Isogeny Graphs in Cryptography

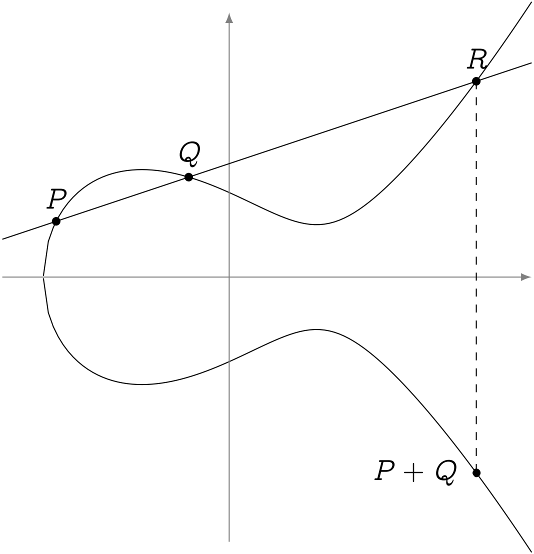
Luca De Feo
hand-drawings by Rachel Deyts

Université de Versailles & Inria, Université Paris-Saclay

May 31, 2018, Journées du Pré-GDR Sécurité, Paris

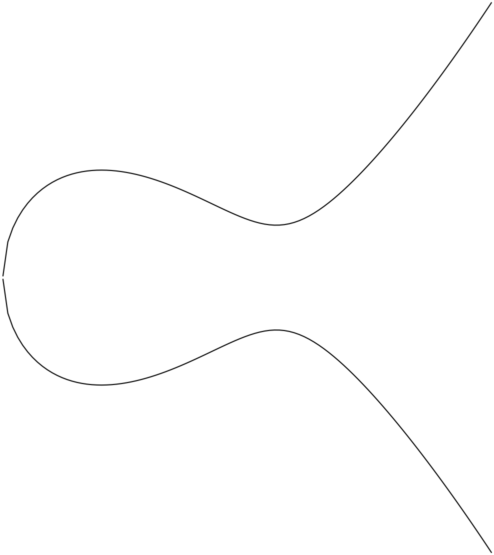
Elliptic curves

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



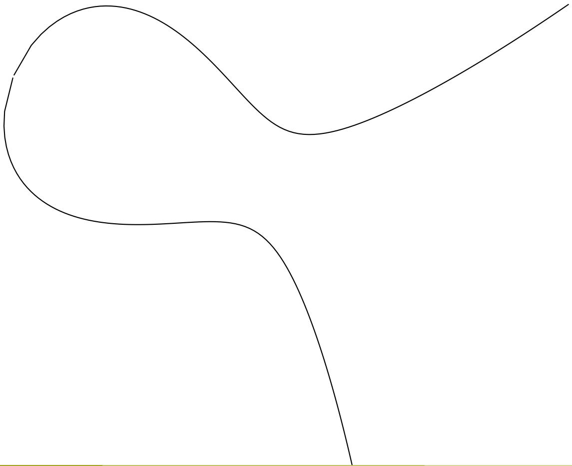
Elliptic curves

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



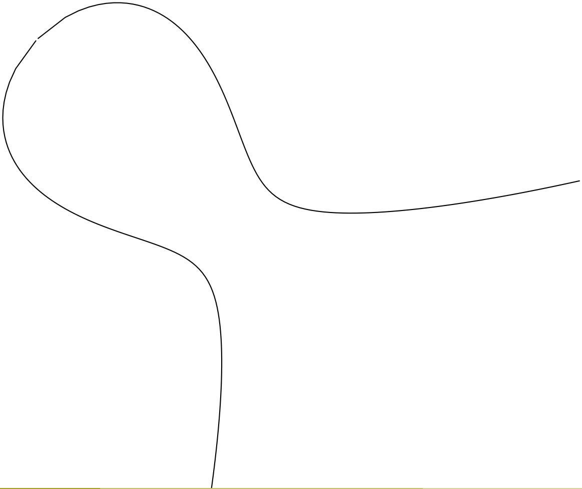
Elliptic curves

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



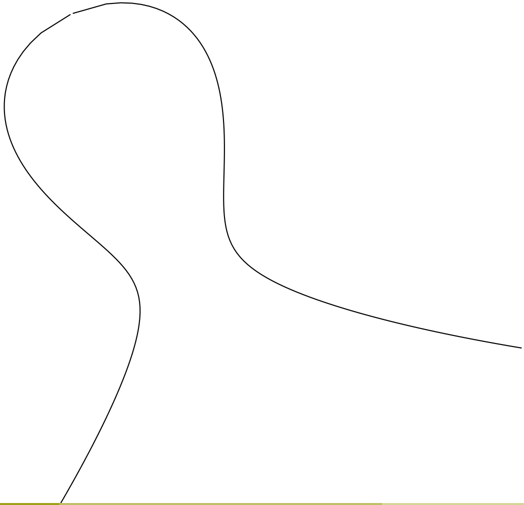
Elliptic curves

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



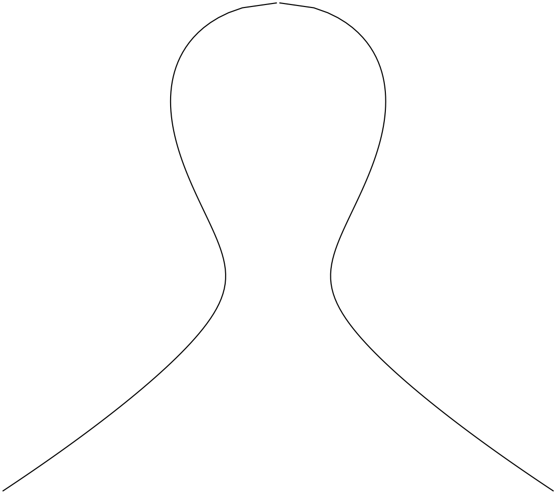
Elliptic curves

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



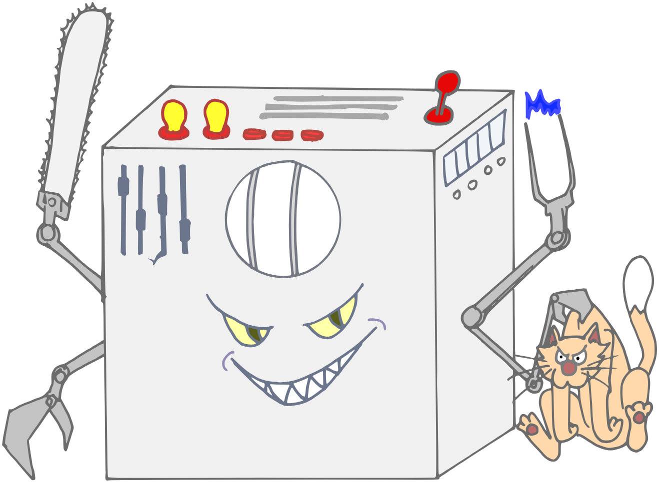
Elliptic curves

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

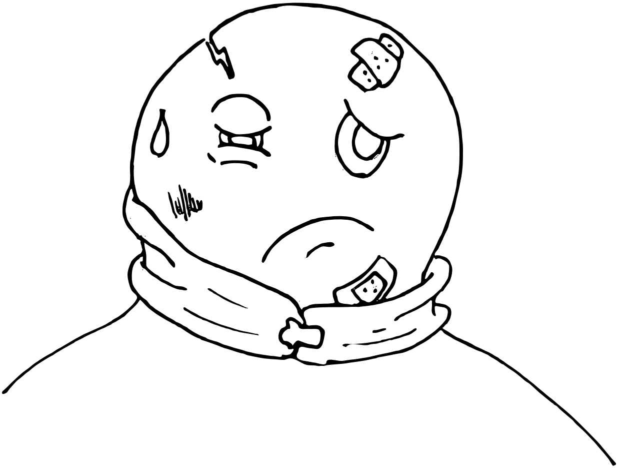


Elliptic curves

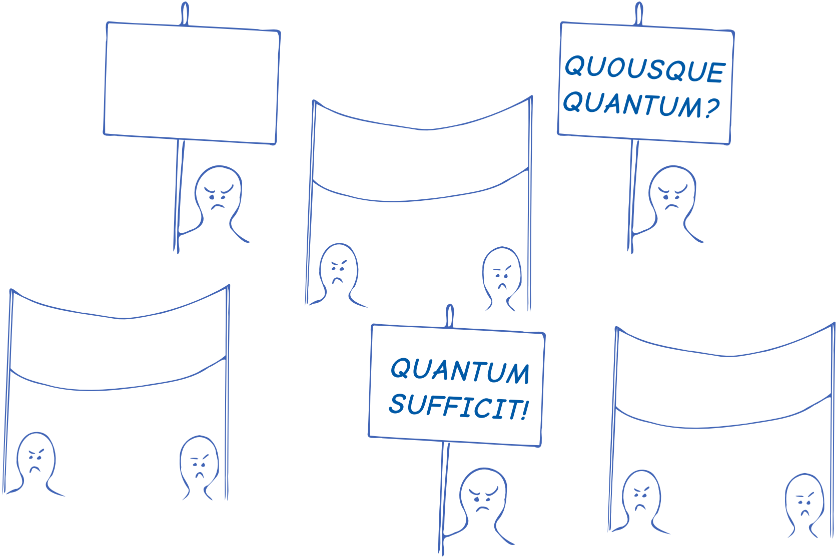
The QUANTHOM Menace



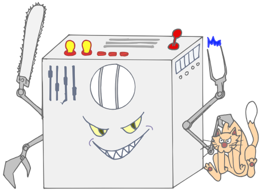
Post-quantum cryptographer?



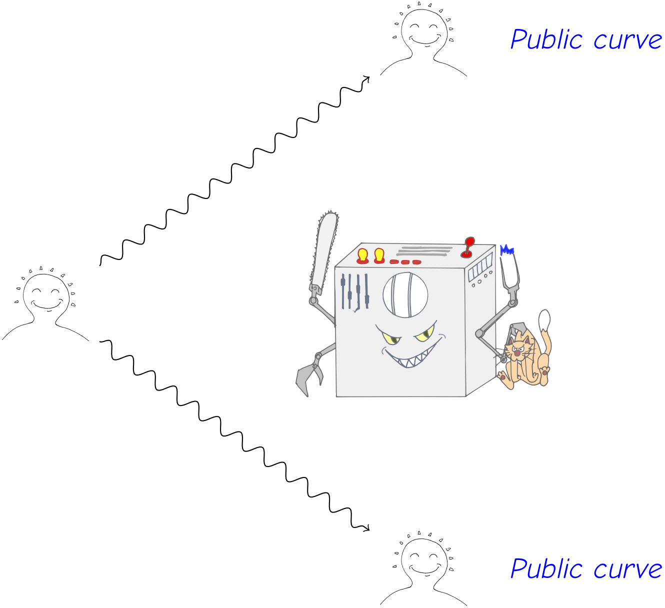
Elliptic curves of the world, UNITE!



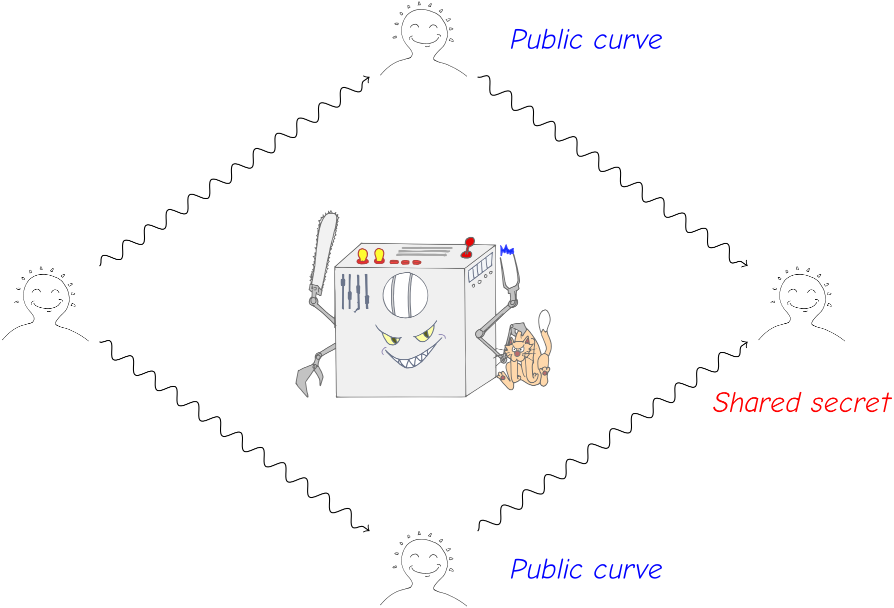
And so, they found a way around the Quanthom...



And so, they found a way around the Quanthom...



And so, they found a way around the Quanthom...



What’s an isogeny?

Rebus: 1-3-7-3-8-6

Isogenies

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

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

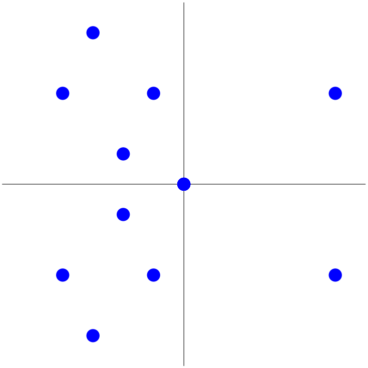
Isogeny degree

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

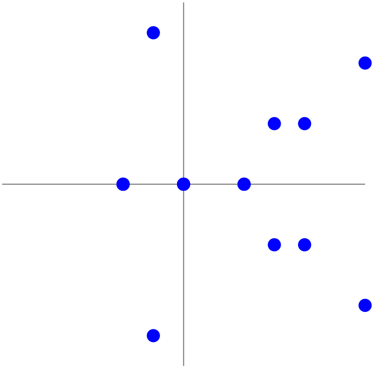
- The degree of ϕ is the cardinality of $\ker \phi$.
- (Bisson) the degree of ϕ is the time needed to compute it.

Isogenies: an example over $\mathbb{F}_{11}$

$E : y^2 = x^3 + x$



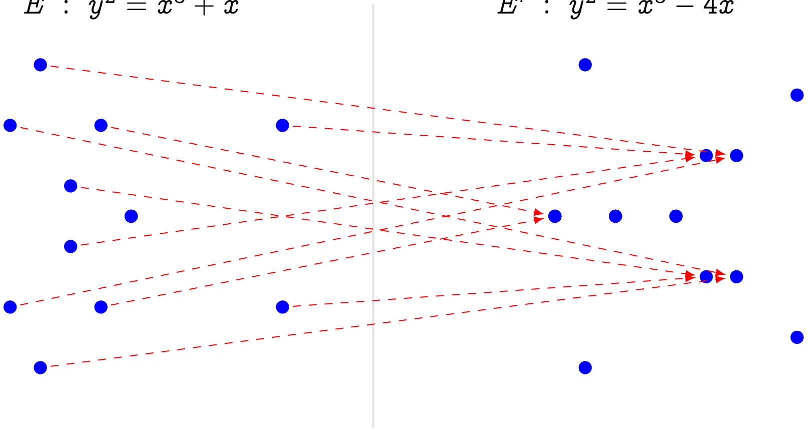
$E' : y^2 = x^3 - 4x$



$$\phi(x, y) = \left(\frac{x^2 + 1}{x}, \quad y\frac{x^2 - 1}{x^2} \right)$$

Isogenies: an example over $\mathbb{F}_{11}$

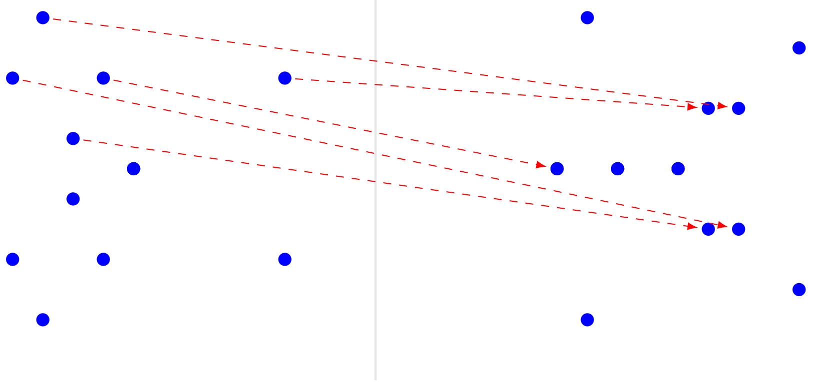
$$E \;:\; y^2 = x^3 + x \qquad\qquad E' \;:\; y^2 = x^3 - 4x$$



$$\phi(x,y) = \left(\frac{x^2+1}{x},\quad y\frac{x^2-1}{x^2}\right)$$

Isogenies: an example over $\mathbb{F}_{11}$

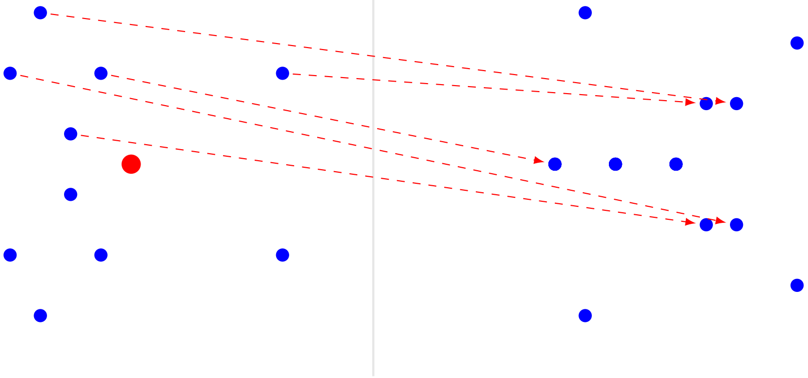
$$E \;:\; y^2 = x^3 + x \qquad\qquad E' \;:\; y^2 = x^3 - 4x$$



$$\phi(x,y) = \left(\frac{x^2+1}{x}, \quad y\frac{x^2-1}{x^2} \right)$$

Isogenies: an example over $\mathbb{F}_{11}$

$$E \;:\; y^2 = x^3 + x \qquad\qquad E' \;:\; y^2 = x^3 - 4x$$

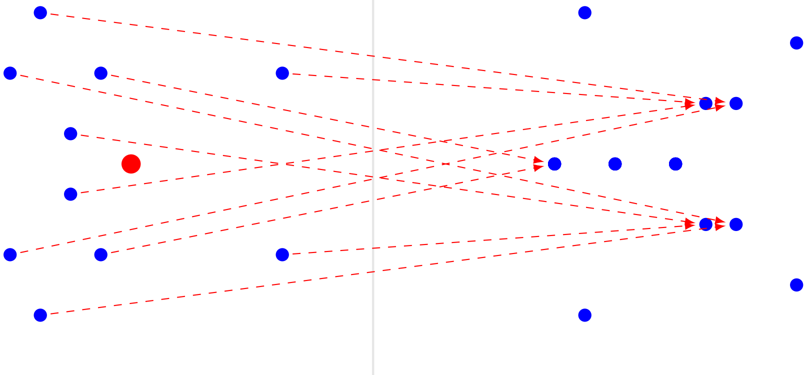


$$\phi(x,y) = \left(\frac{x^2+1}{x},\quad y\frac{x^2-1}{x^2}\right)$$

- Kernel generator in red.

Isogenies: an example over $\mathbb{F}_{11}$

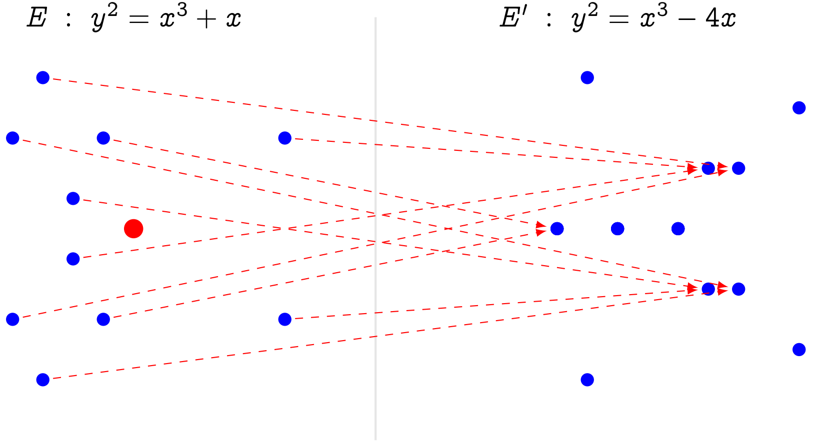
$$E : y^2 = x^3 + x \qquad\qquad E' : y^2 = x^3 - 4x$$



$$\phi(x, y) = \left(\frac{x^2+1}{x}, \quad y\frac{x^2-1}{x^2} \right)$$

- Kernel generator in red.
- This is a degree 2 map.

Isogenies: an example over $\mathbb{F}_{11}$



$$\phi(x,y) = \left(\frac{x^2+1}{x}, \quad y\frac{x^2-1}{x^2} \right)$$

- Kernel generator in red.
- This is a degree 2 map.
- Analogous to $x \mapsto x^2$ in $\mathbb{F}_q^*$.

Easy and hard problems

In practice: an isogeny ϕ is just a pair of rational fractions

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

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'.

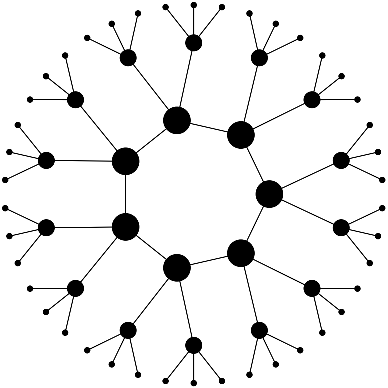
Exponential separation... Crypto happens!

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 (algebraic closure)

- 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;

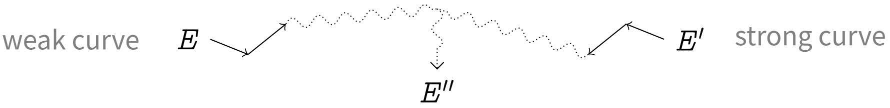
1997 His paper gets rejected;

1997–2006 …Nothing happens for about 10 years.

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

Isogeny walks and cryptanalysis[5]

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.

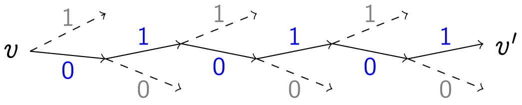
Note: Can be used to build trapdoor systems[4].

[4] Teske 2006.

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

Random walks and hash functions

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.

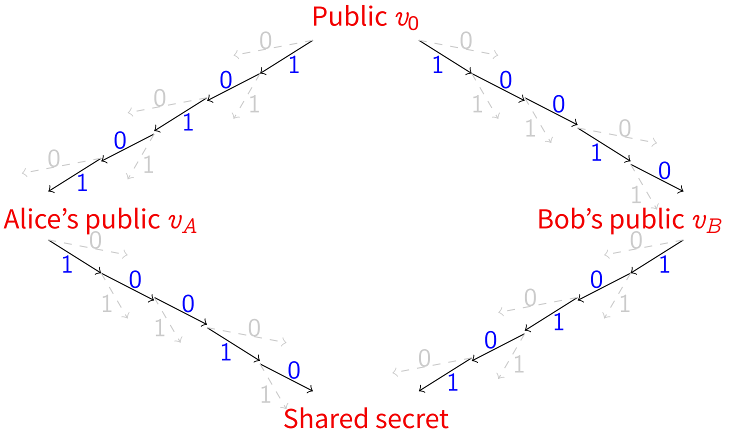
Provably secure hash functions

- 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'.

[a] Charles, Lauter, and Goren 2009.

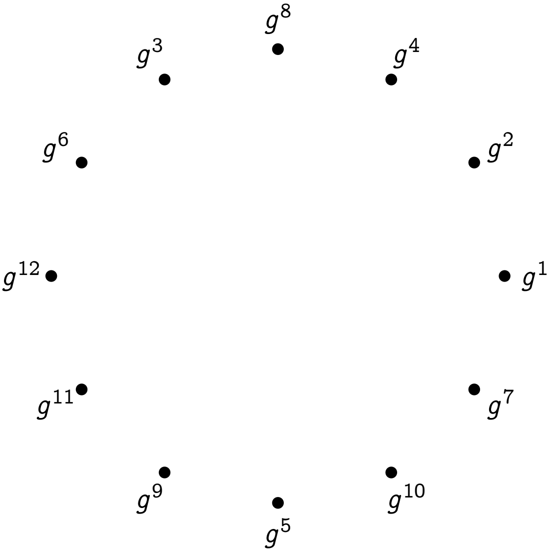
Random walks and key exchange

Let's try something harder...



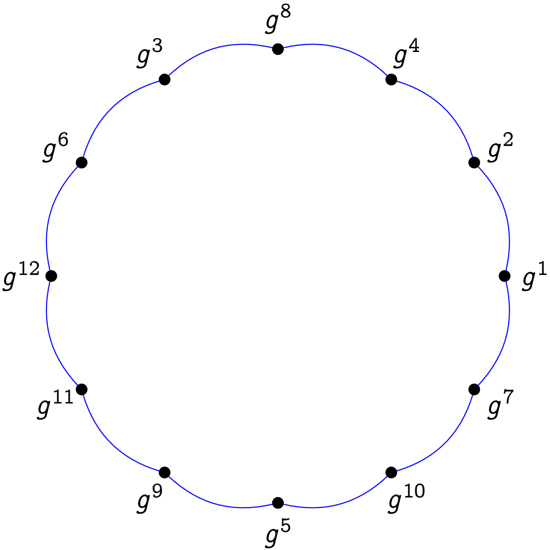
...is this even possible?

Expander graphs from groups



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

Expander graphs from groups

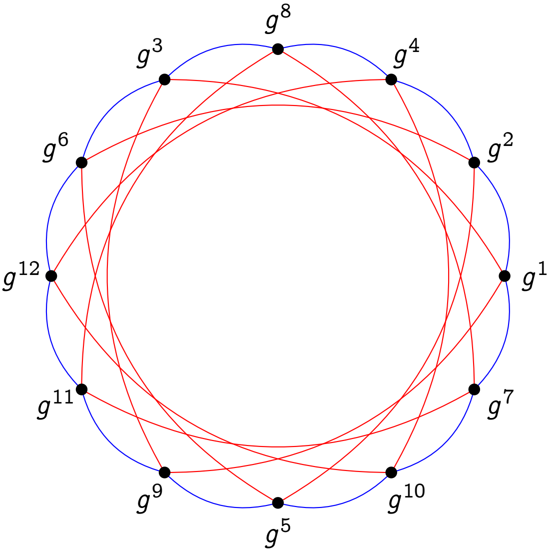


Let $G = \langle g \rangle$ be a cyclic group of order p. Let $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$ s.t. $S^{-1} \subset S$.

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

— $x \mapsto x^2$

Expander graphs from groups



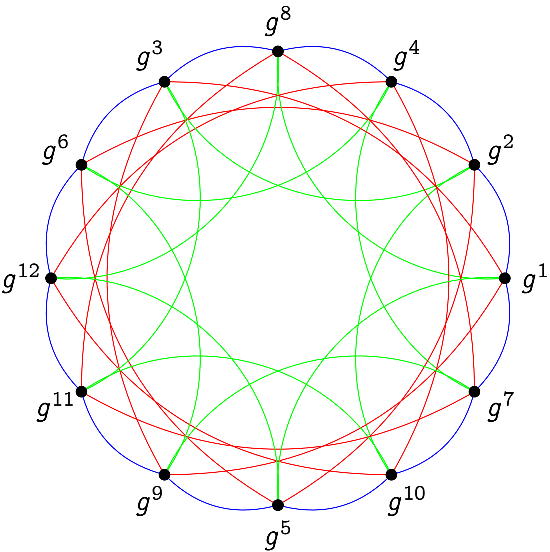
Let $G = \langle g \rangle$ be a cyclic group of order p. Let $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$ s.t. $S^{-1} \subset S$.

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

— $x \mapsto x^2$

— $x \mapsto x^3$

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

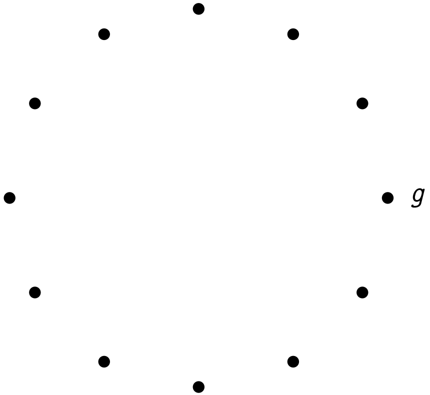
The Schreier graph of $(S, G \setminus \{1\})$ is (usually) an expander.

— $x \mapsto x^2$

— $x \mapsto x^3$

— $x \mapsto x^5$

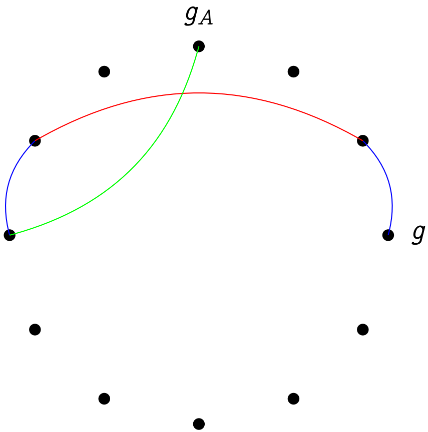
Key exchange from Schreier graphs



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

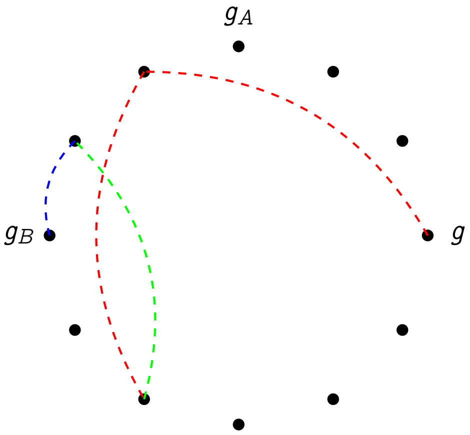


Public parameters:

- 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

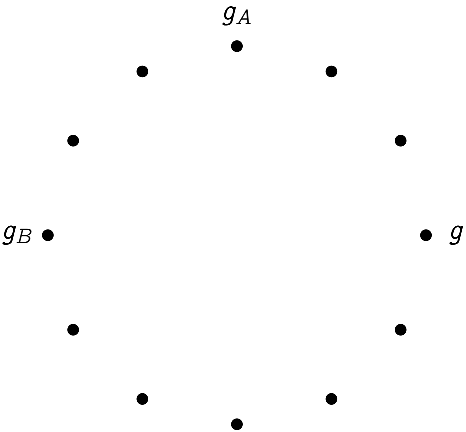


Public parameters:

- 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

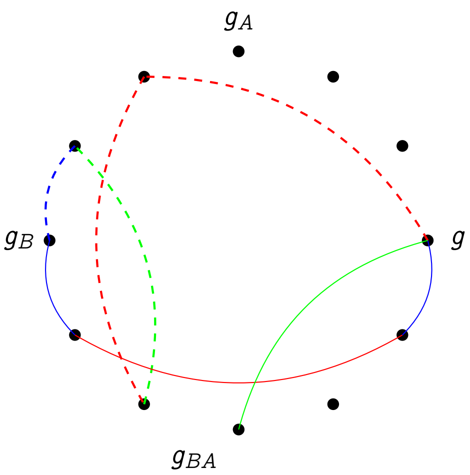


Public parameters:

- 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

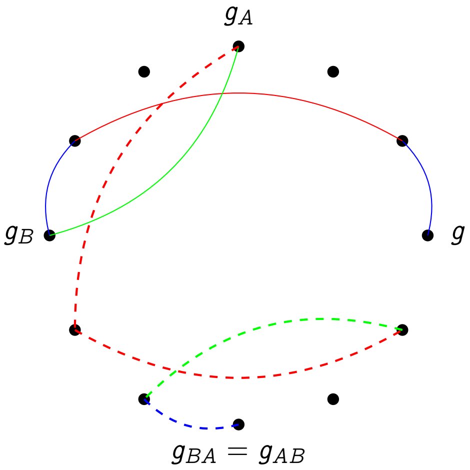


Public parameters:

- 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

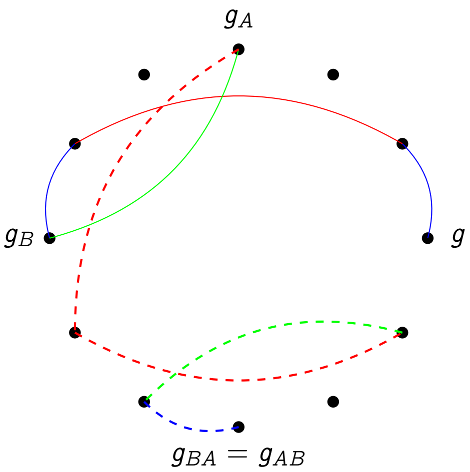


Public parameters:

- 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

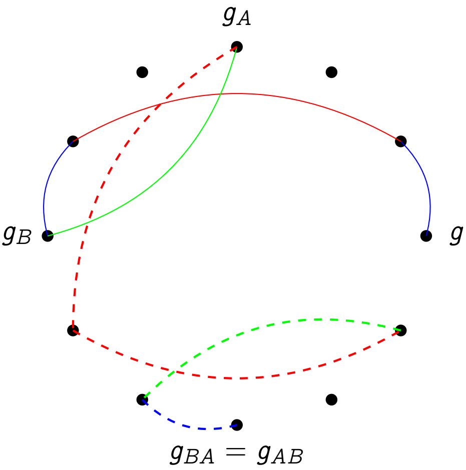


Why does this work?

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

and g_A, g_B, g_{AB} are (nearly) uniformly distributed in G…

Key exchange from Schreier graphs



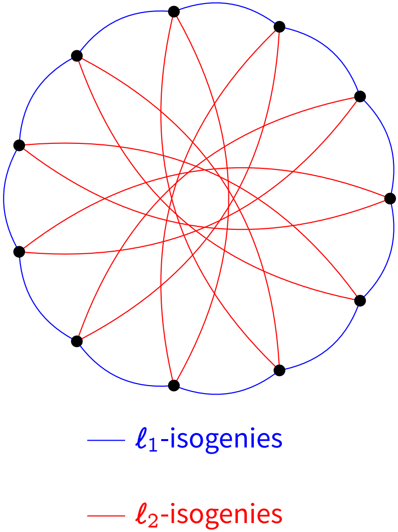
Why does this work?

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

and g_A, g_B, g_{AB} are (nearly) uniformly distributed in G…

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

Group action on isogeny graphs



- 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)


Class Group Action

Key exchange in graphs of ordinary isogenies[6] (CRS)

Parameters:

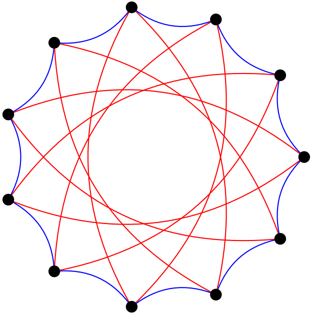
- $E/\mathbb{F}_p$ ordinary elliptic curve,
- (small) primes ℓ_1,ℓ_2,...such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.
- elements $\mathfrak{f}_1 = (\ell_1, \pi - \lambda_1)$, $\mathfrak{f}_2 = (\ell_2, \pi - \lambda_2)$ in $\mathrm{Cl}(\mathcal{O})$.

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

$$\begin{tikzcd}
 & E \arrow[dl, "\mathfrak{f}_1^{a_1}\mathfrak{f}_2^{a_2}\cdots = \mathfrak{a}"'] \arrow[dr, "\mathfrak{b} = \mathfrak{f}_1^{b_1}\mathfrak{f}_2^{b_2}\cdots"] & \\
\mathfrak{a} * E \arrow[dr] & & \mathfrak{b} * E \arrow[dl] \\
 & \mathfrak{a}\mathfrak{b} * E = \mathfrak{b}\mathfrak{a} * E &
\end{tikzcd}$$

[6] Couveignes 2006; Rostovtsev and Stolbunov 2006.

CRS 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.

In practice[7]: 5 minutes for a key exchange at 128-bits security level…

[7] De Feo, Kieffer, and Smith 2018.

CSIDH *(pron.: Seaside)*[8]

One walk step in CRS: the explicit isogeny problem

Input: Curves E and E/H, an isogeny degree ℓ_i.

Output: The rational fraction N/D.

Algorithm: Elkies' algorithm (very expensive). $\tilde{O}(n)$

CSIDH: Key observations

1. If we know the kernel H in advance, we can apply Vélu's formulas (much faster than Elkies).
2. If the curves are supersingular, it is very easy to control the kernels.
3. If we restrict to supersingular isogenies defined over $\mathbb{F}_p$, the isogeny graph structure is identical to CRS![a]

[a] Delfs and Galbraith 2016.

Result: Same security as CRS in less than 100ms!

[8] Castryck, Lange, Martindale, Panny, and Renes 2018.

CRS and CSIDH: quantum security

Fact: Shor's algorithm does not apply to Diffie-Hellman protocols from group actions.

Subexponential attack $\exp(\sqrt{\log p \log\log p})$

- Reduction to the hidden shift problem by evaluating the class group action in quantum superssposition[a] (subexpoential cost);
- Well known reduction from the hidden shift to the dihedral (non-abelian) hidden subgroup problem;
- Kuperberg's algorithm[b] solves the dHSP with a subexponential number of class group evaluations.

[a] Childs, Jao, and Soukharev 2014.
[b] Kuperberg 2005; Regev 2004; Kuperberg 2013.

Key exchange in the full supersingular graph

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

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

However: an algebraic structure is still acting on supersingular graphs: ideals of maximal orders of a quaternion algebra.

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

- The action is not commutative, we cannot use the same technique;
- We let instead Alice and Bob walk in two different isogeny graphs on the same vertex set.

Key exchange with supersingular curves

In practice, we fix:

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

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

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

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

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

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

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

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

Supersingular Isogeny Diffie-Hellman[9]

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:

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

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

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

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

Supersingular Isogeny Diffie-Hellman[9]

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:

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

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

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

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

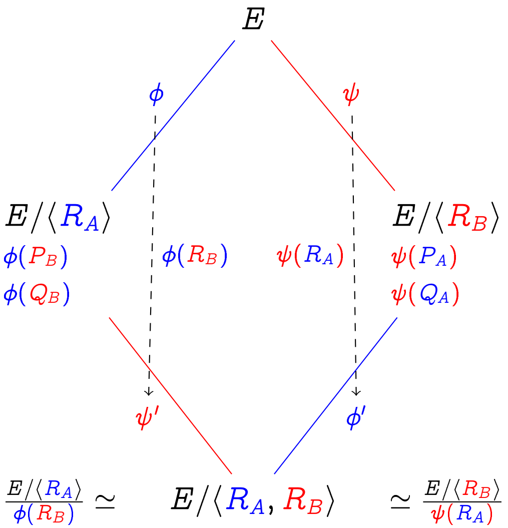
Supersingular Isogeny Diffie-Hellman[9]

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:

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



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

CSIDH vs SIDH

	CSIDH	**SIDH**
Speed (NIST 1)	<100ms	$\sim$ 10ms
Public key size (NIST 1)	64B	378B
Key compression[10]		
↳ speed		$\sim$ 15ms[11]
↳ size		222B
Constant time impl.	not yet	yes
Submitted to NIST	no	yes
Best classical attack	$p^{1/4}$	$p^{1/4}$
Best quantum attack	subexponential	$p^{1/6}$
Key size scales	quadratically	linearly
Security assumption	isogeny walk problem	ad hoc
CPA security	yes	yes
CCA security	yes	Fujisaki-Okamoto
Non-interactive key ex.	yes	no
Signatures	unclear	very slow

[10] Zanon, Simplicio, Pereira, Doliskani, and Barreto 2018.

[11] https://twitter.com/PatrickLonga/status/1002313366466015232?s=20

SIKE: Supersingular Isogeny Key Encapsulation

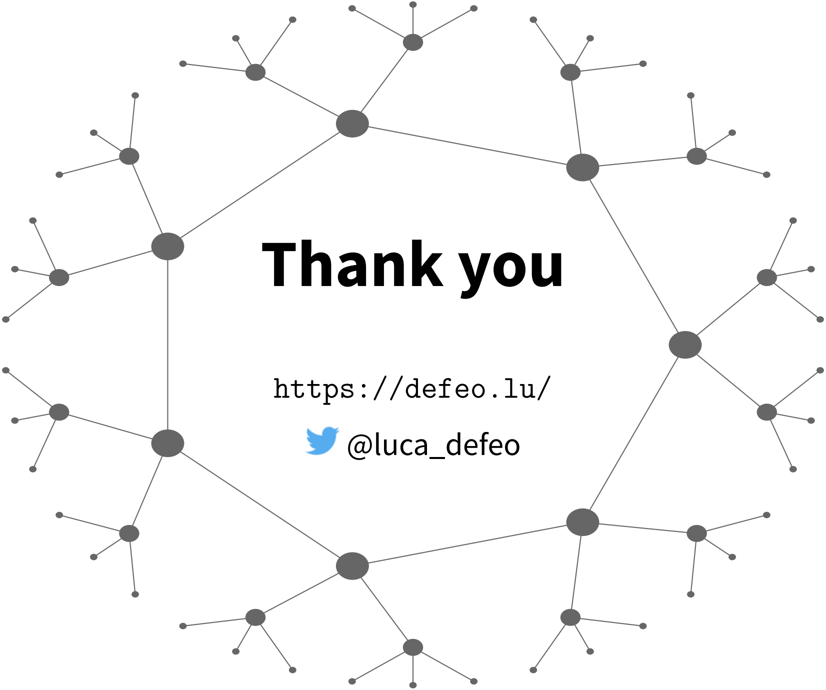
- Submission to the NIST PQ competition:

  SIKE.PKE: El Gamal-type system with IND-CPA security proof,

  SIKE.KEM: generically transformed system with IND-CCA security proof.

- Security levels 1, 3 and 5.
- Smallest communication complexity among all proposals in each level.
- Slowest among all benchmarked proposals in each level.
- A team of 14 submitters, from 8 universities and companies.
- Visit `https://sike.org/`.

	p	cl. security	q. security	speed	comm.
SIKEp503	$2^{250}3^{159}-1$	126 bits	84 bits	10ms	0.4KB
SIKEp751	$2^{372}3^{239}-1$	188 bits	125 bits	30ms	0.6KB
SIKEp964	$2^{486}3^{301}-1$	241 bits	161 bits		0.8KB



Thank you

`https://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 (Dec. 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 (June 2009).
"Expander graphs based on GRH with an application to elliptic curve cryptography."
In: Journal of Number Theory 129.6,
Pp. 1491–1504.

References V

Teske, Edlyn (Jan. 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 VI

Bisson, Gaetan and Andrew V. Sutherland (June 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 (Jan. 2009).
"Cryptographic Hash Functions from Expander Graphs."
In: Journal of Cryptology 22.1,
Pp. 93–113.

Couveignes, Jean-Marc (2006).
Hard Homogeneous Spaces.
URL: http://eprint.iacr.org/2006/291/.

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

References VII

De Feo, Luca, Jean Kieffer, and Benjamin Smith (2018).
Towards practical key exchange from ordinary isogeny graphs.
Cryptology ePrint Archive, Report 2018/485.
https://eprint.iacr.org/2018/485.

Delfs, Christina and Steven D. Galbraith (2016).
"Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$."
In: Des. Codes Cryptography 78.2,
Pp. 425–440.

Castryck, Wouter, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes (2018).
CSIDH: An Efficient Post-Quantum Commutative Group Action.
Cryptology ePrint Archive, Report 2018/383.
https://eprint.iacr.org/2018/383.

References VIII

Childs, Andrew, David Jao, and Vladimir Soukharev (2014).
"Constructing elliptic curve isogenies in quantum subexponential time."
In: Journal of Mathematical Cryptology 8.1,
Pp. 1–29.

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`.

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

References IX

Kuperberg, Greg (2013).
"Another Subexponential-time Quantum Algorithm for the Dihedral Hidden Subgroup Problem."
In: 8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013).
Ed. by Simone Severini and Fernando Brandao.
Vol. 22.
Leibniz International Proceedings in Informatics (LIPIcs).
Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik,
Pp. 20–34.

References X

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 XI

Zanon, Gustavo H. M., Marcos A. Simplicio, Geovandro C. C. F. Pereira, Javad Doliskani, and Paulo S. L. M. Barreto (2018). "Faster Isogeny-Based Compressed Key Agreement." In: Post-Quantum Cryptography. Ed. by Tanja Lange and Rainer Steinwandt. Cham: Springer International Publishing, Pp. 248–268.