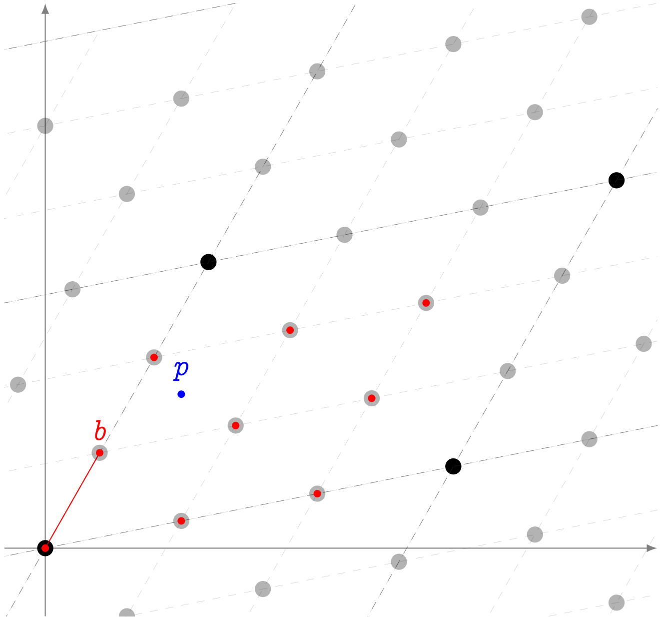

Taking a point $b$ not in the kernel of $\phi$, we obtain a new degree $\ell$ cover

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

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

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

# Isogenies



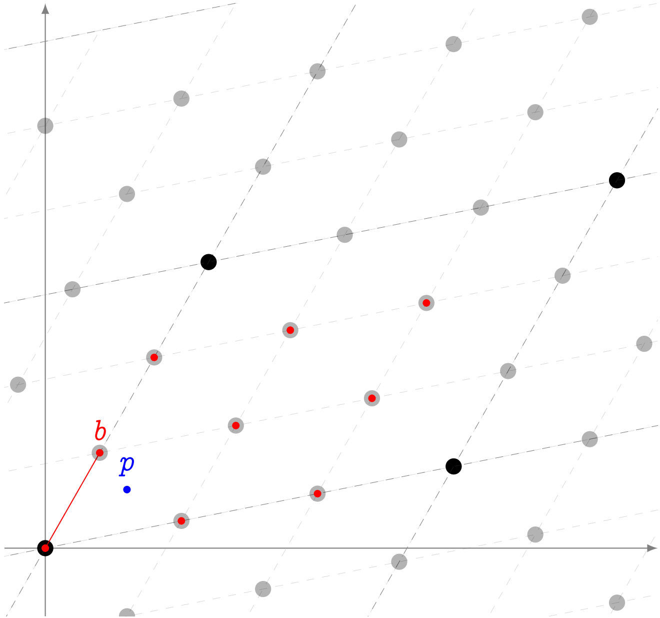

Taking a point $b$ not in the kernel of $\phi$, we obtain a new degree $\ell$ cover

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

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

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

# Isogenies




Taking a point $b$ not in the kernel of $\phi$, we obtain a new degree $\ell$ cover

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

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

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

# 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

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

## Isogeny degree

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

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

# Easy and hard problems

In practice: an isogeny $\phi$ 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 $N/D$.

Instances
- Input = kernel generator ▸ Velu's formulas; $\tilde{O}(n)$
- Input = $E$ and $E/H$
  - Elkies' algorithm[a] (and variants); $\tilde{O}(n)$
  - Couveignes' algorithm[b] (and variants). $\tilde{O}(n^2)$

Lower bound: $\Omega(n)$.

[a] Elkies 1998.

[b] Couveignes 1996.

# Easy and hard problems

## The isogeny evaluation problem

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

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

Examples
- Input = rational fraction; $O(n)$
- Input = composition of *low degree* isogenies; $\tilde{O}(\log n)$
- Input = kernel generator; $O(??)$

# Easy and hard problems

## The isogeny evaluation problem

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

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

Examples
- Input = rational fraction; $O(n)$
- Input = composition of *low degree* isogenies; $\tilde{O}(\log n)$
- Input = kernel generator; $O(??)$

**Exponential separation...**

# Easy and hard problems

## The isogeny evaluation problem

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

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

**Examples**

- Input = rational fraction; $O(n)$
- Input = composition of *low degree* isogenies; $\tilde{O}(\log n)$
- Input = kernel generator; $O(??)$

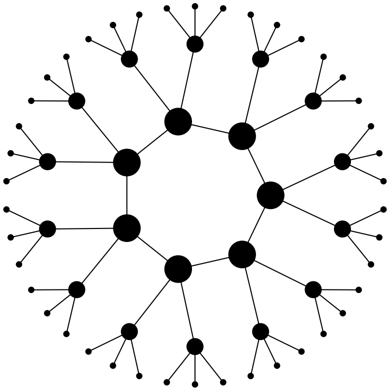
**Exponential separation...Crypto happens!**

# Isogeny graphs

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

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

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



# 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 (isogeny volcanoes)

- Nodes can have degree $0, 1, 2$ or $\ell + 1$.
  - For $\sim 50\%$ of the primes $\ell$, graphs are just isolated points;
  - For other $\sim 50\%$, graphs are 2-regular;
  - other cases only happen for finitely many $\ell$'s.

### Supersingular case

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

[1] Deuring 1941; Kohel 1996; Fouquet and Morain 2002.

# Expander graphs from isogenies

## Expander graphs

An infinite family of connected $k$-regular graphs on $n$ vertices is an expander family if there exists an $\epsilon > 0$ such that all non-trivial eigenvalues satisfy $|\lambda| \leq (1-\epsilon)k$ for $n$ large enough.

- Expander graphs have short diameter ($O(\log n)$);
- Random walks mix rapidly (after $O(\log n)$ steps, the induced distribution on the vertices is close to uniform).

**Supersingular** Let $\ell$ be fixed, the graphs of all supersingular curves with $\ell$-isogenies are expanders;[2]

**Ordinary*** Let $\mathcal{O} \subset \mathbb{Q}[\sqrt{-D}]$ be an order in a quadratic imaginary field. The graphs of all curves over $\mathbb{F}_q$ with complex multiplication by $\mathcal{O}$, with isogenies of prime degree bounded by $(\log q)^{2+\delta}$, are expanders.[3]

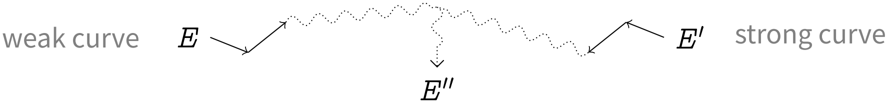
*(may contain traces of GRH)

[2] Pizer 1990, 1998.

[3] Jao, Miller, and Venkatesan 2009.

# Isogeny walks and cryptanalysis[5]

(alternative) fact: Having a weak DLP is not (always) 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[4].

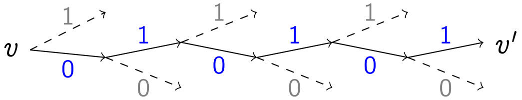
---

[4] Teske 2006.

[5] Steven D. Galbraith 1999; Steven D. Galbraith, Hess, and Smart 2002; 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.

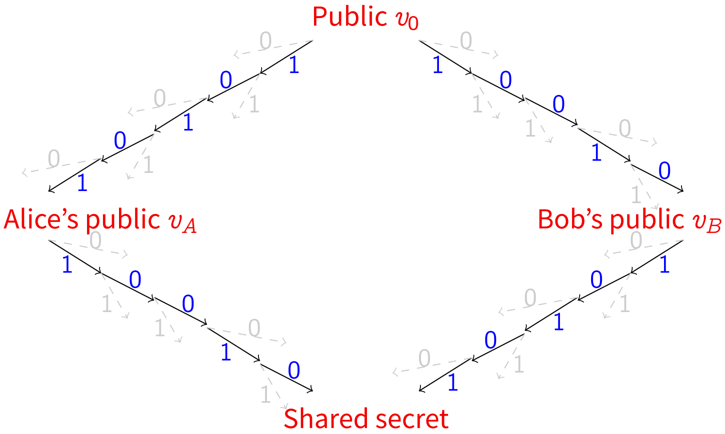
## Provably secure hash functions

- Use the expander 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 $v'$.
- Partly broken, known weak instances.[b]

[a] Charles, K. E. Lauter, and Goren 2009.
[b] Kohel, K. Lauter, Petit, and Tignol 2014.

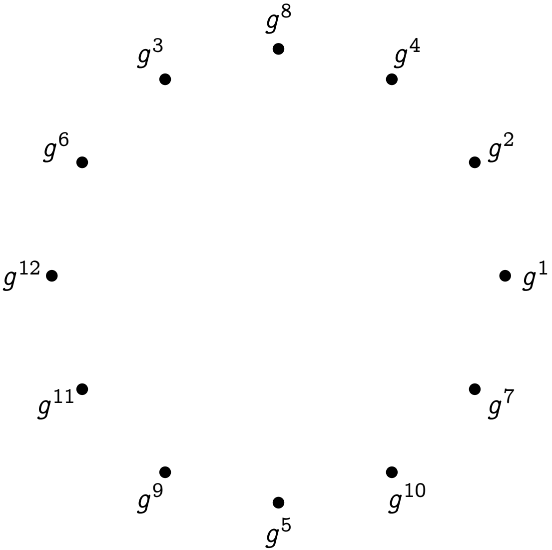
# Random walks and key exchange

Let's try something harder...



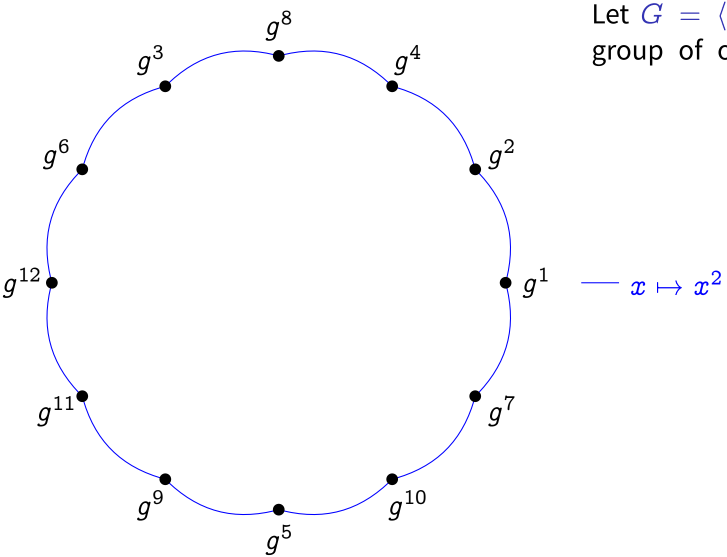

...is this even possible?

# Expander graphs from groups



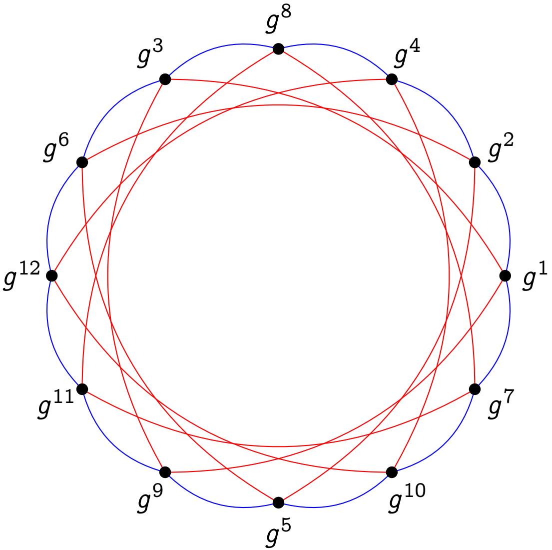

Let $G = \langle g \rangle$ be a cyclic group of order $p$.

# Expander graphs from groups

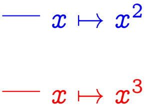



Let $G = \langle g \rangle$ be a cyclic group of order $p$.

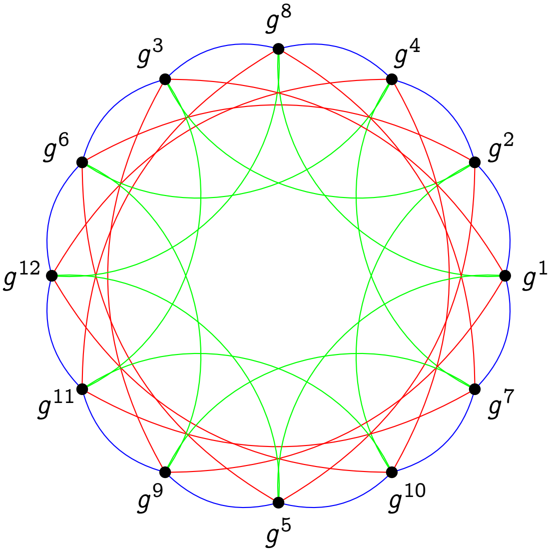
# Expander graphs from groups




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



# Expander graphs from groups



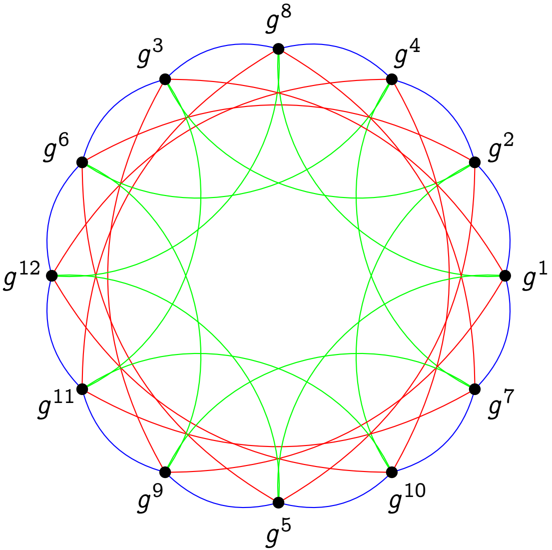

Let $G = \langle g \rangle$ be a cyclic group of order $p$.

— $x \mapsto x^2$

— $x \mapsto x^3$

— $x \mapsto x^5$

# Expander graphs from groups




Let $G = \langle g \rangle$ be a cyclic group of order $p$. Let $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$ s.t. $S^{-1} \subset S$.

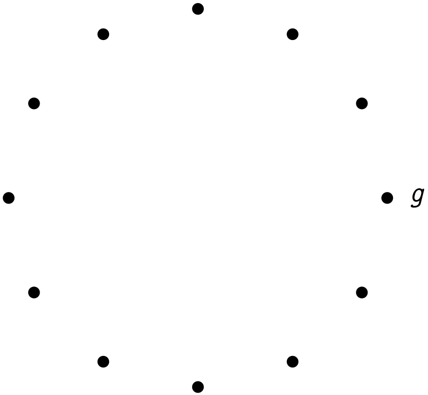
The Schreier graph of $(S, G \setminus \{1\})$ is (usually) an expander.

— $x \mapsto x^2$

— $x \mapsto x^3$

— $x \mapsto x^5$

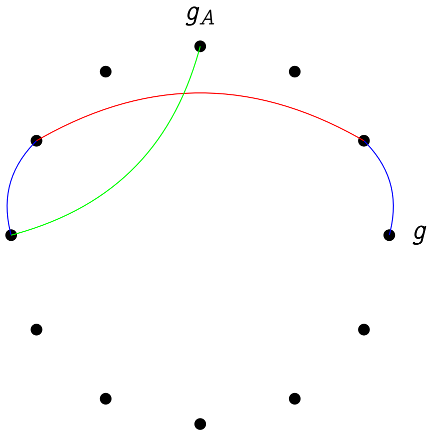
# Key exchange from Schreier graphs




**Public parameters:**

- A group $G = \langle g \rangle$ of order $p$;
- A subset $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$.

# Key exchange from Schreier graphs

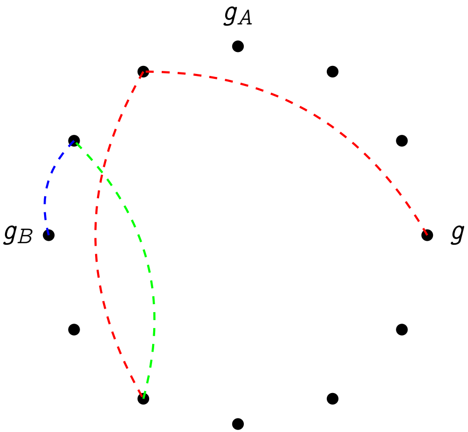



**Public parameters:**

- A group $G = \langle g \rangle$ of order $p$;
- A subset $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$.

1. **Alice** takes a secret random walk $s_A : g \to g_A$ of length $O(\log p)$;

# Key exchange from Schreier graphs

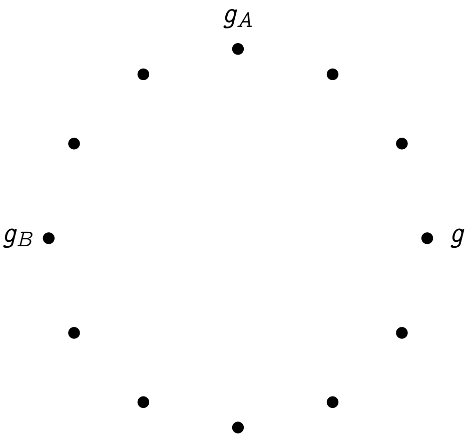



**Public parameters:**

- A group $G = \langle g \rangle$ of order $p$;
- A subset $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$.

1. **Alice** takes a secret random walk $s_A : g \to g_A$ of length $O(\log p)$;
2. **Bob** does the same;

# Key exchange from Schreier graphs

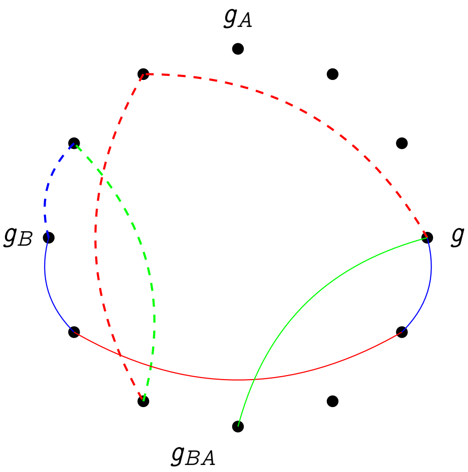



**Public parameters:**

- A group $G = \langle g \rangle$ of order $p$;
- A subset $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$.

1. **Alice** takes a secret random walk $s_A : g \to g_A$ of length $O(\log p)$;
2. **Bob** does the same;
3. They publish $g_A$ and $g_B$;

# Key exchange from Schreier graphs

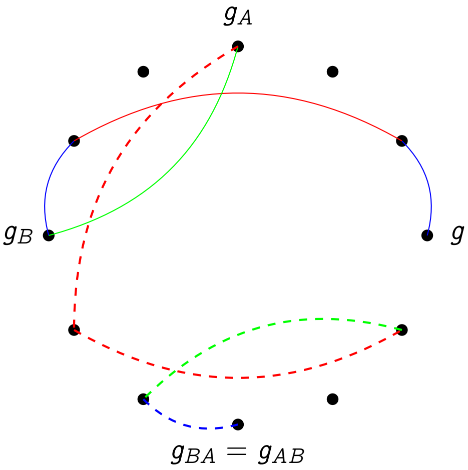



**Public parameters:**

- A group $G = \langle g \rangle$ of order $p$;
- A subset $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$.

1. **Alice** takes a secret random walk $s_A : g \to g_A$ of length $O(\log p)$;
2. **Bob** does the same;
3. They publish $g_A$ and $g_B$;
4. **Alice** repeats her secret walk $s_A$ starting from $g_B$.

# Key exchange from Schreier graphs

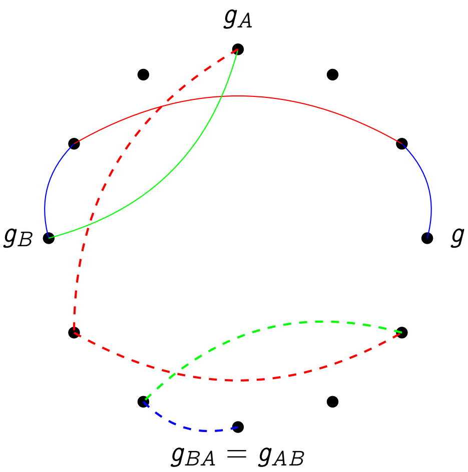



**Public parameters:**

- A group $G = \langle g \rangle$ of order $p$;
- A subset $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$.

1. **Alice** takes a secret random walk $s_A : g \to g_A$ of length $O(\log p)$;
2. **Bob** does the same;
3. They publish $g_A$ and $g_B$;
4. **Alice** repeats her secret walk $s_A$ starting from $g_B$.
5. **Bob** repeats his secret walk $s_B$ starting from $g_A$.

# Key exchange from Schreier graphs




**Why does this work?**

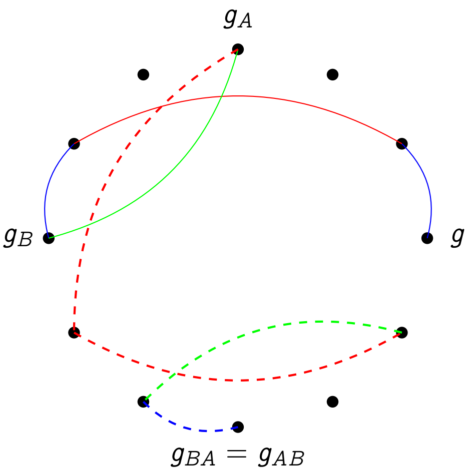
$$g_A = g^{2\cdot 3\cdot 2\cdot 5},$$

$$g_B = g^{3^2\cdot 5\cdot 2},$$

$$g_{BA} = g_{AB} = g^{2^3\cdot 3^3\cdot 5^2};$$

and $g_A$, $g_B$, $g_{AB}$ are uniformly distributed in $G$…

# Key exchange from Schreier graphs



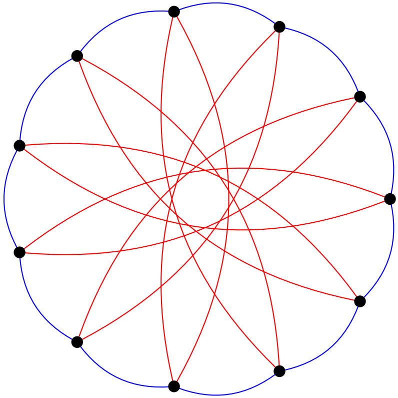

**Why does this work?**

$$g_A = g^{2\cdot 3\cdot 2\cdot 5},$$
$$g_B = g^{3^2\cdot 5\cdot 2},$$
$$g_{BA} = g_{AB} = g^{2^3\cdot 3^3\cdot 5^2};$$

and $g_A$, $g_B$, $g_{AB}$ are uniformly distributed in $G$…

…Indeed, this is just a twisted presentation of the classical Diffie-Hellman protocol!

# Group action on isogeny graphs



— $\ell_1$-isogenies

— $\ell_2$-isogenies

- There is a group action of the ideal class group $\mathrm{Cl}(\mathcal{O})$ on the set of ordinary curves with complex multiplication by $\mathcal{O}$.
- Its Schreier graph is an isogeny graph (and an expander if we take enough generators)

# Key exchange in graphs of ordinary isogenies[6]

Parameters:

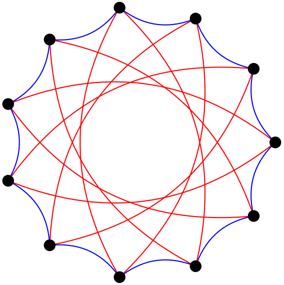
- $E/\mathbb{F}_p$ ordinary elliptic curve with *Frobenius endomorphism* $\pi$,
- primes $\ell_1$,$\ell_2$,... such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.
- A *direction* for each $\ell_i$ (i.e. an eigenvalue of $\pi$).

Secret data: Random walks $\mathfrak{a}, \mathfrak{b} \in \mathrm{Cl}(\mathcal{O})$ in the isogeny graph.

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

[6] Couveignes 2006; Rostovtsev and Stolbunov 2006.

# R&S key exchange



Key generation: compose small degree isogenies
polynomial in the length of the random walk.

Attack: find an isogeny between two curves
polynomial in the degree, exponential in the length.

Quantum[7]: QFT (hidden shift problem) + isogeny evaluation
subexponential in the length of the walk.

Open problem: Make this thing practical!

[7] Childs, Jao, and Soukharev 2010.

# 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.

Idea: Let Alice and Bob walk in two different isogeny graphs on the same vertex set.

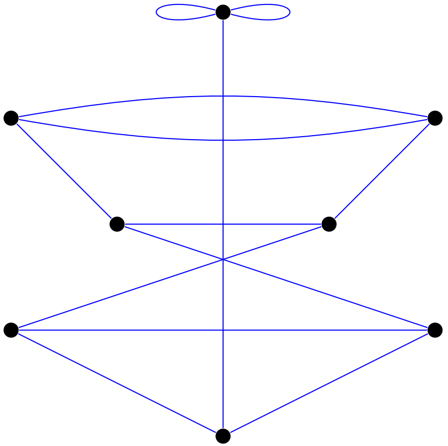


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

# 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.

Idea: Let Alice and Bob walk in two different isogeny graphs on the same vertex set.

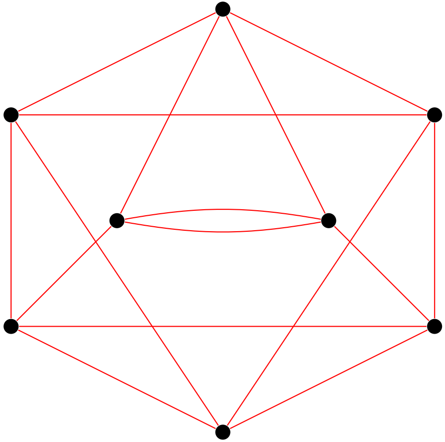


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

# 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.

**Idea:** Let Alice and Bob walk in two different isogeny graphs on the same vertex set.

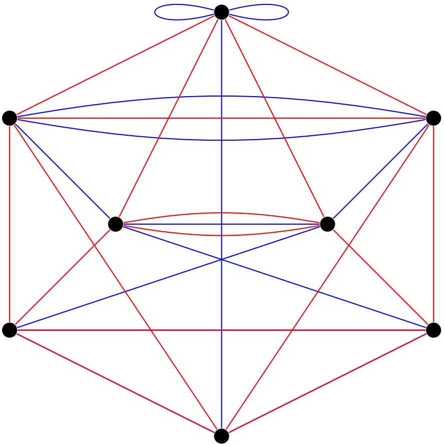


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

# Key exchange with supersingular curves

- Fix small primes $\ell_A$, $\ell_B$;
- No canonical labeling of the $\ell_A$- and $\ell_B$-isogeny graphs; however…

**Walk of length $e_A$**

$$=$$

**Isogeny of degree $\ell_A^{e_A}$**

$$=$$

**Kernel $\langle P\rangle \subset E[\ell_A^{e_A}]$**

$$\ker\phi = \langle P\rangle \subset E[\ell_A^{e_A}]$$
$$\ker\psi = \langle Q\rangle \subset E[\ell_B^{e_B}]$$
$$\ker\phi' = \langle \psi(P)\rangle$$
$$\ker\psi' = \langle \phi(Q)\rangle$$

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

# Supersingular Isogeny Diffie-Hellman[8]

**Parameters:**

- 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:**

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

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

[8] Jao and De Feo 2011; De Feo, Jao, and Plût 2014.

# Supersingular Isogeny Diffie-Hellman[8]

Parameters:

- 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:

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

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

$\phi(P_B)$ $\psi(P_A)$

$\phi(Q_B)$ $\psi(Q_A)$

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

[8] Jao and De Feo 2011; De Feo, Jao, and Plût 2014.

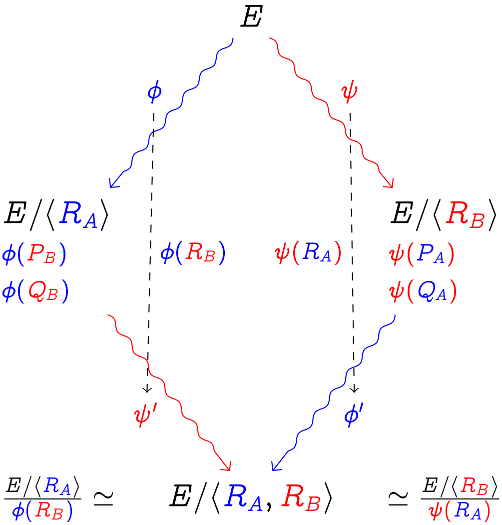
# Supersingular Isogeny Diffie-Hellman[8]

**Parameters:**

- 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:**

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




[8] Jao and De Feo 2011; De Feo, Jao, and Plût 2014.

# Performance

- For efficiency choose $p$ 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:

- Use new quasi-linear algorithm for isogeny evaluation[a].
- Optimize arithmetic for $\mathbb{F}_p$.[b,c]
- $-1$ 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*.[b]

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

[a] De Feo, Jao, and Plût 2014.
[b] Costello, Longa, and Naehrig 2016.
[c] Karmakar, Roy, Vercauteren, and Verbauwhede 2016.

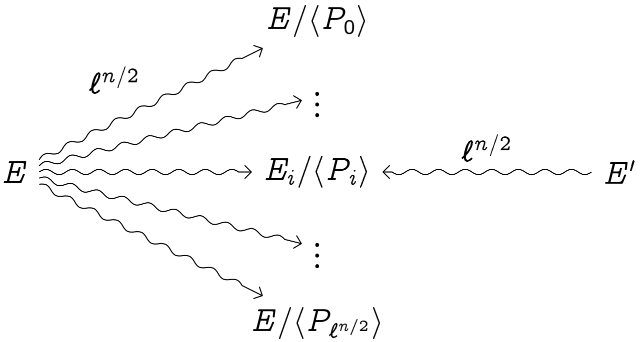
# Comparison

| | Speed | Communication |
|---|---|---|
| RSA 3072 | 4ms | 0.3KiB |
| ECDH nistp256 | 0.7ms | 0.03KiB |
| Code-based | 0.5ms | 360KiB |
| NTRU | 0.3-1.2ms | 1KiB |
| Ring-LWE | 0.2-1.5ms | 2-4KiB |
| LWE | 1.4ms | 11KiB |
| SIDH | 35-400ms | 0.5KiB |

Source: D. Stebila, *Preparing for post-quantum cryptography in TLS*

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

[9] Tani 2009.

# 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 $E_0/\langle R\rangle$.[c]

[a] Biasse, Jao, and Sankar 2014.
[b] Kohel, K. Lauter, Petit, and Tignol 2014.
[c] Steven D Galbraith, Petit, Shani, and Ti 2016.

**Open problem:** exploit the additional information transmitted by the protocol to improve attacks (classical or quantum).

# 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.[c]

---

[a] Steven D Galbraith, Petit, Shani, and Ti 2016.
[b] Costello, Longa, and Naehrig 2016.
[c] Gélin and Wesolowski 2017; Ti 2017.

**Open problem:** Create a protocol secure against active adversaries.

# Bonus: a ZK proof of knowledge[10]

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

$$E \xrightarrow{\quad\quad\phi\quad\quad} E/\langle S\rangle$$

[10] De Feo, Jao, and Plût 2014.

# Bonus: a ZK proof of knowledge[10]

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

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

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

[10] De Feo, Jao, and Plût 2014.

# Bonus: a ZK proof of knowledge[10]

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;

[10] De Feo, Jao, and Plût 2014.

# Bonus: a ZK proof of knowledge[10]

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

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

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.

[10] De Feo, Jao, and Plût 2014.

# Other protocols based on SIDH

## Non-interactive protocols

- El-Gamal encryption.

## Interactive protocols

- Signatures (using Fiat-Shamir)[a],
- Undeniable signatures[b],
- Strong designated verifier signatures[c],
- Authenticated encryption[d].

[a] Steven D Galbraith, Petit, Shani, and Ti 2016.
[b] Jao and Soukharev 2014.
[c] Sun, Tian, and Wang 2012.
[d] Soukharev, Jao, and Seshadri 2016.

**Open problem:** Efficient signatures, …

# Thank you

`http://defeo.lu/`

@luca_defeo

# References I


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

Elkies, Noam D. (1998).
"Elliptic and modular curves over finite fields and related computational issues."
In: Computational perspectives on number theory (Chicago, IL, 1995).
Vol. 7.
Studies in Advanced Mathematics.
Providence, RI: AMS International Press,
Pp. 21–76.

# References II

Couveignes, Jean-Marc (1996).
"Computing l-Isogenies Using the p-Torsion."
In: ANTS-II: Proceedings of the Second International Symposium on Algorithmic Number Theory.
London, UK: Springer-Verlag,
Pp. 59–65.

Deuring, Max (1941).
"Die Typen der Multiplikatorenringe elliptischer Funktionenkörper."
In: Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 14.1,
Pp. 197–272.

# References III


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.

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

# References IV

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

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.

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

# References V

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 VI


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.

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.

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 VII


Couveignes, Jean-Marc (2006).
Hard Homogeneous Spaces.

Rostovtsev, Alexander and Anton Stolbunov (2006).
Public-key cryptosystem based on isogenies.
http://eprint.iacr.org/2006/145/.

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

# References VIII

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 (2014).
"Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies."
In: Journal of Mathematical Cryptology 8.3,
Pp. 209–247.

# References IX


Costello, Craig, Patrick Longa, and Michael Naehrig (2016).
"Efficient Algorithms for Supersingular Isogeny Diffie-Hellman."
In: Advances in Cryptology – CRYPTO 2016: 36th Annual International Cryptology Conference.
Ed. by Matthew Robshaw and Jonathan Katz.
Springer Berlin Heidelberg,
Pp. 572–601.

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.

# References X


Tani, Seiichiro (2009).
"Claw finding algorithms using quantum walk."
In: Theoretical Computer Science 410.50,
Pp. 5285–5297.

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.

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.

# References XI


Gélin, Alexandre and Benjamin Wesolowski (2017).
"Loop-abort faults on supersingular isogeny cryptosystems."
In: to appear in PQCrypto 2017 – International Workshop on Post-Quantum Cryptography.

Ti, Yan Bo (2017).
"Fault attack on Supersingular Isogeny Cryptosystems."
In: to appear in PQCrypto 2017 – International Workshop on Post-Quantum Cryptography.

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

# References XII


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.