20 years of isogeny-based cryptography

Luca De Feo
feat. Jean Kieffer, Benjamin Smith

Université Paris Saclay, UVSQ & Inria

November 14, 2017, Elliptic Curve Cryptography, Nijmegen

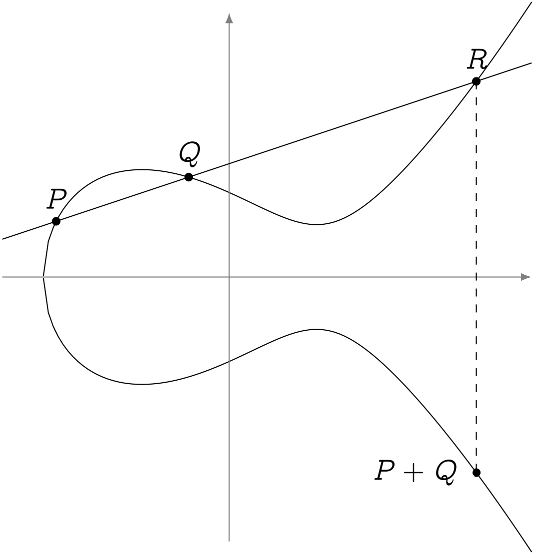
Slides online at `http://defeo.lu/docet/`

Overview

1. Isogenies
2. Isogeny graphs in cryptography
3. Recent work

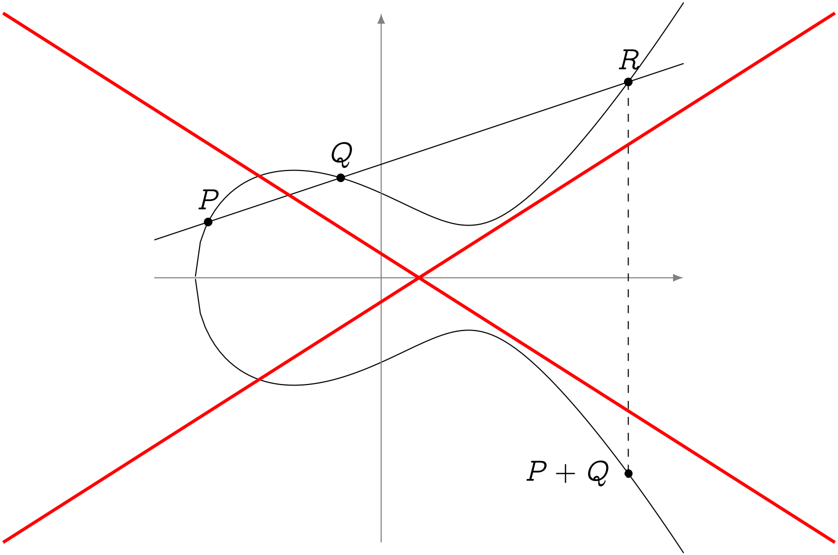
Elliptic curves

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

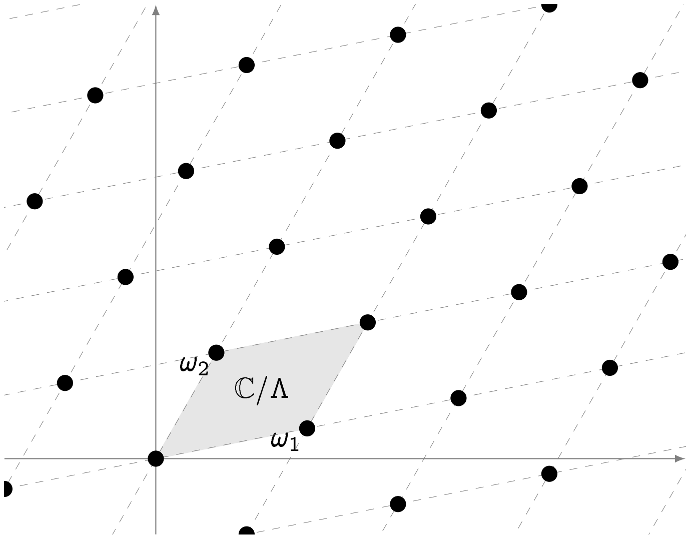


Elliptic curves

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



Elliptic curves

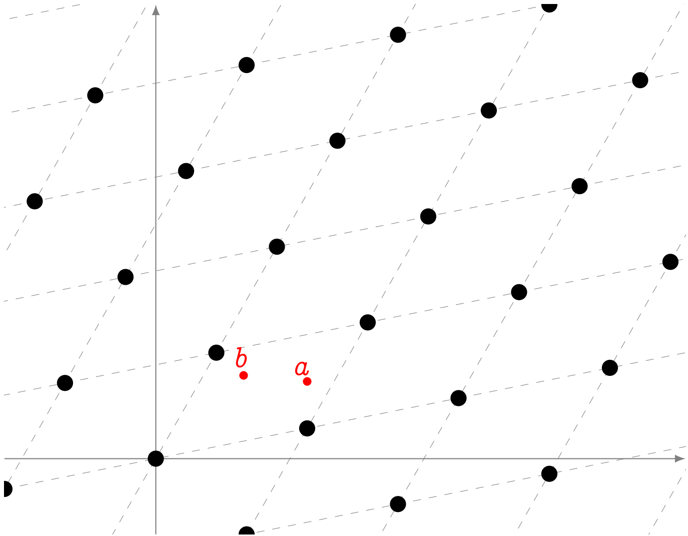


Let $\omega_1, \omega_2 \in \mathbb{C}$ be linearly independent complex numbers. Set

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

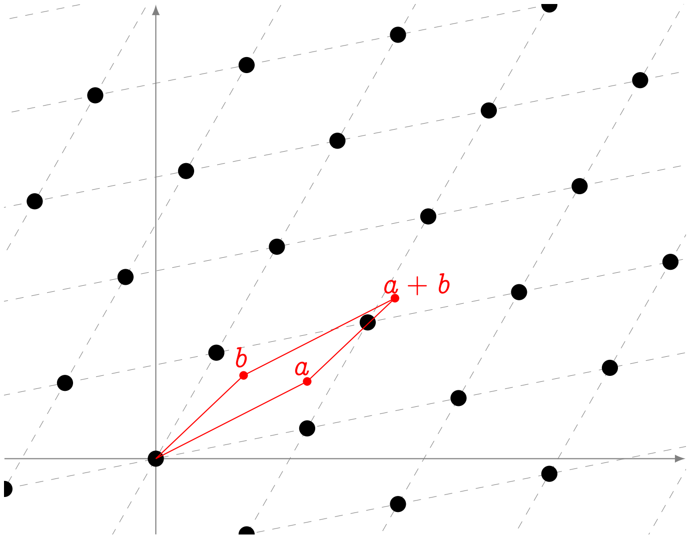
$\mathbb{C}/\Lambda$ is an elliptic curve.

Elliptic curves



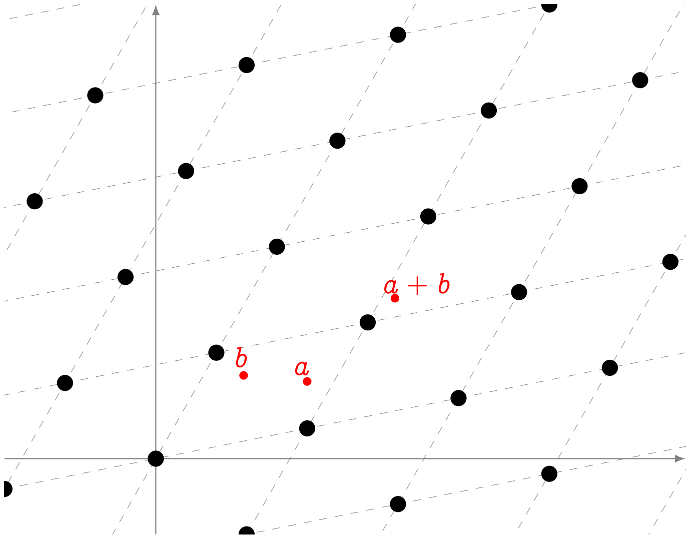
Addition law induced by addition on $\mathbb{C}$.

Elliptic curves



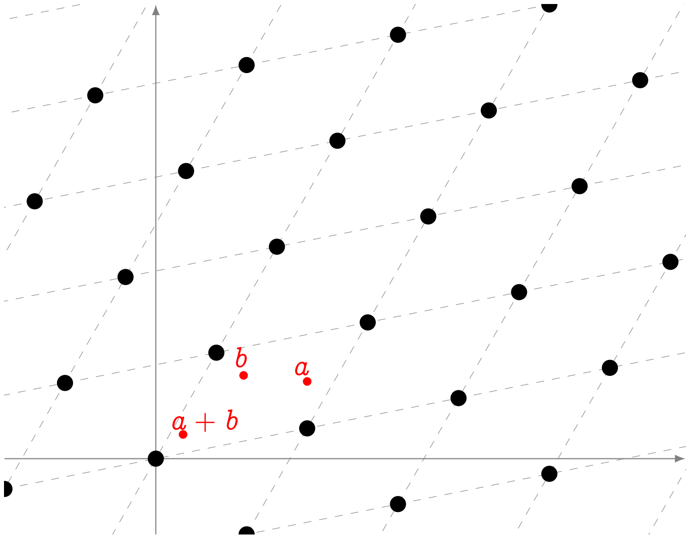
Addition law induced by addition on $\mathbb{C}$.

Elliptic curves



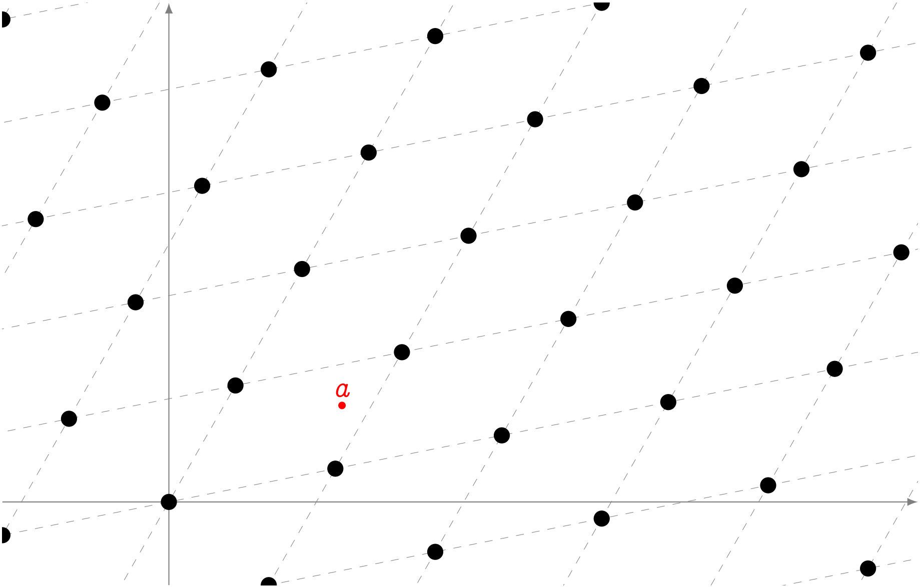
Addition law induced by addition on $\mathbb{C}$.

Elliptic curves

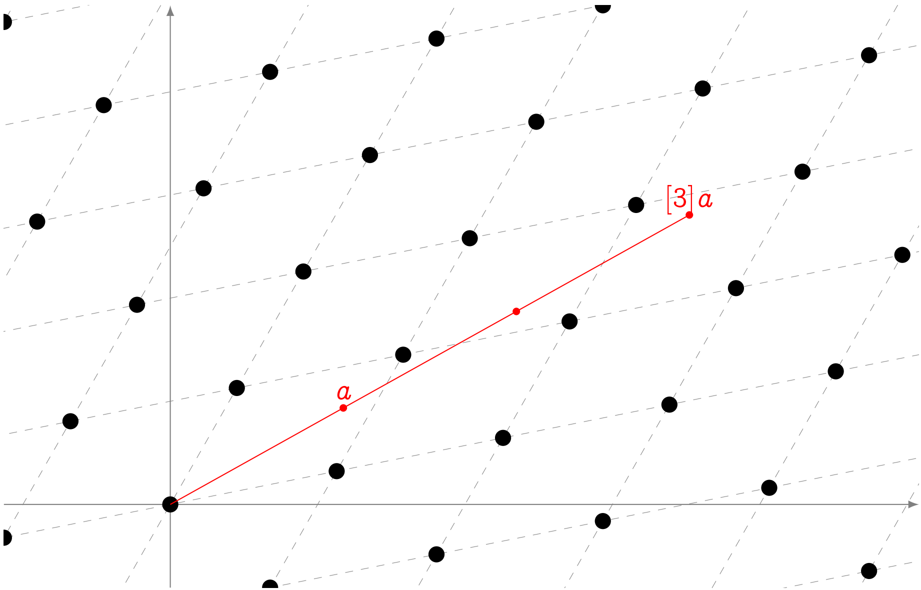


Addition law induced by addition on $\mathbb{C}$.

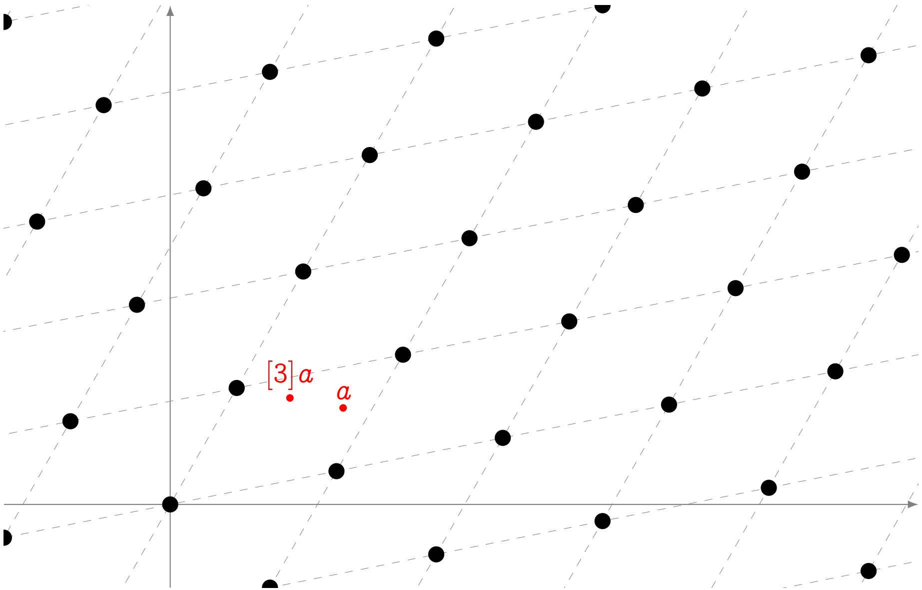
Multiplication



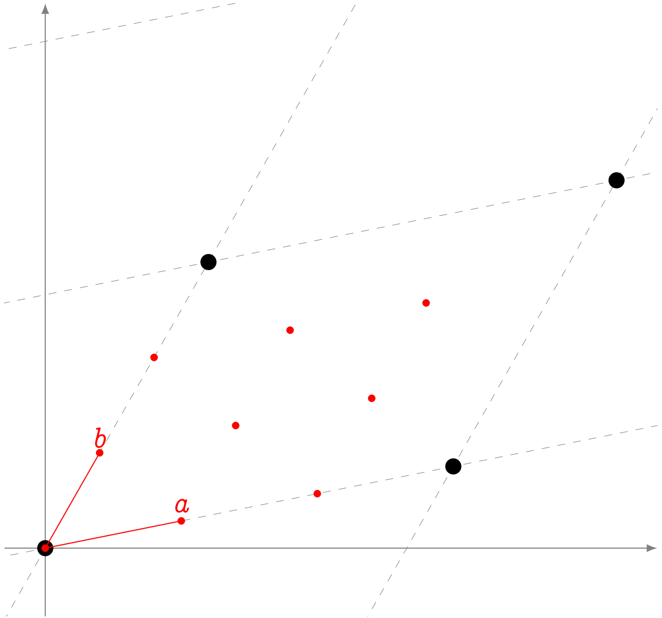
Multiplication



Multiplication



Torsion subgroups



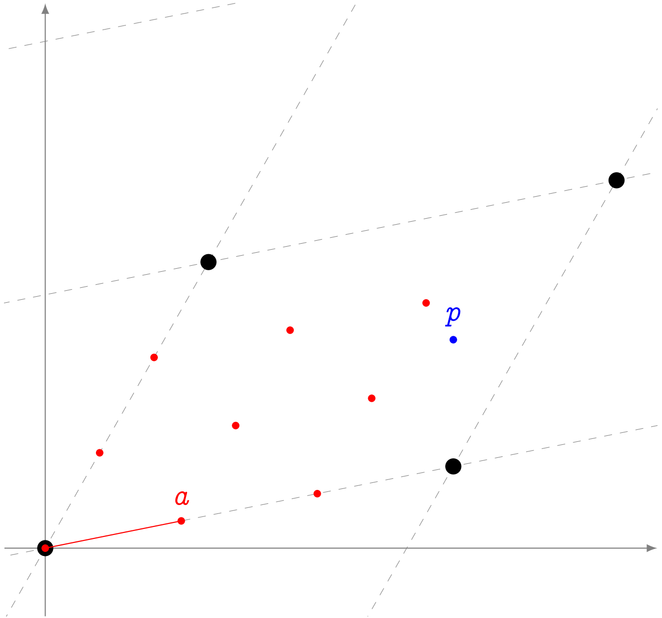
The ℓ-torsion subgroup is made up by the points

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

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

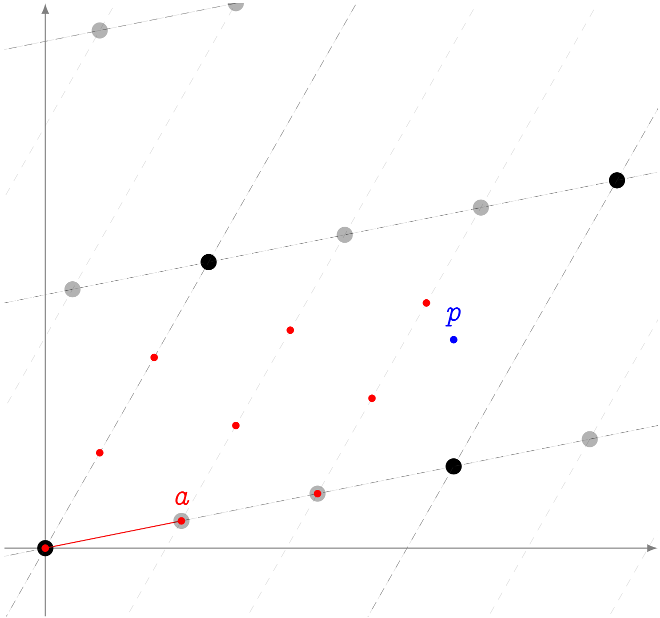
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

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

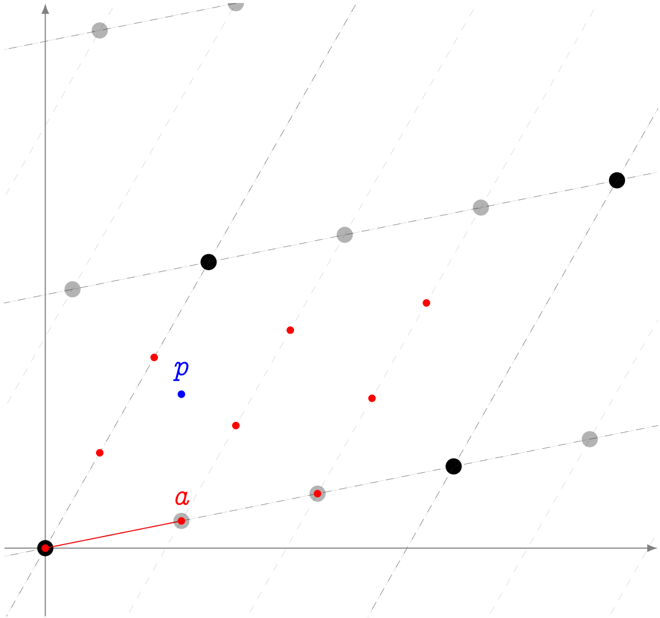
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

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

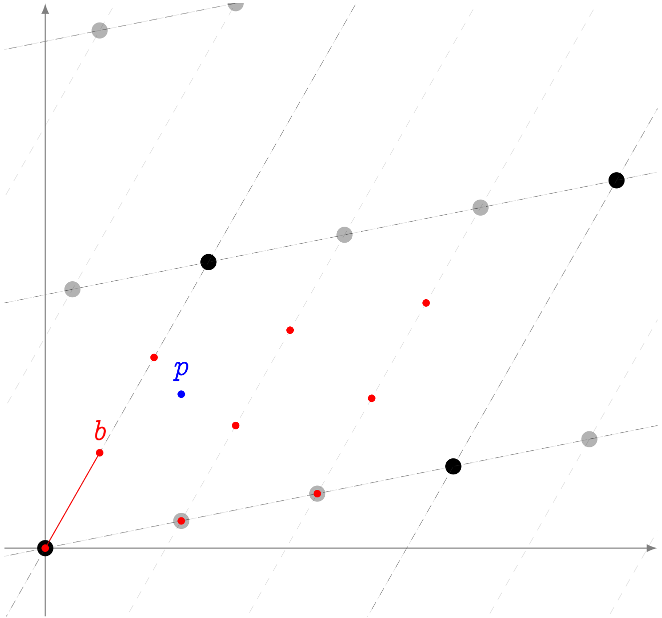
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

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



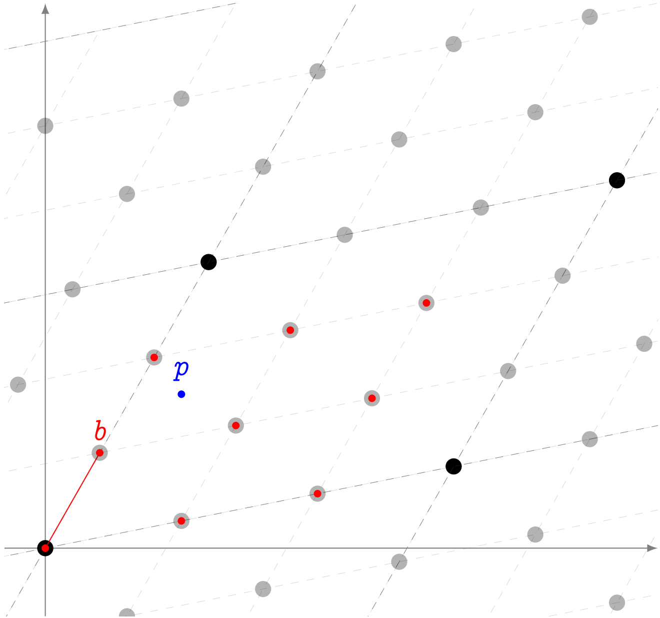
Taking a point b not in the kernel of ϕ, we obtain a new degree ℓ cover

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

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



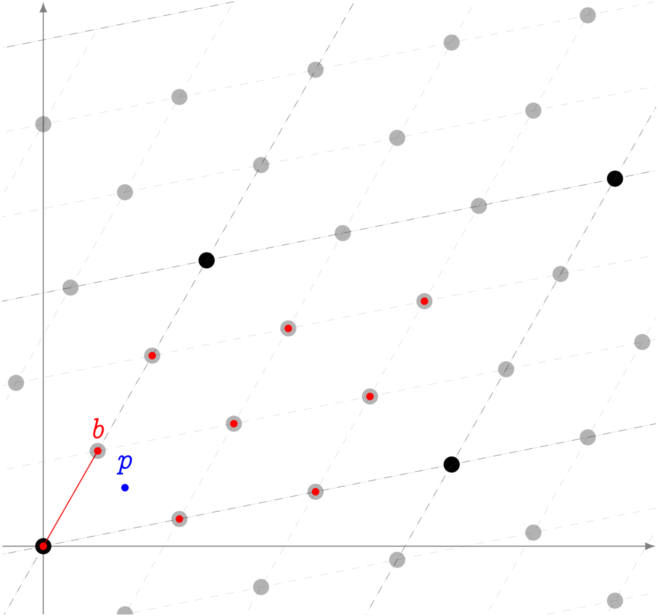
Taking a point b not in the kernel of ϕ, we obtain a new degree ℓ cover

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

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 ⇔ 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.

Easy and hard problems

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 $\ker \phi$.

Vélu's formulas $\tilde{O}(n)$

Input: A generator of the kernel H of the isogeny.

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

The explicit isogeny problem

Input: The curves E and E/H, the degree n.

Output: The rational fraction N/D.

Algorithms[a]

- Elkies' algorithm (and variants); $\tilde{O}(n)$
- Couveignes' algorithm (and variants). $\tilde{O}(n^2)$

[a] Elkies 1998; Couveignes 1996.

Easy and hard problems

Isogeny evaluation

Input: A *description* of the isogeny ϕ, 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; $\tilde{O}(\log n)$

The isogeny walk problem $O(??)$

Input: Isogenous curves E, E'.

Output: A path of low degree isogenies from E to E'.

Easy and hard problems

Isogeny evaluation

Input: A *description* of the isogeny ϕ, 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; $\tilde{O}(\log n)$

The isogeny walk problem $O(??)$

Input: Isogenous curves E, E'.

Output: A path of low degree isogenies from E to E'.

Exponential separation…

Easy and hard problems

Isogeny evaluation

Input: A *description* of the isogeny ϕ, 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; $\tilde{O}(\log n)$

The isogeny walk problem $O(??)$

Input: Isogenous curves E, E'.

Output: A path of low degree isogenies from E to E'.

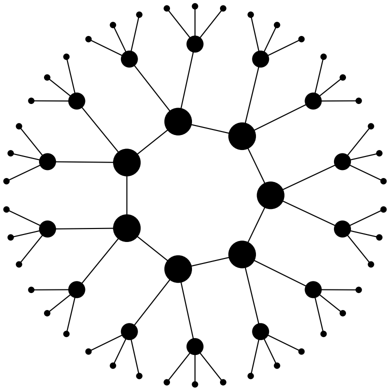
Exponential separation... Crypto happens!

Isogeny graphs

We look at 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[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 ℓ, graphs are just isolated points;
  - For other $\sim 50\%$, graphs are 2-regular;
  - other cases only happen for finitely many ℓ'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 ℓ be fixed, the graphs of all supersingular curves with ℓ-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.

The first 10 years of isogeny based cryptography

- 1996 Couveignes suggests isogeny-based key-exchange at a seminar in École Normale Supérieure;
- 1997 He submits “Hard Homogeneous Spaces” to Crypto;

The first 10 years of isogeny based cryptography

1996 Couveignes suggests isogeny-based key-exchange at a seminar in École Normale Supérieure;

1997 He submits “Hard Homogeneous Spaces” to Crypto;

1997 His paper gets rejected;

The first 10 years of isogeny based cryptography

1996 Couveignes suggests isogeny-based key-exchange at a seminar in École Normale Supérieure;

1997 He submits “Hard Homogeneous Spaces” to Crypto;

1997 His paper gets rejected;

1997–2006 …Nothing happens for about 10 years.

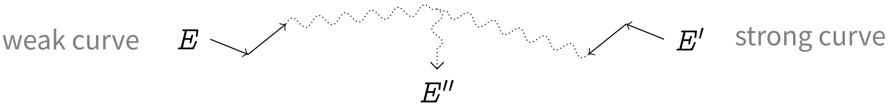
The first 10 years of isogeny based cryptography

1996	Couveignes suggests isogeny-based key-exchange at a seminar in École Normale Supérieure;
1997	He submits “Hard Homogeneous Spaces” to Crypto;
1997	His paper gets rejected;
1997–2006	…Nothing happens for about 10 years.

Ok. Let’s move on to the next 10 years!

Isogeny walks and cryptanalysis[5] (circa 2000)

(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.

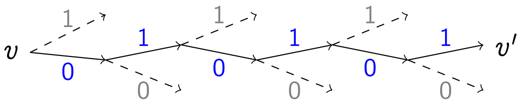
Note: Can be used to build trapdoor systems[4].

[4] Teske 2006.

[5] Galbraith 1999; Galbraith, Hess, and Smart 2002; Bisson and Sutherland 2011.

Random walks and hash functions (circa 2006)

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.

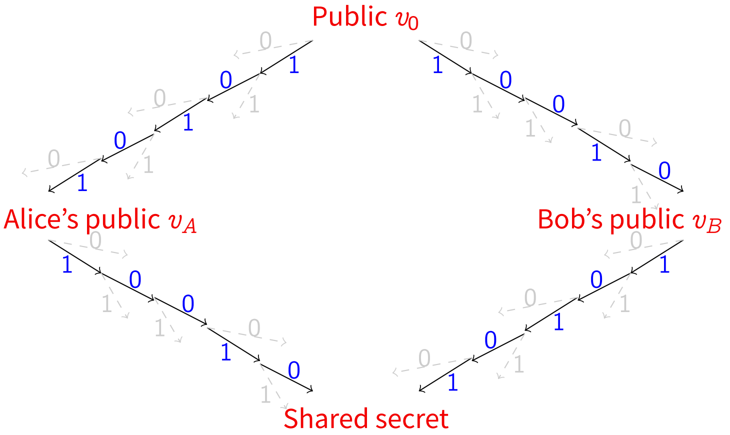
Provably secure hash functions

- 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.

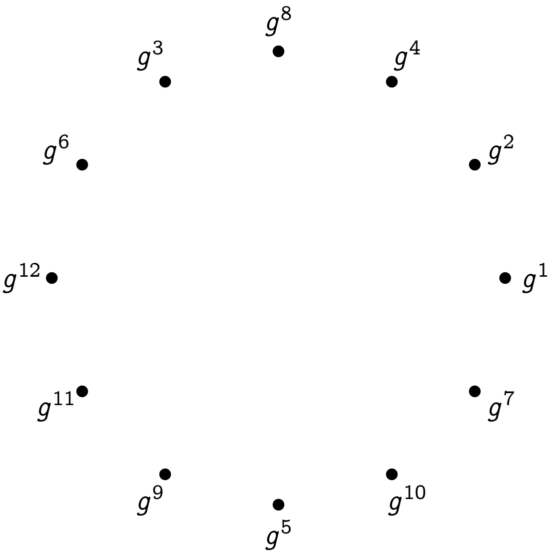
Random walks and key exchange

Let's try something harder...



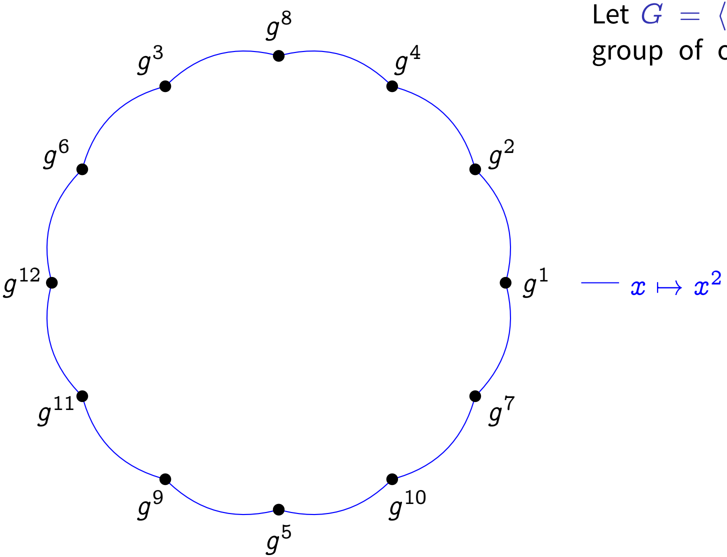
...is this even possible?

Expander graphs from groups



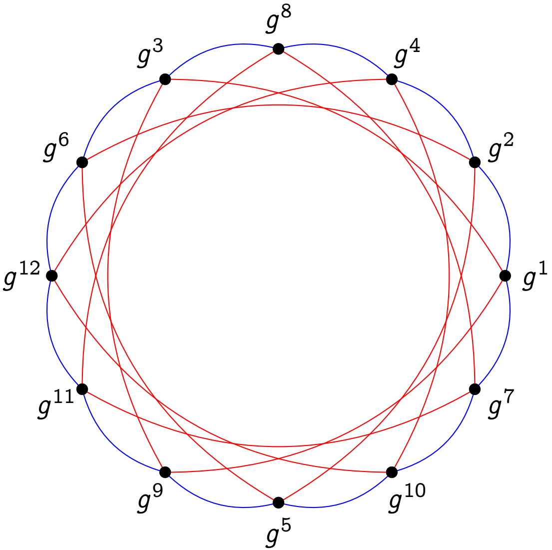
Let $G = \langle g \rangle$ be a cyclic group of order p.

Expander graphs from groups



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

Expander graphs from groups

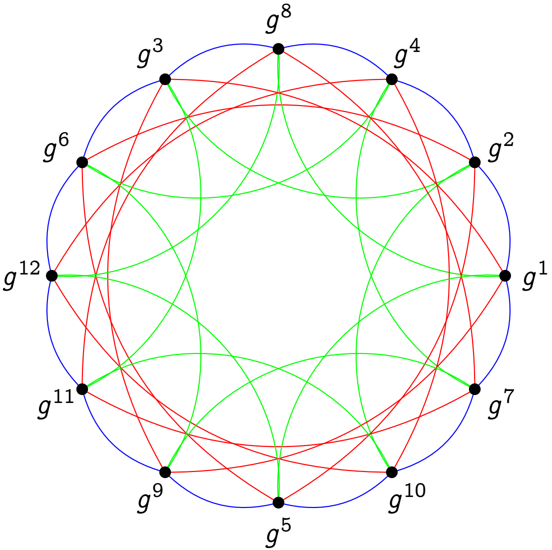


Let $G = \langle g \rangle$ be a cyclic group of order p.

— $x \mapsto x^2$

— $x \mapsto x^3$

Expander graphs from groups



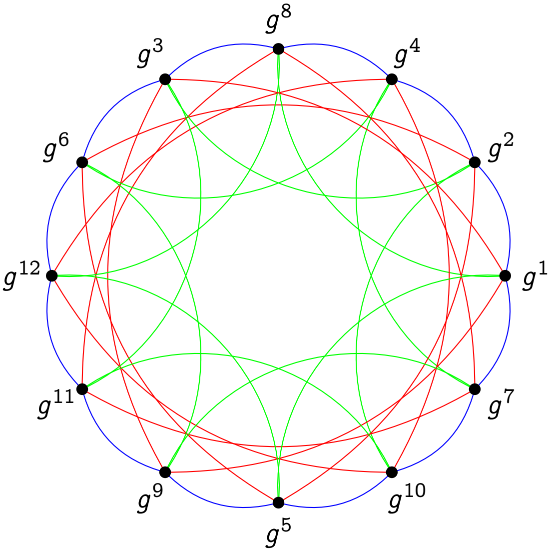
Let $G = \langle g \rangle$ be a cyclic group of order p.

— $x \mapsto x^2$

— $x \mapsto x^3$

— $x \mapsto x^5$

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. $S^{-1} \subset S$.

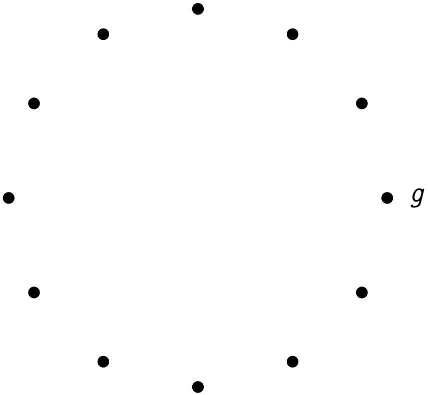
The Schreier graph of $(S, G \setminus \{1\})$ is (usually) an expander.

— $x \mapsto x^2$

— $x \mapsto x^3$

— $x \mapsto x^5$

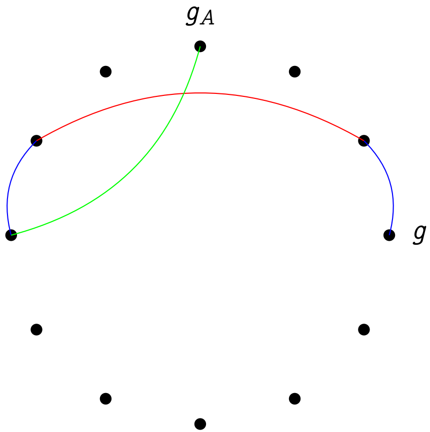
Key exchange from Schreier graphs



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

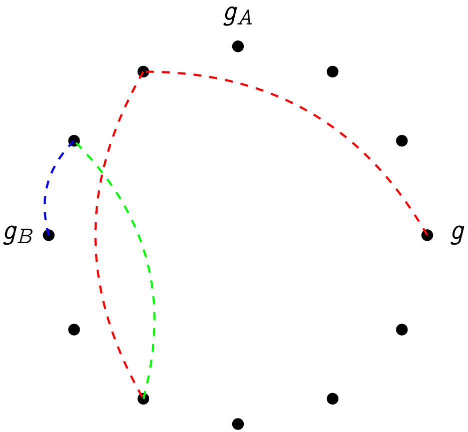


Public parameters:

- 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

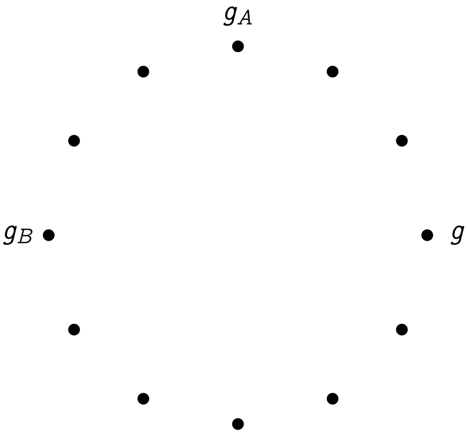


Public parameters:

- 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

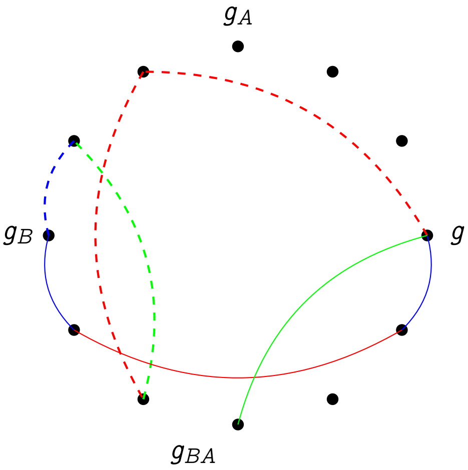


Public parameters:

- 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

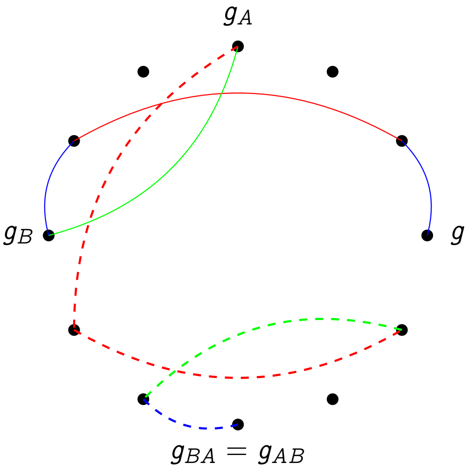


Public parameters:

- 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

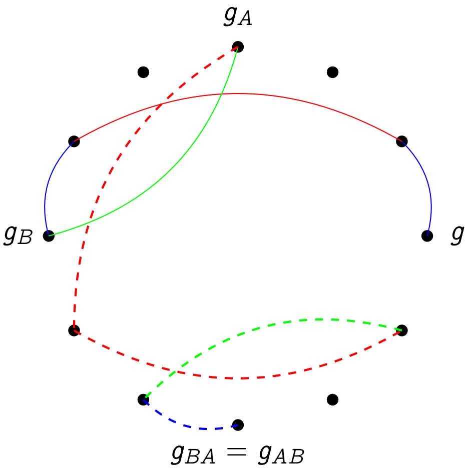


Public parameters:

- 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

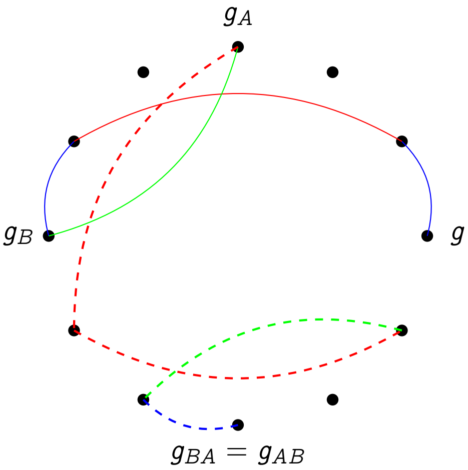


Why does this work?

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

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

Key exchange from Schreier graphs



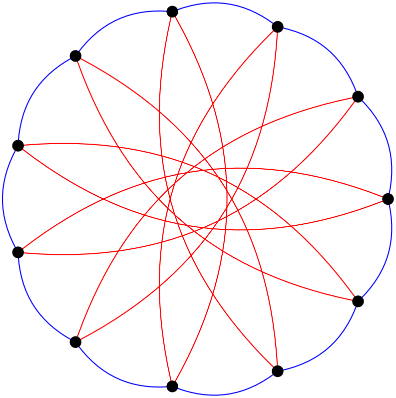
Why does this work?

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

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



— ℓ_1-isogenies

— ℓ_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] (circa 2006)

Parameters:

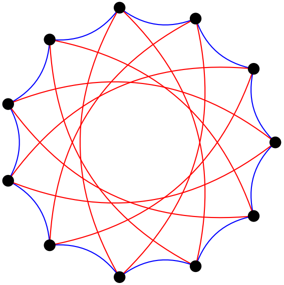
- $E/\mathbb{F}_p$ ordinary elliptic curve with *Frobenius endomorphism* π,
- primes ℓ_1,ℓ_2,... such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.
- A *direction* for each ℓ_i (i.e. an eigenvalue of π).

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: isogeny walk problem
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! (more on this later)

[7] Childs, Jao, and Soukharev 2010.

Key exchange with supersingular curves (2011)

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.

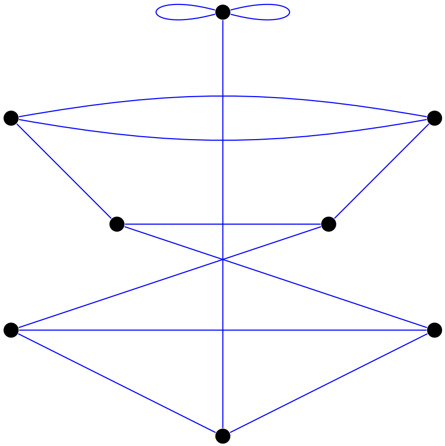


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

Key exchange with supersingular curves (2011)

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.

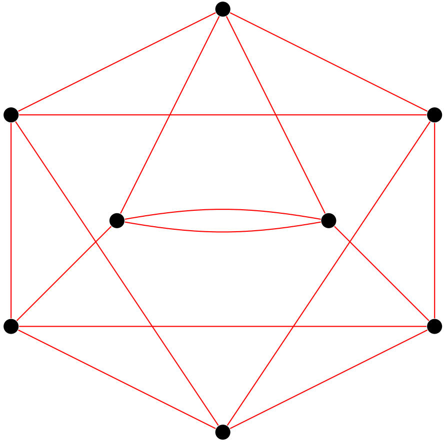


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

Key exchange with supersingular curves (2011)

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.

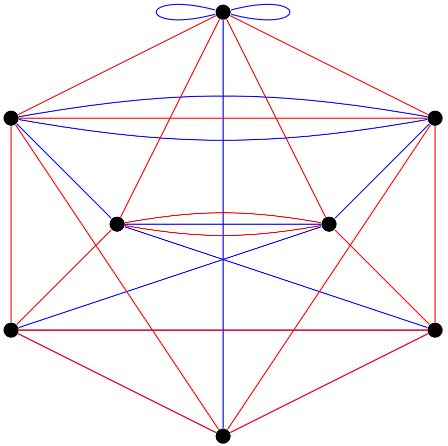


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

ECC 2011 crowd standing against quantum computers

From the ECC 2009 archives

Source: http://math.ucalgary.ca/ecc/files/ecc/u5/Bernstein_ECC2009.pdf

Is cryptography dead?

Imagine:
15 years from now
someone announces
successful construction
of a large quantum computer.

New York Times headline:
"INTERNET CRYPTOGRAPHY
KILLED BY PHYSICISTS."

Users panic.

What happens to cryptography?

RSA: Dead.
DSA: Dead.
ECDSA: Dead.
ECC in general: Dead.
HECC in general: Dead.
Buchmann–Williams: Dead.
Class groups in general: Dead.

"They're all dead, Dave."

ECC and Isogeny based crypto

At ECC 2011, D. Jao gives a talk titled "Isogenies in a quantum world":

- First presentation of SIDH outside the walls of UWaterloo.
- Announces key exchange in 0.5 seconds.

ECC and Isogeny based crypto

At ECC 2011, D. Jao gives a talk titled "Isogenies in a quantum world":

- First presentation of SIDH outside the walls of UWaterloo.
- Announces key exchange in 0.5 seconds.

The same day at the Rump session:

- L. De Feo and J. Plût give a moderately silly talk titled "Faster isogenies in a quantum world";
- They announce an asymptotically faster algorithm to evaluate composite-degree isogenies.
- Some weeks later, performance drops to $\sim$30ms.

ECC 2011: Virtual tomato thrower

Quick start

- Just head to this page and log in using the login/password printed on your badge.
- Once logged in, you'll be presented with a list of hexadecimal numbers, or **tomato tokens**.
- To throw a tomato, either click on the corresponding **Throw it!** button, or copy/paste its token into the input box you'll find on this page.
- Each tomato token can be used only **once**!

Security

In order to protect this application against any kind of abuse or foul play, our senior security experts at **Bullsh't Tech, Inc.**™ have devised a revolutionary protocol based on bleeding-edge cryptographic technology, namely the recent **Rivest-Shamir-Adleman algorithm** (or RSA, for short).

Aware of the presence of internationally renowned—yet malicious—cryptographers in the audience, the security parameters of this cryptosystem were carefully picked so as to prevent even the most advanced attacks against it: the chosen **RSA modulus** is indeed **103-digit long**, which is, well... very long, like, if you try to memorize it, or just write it down on a piece of paper or something. No, really, it's huge. Just have a look:

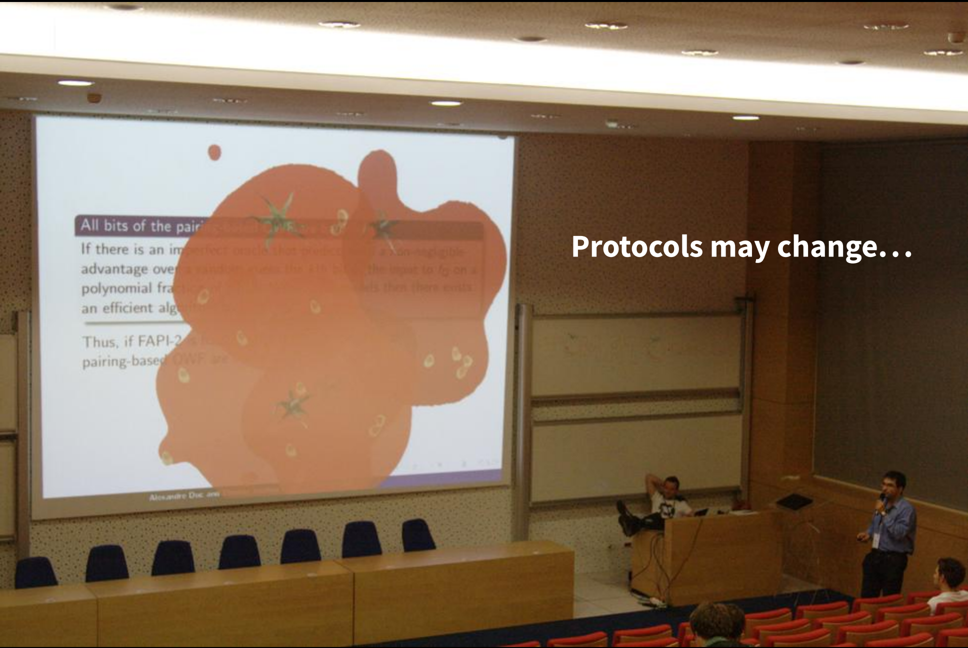
$N :=$ 3178596799904430539531118093572909377533245016659924241839251998632652703620411662777401318 406813551573.

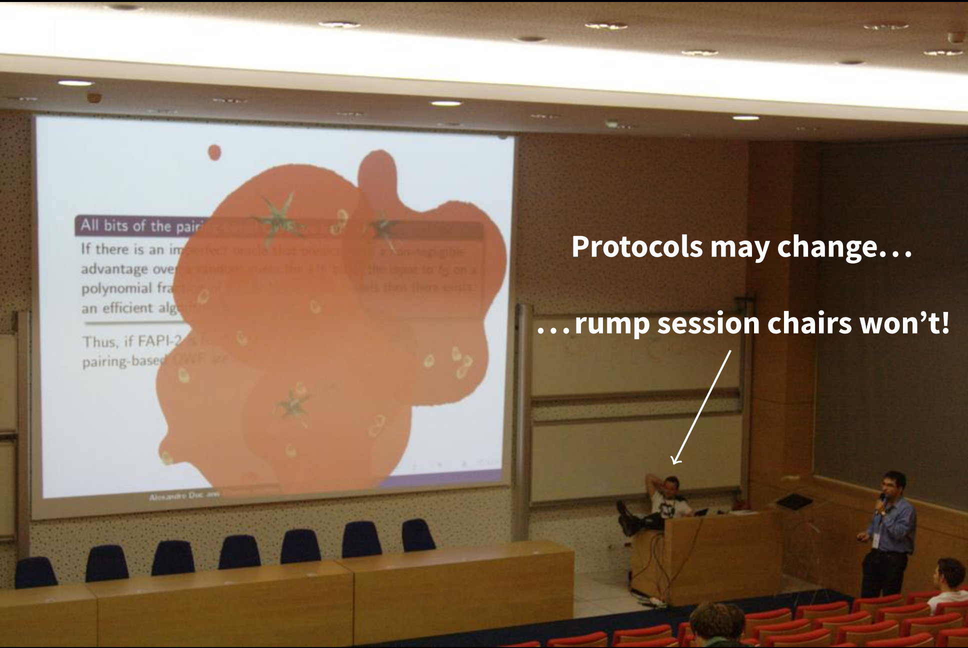
Just wow, isn't it? Not to brag, but it's larger than the number of atoms in the Universe! It's even longer than the keys of those wankers who use, er... what's-their-name... ecliptic curbs or something.

$\rightarrow$ http://ecc2011.loria.fr/tomato.html $\leftarrow$


All bits of the pairi
If there is an im
advantage ove
polynomial fra
an efficient alg
Thus, if FAPI-2
pairing-based
Alexandre Duc an

Protocols may change…





Protocols may change…

…rump session chairs won't!

Key exchange with supersingular curves

- Fix small primes ℓ_A, ℓ_B;
- No canonical labeling of the ℓ_A- and ℓ_B-isogeny graphs; however…

Walk of length e_A

$=$

Isogeny of degree $\ell_A^{e_A}$

$=$

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

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

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

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

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

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

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:

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

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

[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:

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

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

[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:

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

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

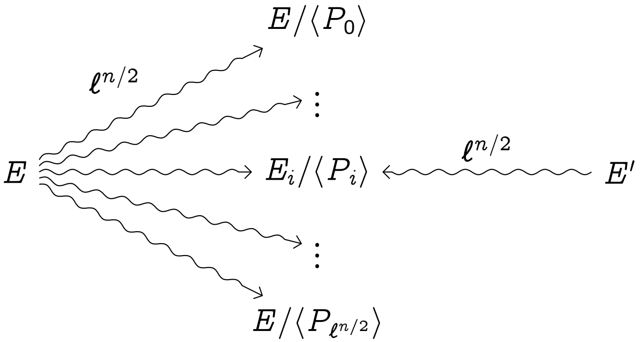
$\phi(P_B)$
$\phi(Q_B)$

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

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

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*) $O(\ell^{n/2})$.
- A quantum claw finding[9] algorithm solves the problem in $O(\ell^{n/3})$.

[9] Tani 2009.

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.[d]
- 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.
[d] Faz-Hernández, López, Ochoa-Jiménez, and Rodríguez-Henríquez 2017.

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*

Can we port some SIDH goodness to ordinary graphs?

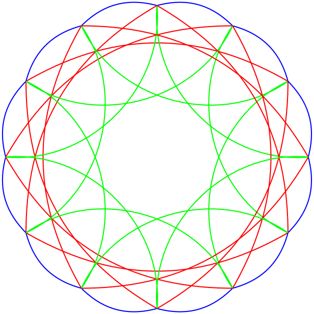
Why?

- A quantum subexponential attack is **not a total break**.
- Security of ordinary graphs is based on purer problems (isogeny walk problem, no additional input).

What makes SIDH fast?

- Only use two small prime isogeny degrees (e.g., 2 and 3);
- Rational points generate isogeny kernels
  $\rightarrow$ evaluate isogenies using Vélu's formulas.

Isogeny degrees



- Graphs of horizontal ℓ-isogenies are 2-regular:

$\rightarrow$ Each different prime degree adds roughly 1 bit of security;

$\rightarrow$ Isogeny degrees must go up to some hundreds!

Not much we can do, except, maybe, use higher genus?

Evaluating isogenies

The SIDH way

- Choose p, E_0 so that $\#E_0(\mathbb{F}_{p^2}) = (2^a 3^b)^2$;
- Secret is a point of order 2^a (or 3^b),
  - $\rightarrow$ defines an isogeny walk of length a,
  - $\rightarrow$ evaluate by Vélu's formulas.

The Rostovtsev & Stolbunov way

- Factor: Find the two roots of the modular polynomial $\Phi_\ell(j(E_0), X)$;
- Elkies' algorithm: Solving a differential equation gives the kernels of the two horizontal isogenies;
- *à la* SEA: Compute the action of the Frobenius on the kernels.

Using Vélu's formulas in ordinary graphs

- Force E_0 to have rational torsion for as many isogeny degrees as possible.
- Force $p \equiv -1 \mod \ell$ for each of those degrees ℓ
  - $\rightarrow$ Frobenius equal to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \mod \ell$,
  - $\rightarrow$ One direction rational on E_0, other direction rational on the twist.
- Use Vélu for those ℓ (Elkies for the rest).

How to (brute) force the order

- Start by choosing p and the list of ℓ's;
- Pick j-invariants on well chosen modular curves ($X_1(17)$, $X_0(30)$);
- Count points using SEA + early abort.

- We (well, Jean) found a $\approx$ 500 bits prime and a curve with 11 primes of rational torsion (in $\sim$ 2 cpu-year).
- Key exchange in <5 minutes (still optimizing).
- More details coming soon…

Shameless clickbaiting

You may also like…

"Mathematics of isogeny based cryptography"

Lecture notes, 44 pp., École Mathématique Africaine, arXiv:1711.???

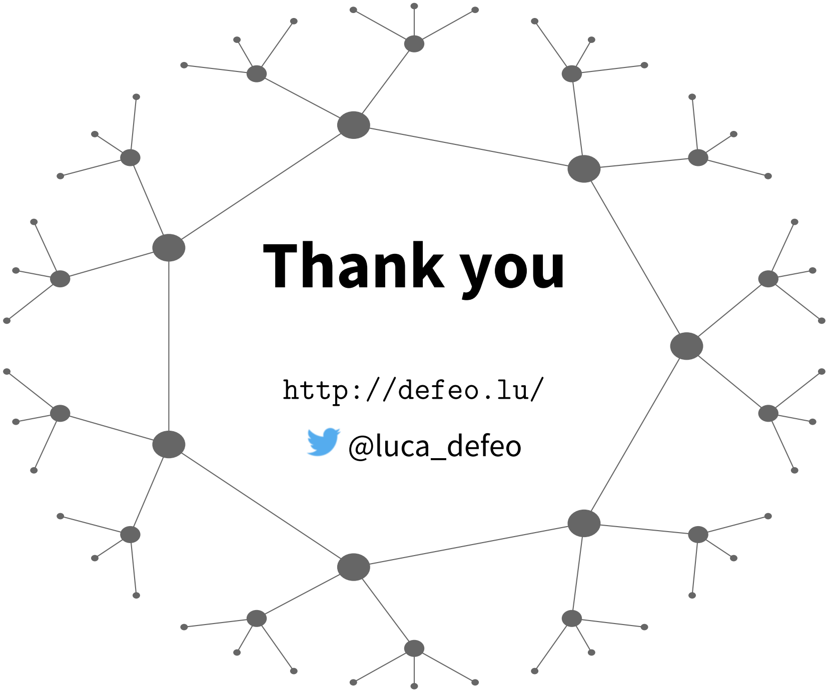
You'll never believe these jobs pay six figures…[1]

Two open post-doc positions in Versailles

- Post-quantum cryptography,
- Fully homomorphic encryption.

https://www.iacr.org/jobs/#1379

[1] and in fact they don't.



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

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

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.

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.

Faz-Hernández, Armando, Julio López, Eduardo Ochoa-Jiménez, and Francisco Rodríguez-Henríquez (2017).
A Faster Software Implementation of the Supersingular Isogeny Diffie-Hellman Key Exchange Protocol.
Cryptology ePrint Archive, Report 2017/1015.
http://eprint.iacr.org/2017/1015.