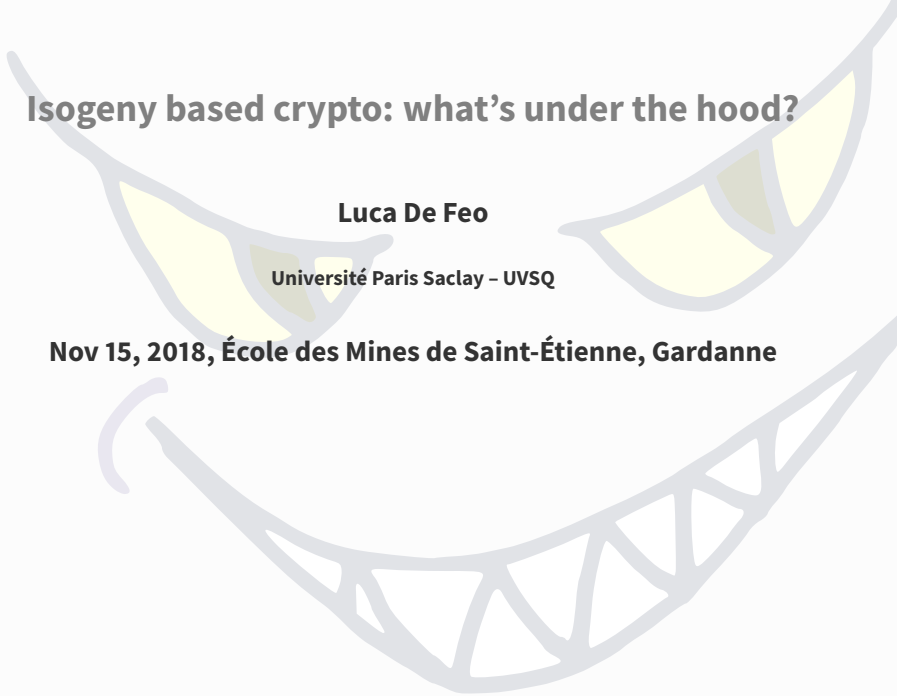


Isogeny based crypto: what's under the hood?

Luca De Feo

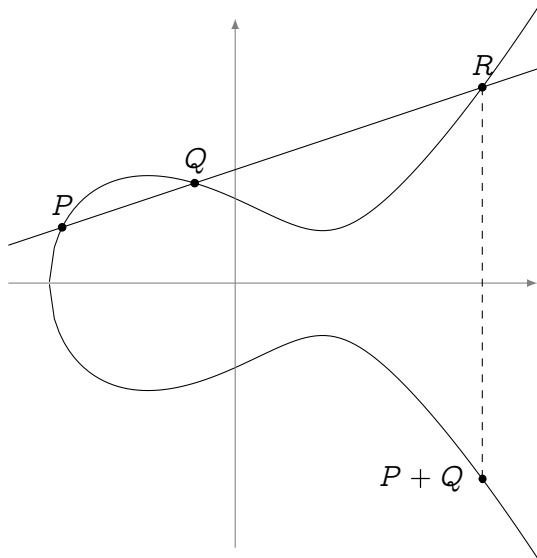
Université Paris Saclay – UVSQ

Nov 15, 2018, École des Mines de Saint-Étienne, Gardanne



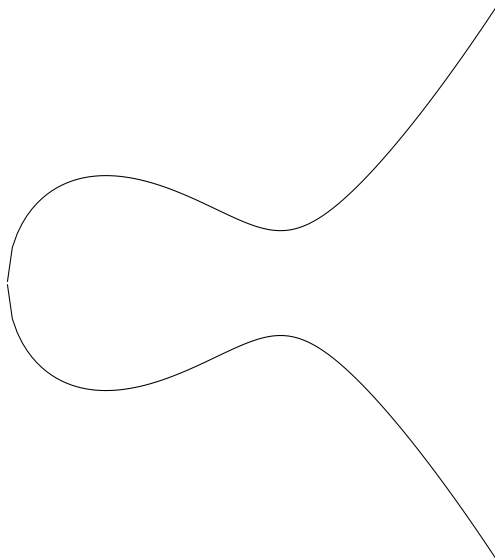
Elliptic curves

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



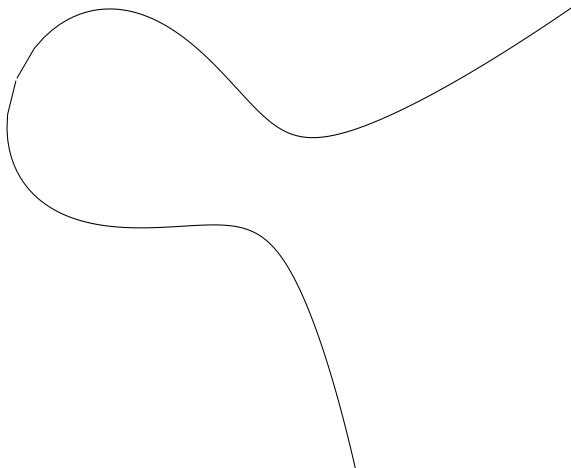
Elliptic curves

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



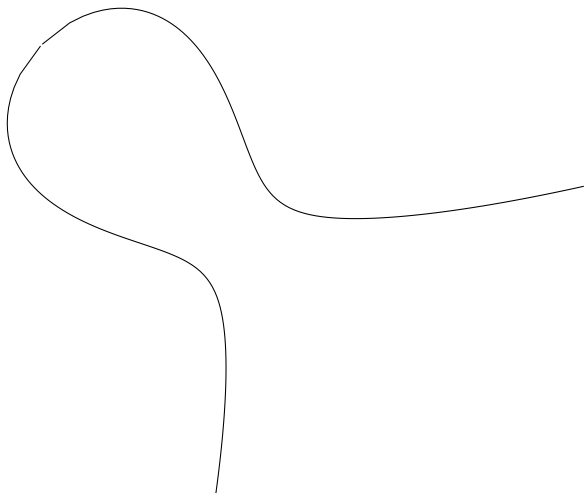
Elliptic curves

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



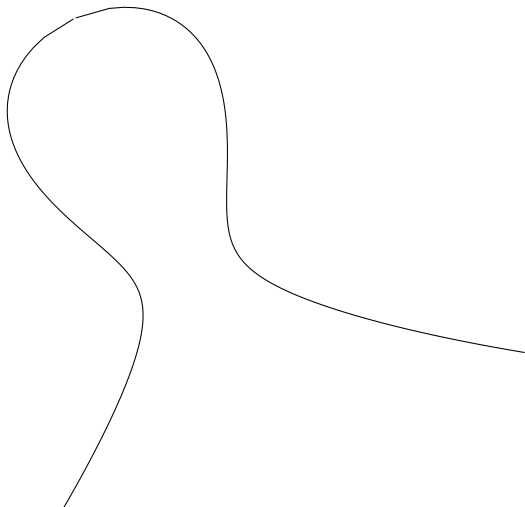
Elliptic curves

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



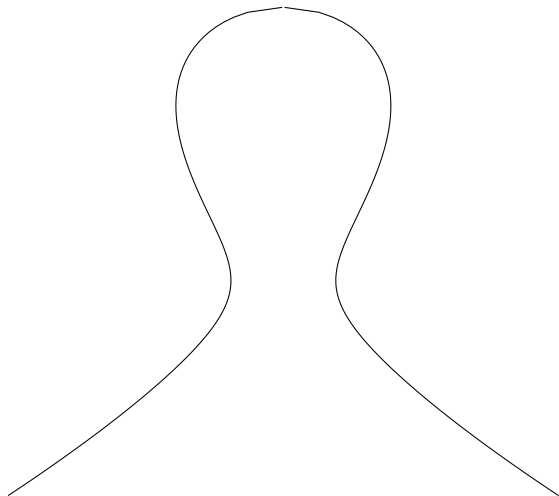
Elliptic curves

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...

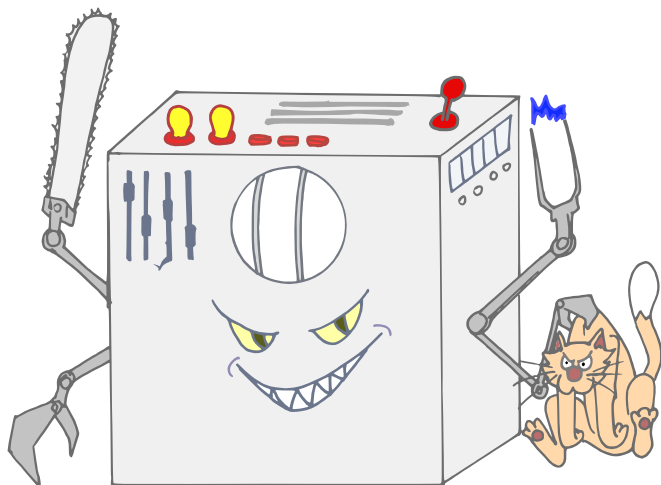


Elliptic curves

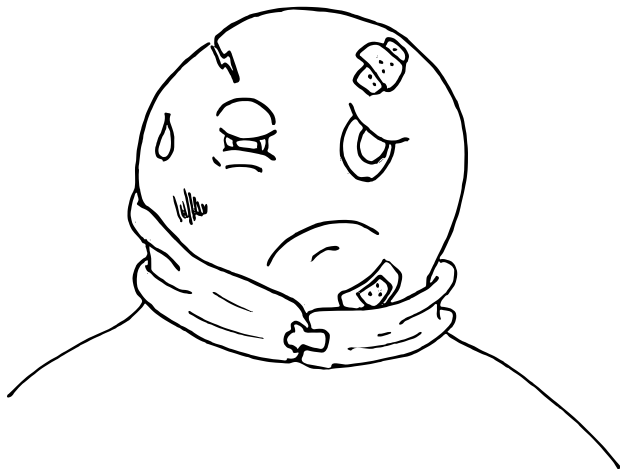


I power 70% of WWW traffic!

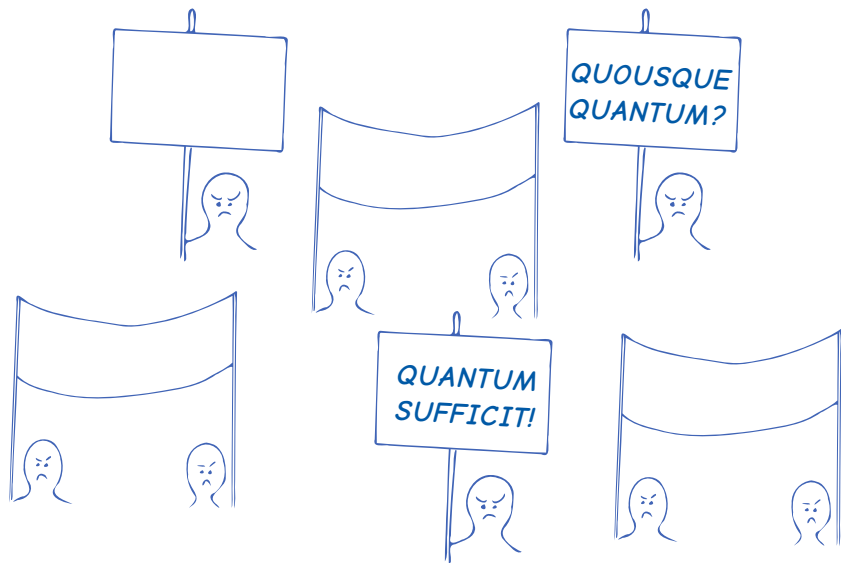
The QUANTHOM Menace



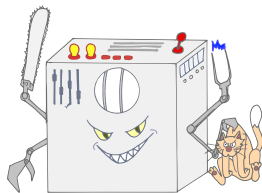
Post-quantum cryptographer?



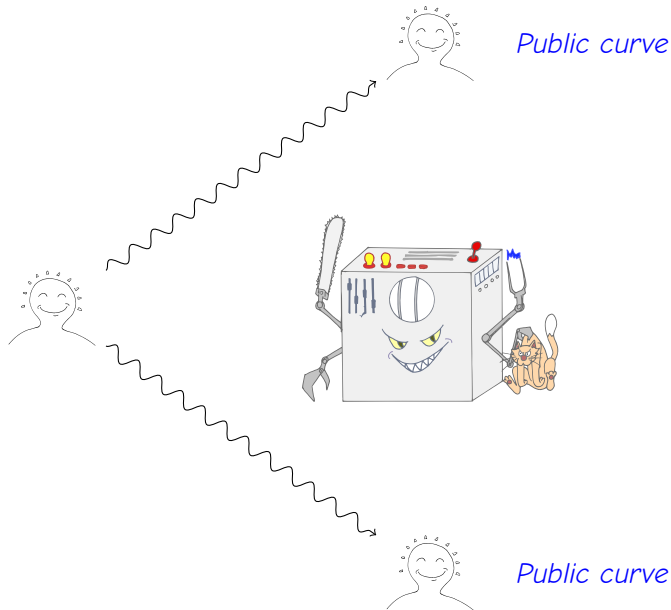
Elliptic curves of the world, UNITE!



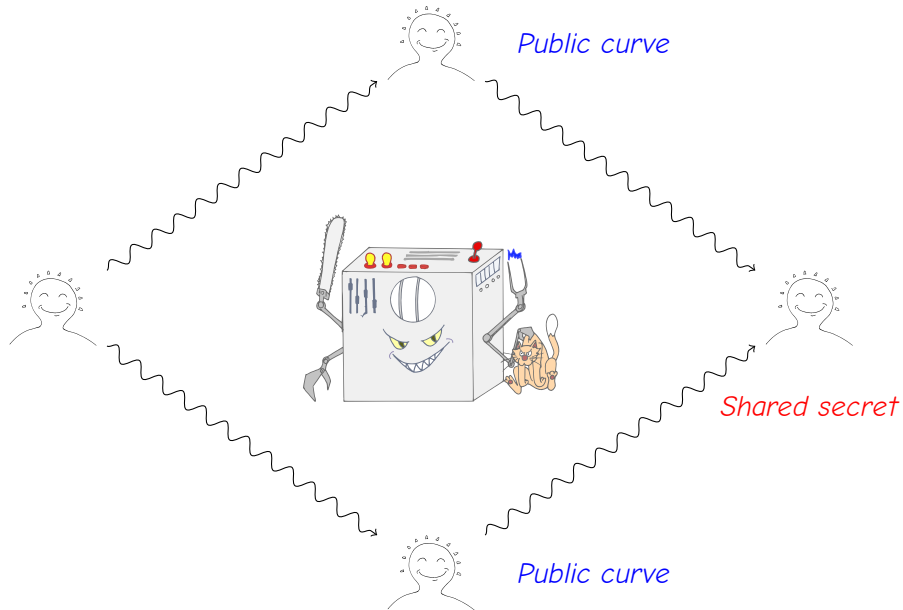
And so, they found a way around the Quantom...



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



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



A brief history of isogeny-based key exchange

- 1996 Couveignes introduces Hard Homogeneous Spaces. His work stays unpublished for 10 years.
- 2006 Rostovtsev & Stolbunov independently rediscover Couveignes ideas, suggest isogeny-based Diffie–Hellman as a quantum-resistant primitive.
- 2006-2010 Other isogeny-based protocols by Teske and Charles, Goren & Lauter.
- 2011-2012 D., Jao & Plût introduce SIDH, an efficient post-quantum key exchange inspired by Couveignes, Rostovtsev, Stolbunov, Charles, Goren, Lauter.
- 2017 SIDH is submitted to the NIST competition (with the name SIKE, only isogeny-based candidate).
- 2018 D., Kieffer & Smith *resurrect* the Couveignes–Rostovtsev–Stolbunov protocol, Castryck, Lange, Martindale, Panny & Renes publish an efficient variant named CSIDH.

What's an isogeny?

Isogenies are just **the right notionTM of morphism** for elliptic curves

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

(Separable) isogenies \Leftrightarrow finite subgroups:

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

Separable isogenies (write this down, now!)

- The kernel H determines the image curve E' up to isomorphism:

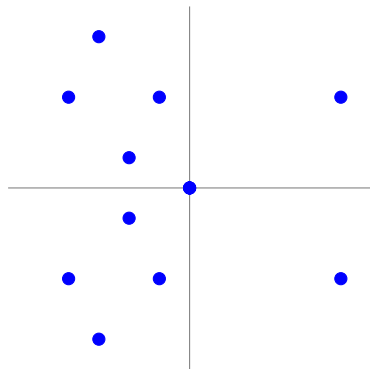
$$E/H \stackrel{\text{def}}{=} E'.$$

- The degree of $\phi : E \rightarrow E/H$ is the size of the kernel H :

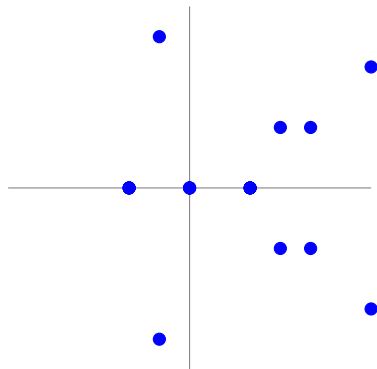
$$\deg \phi \stackrel{\text{def}}{=} \# \ker \phi.$$

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

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



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

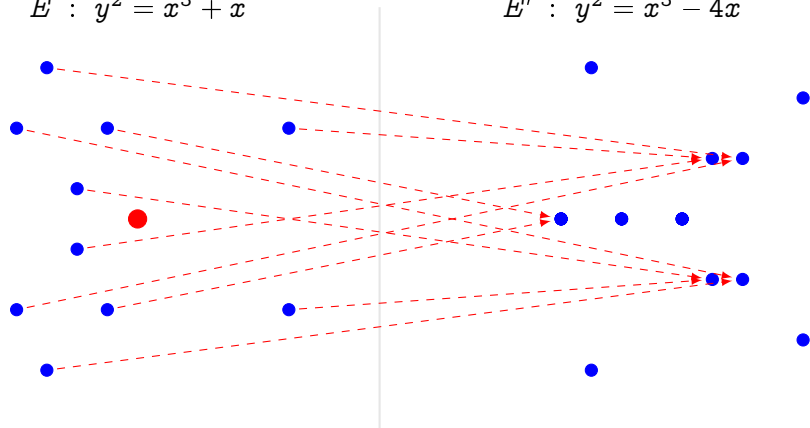


$$\phi(x, y) = \left(\frac{x^2 + 1}{x}, y \frac{x^2 - 1}{x^2} \right)$$

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

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

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



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

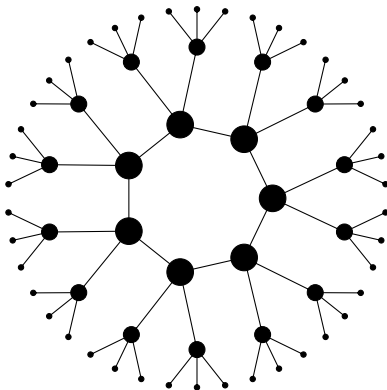
- Kernel generator in red.
- This is a degree 2 map.
- Analogous to $x \mapsto x^2$ in \mathbb{F}_q^* .

Isogeny graphs

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

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ & \searrow \phi' & \updownarrow \wr \\ & & E' \end{array}$$

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



Structure of the graph

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.

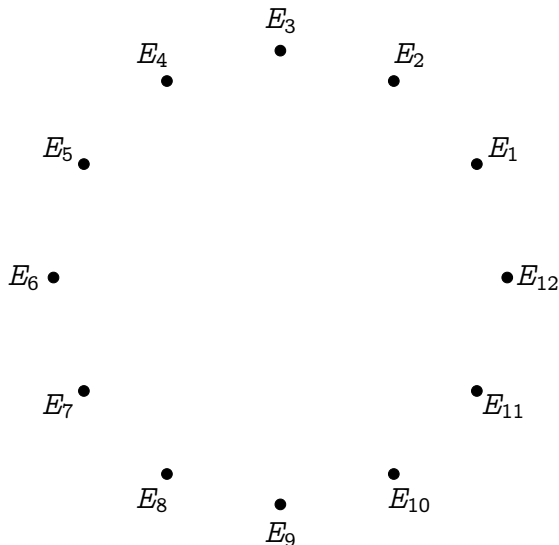
Supersingular
case (\mathbb{F}_p)

- If $\ell = 2$ nodes have degree 1, 2 or 3;
- For $\sim 50\%$ of ℓ , graphs are isolated points;
- For other $\sim 50\%$, graphs are 2-regular;

Supersingular
case (\mathbb{F}_{p^2})

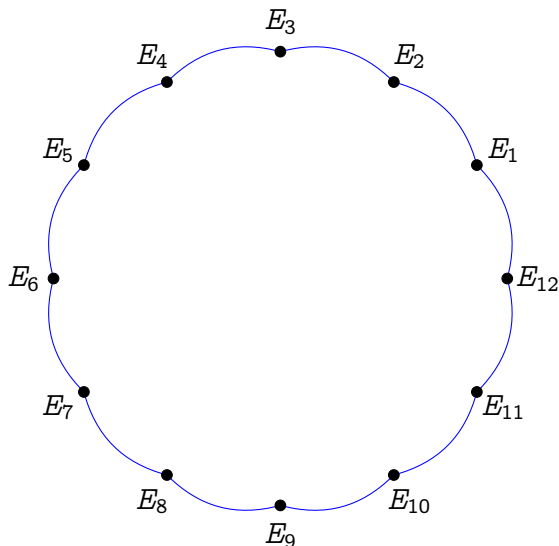
- The graph is $\ell + 1$ -regular.
- There is a **unique (finite) connected component** made of all supersingular curves with the same number of points.

Complex multiplication graphs



Vertices are elliptic curves with complex multiplication by \mathcal{O}_K (i.e., $\text{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

Complex multiplication graphs

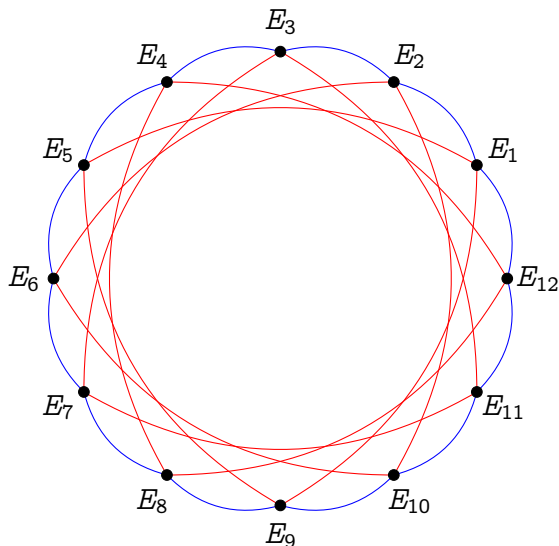


Vertices are elliptic curves with complex multiplication by \mathcal{O}_K (i.e., $\text{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

Edges are horizontal isogenies of bounded prime degree.

— degree 2

Complex multiplication graphs



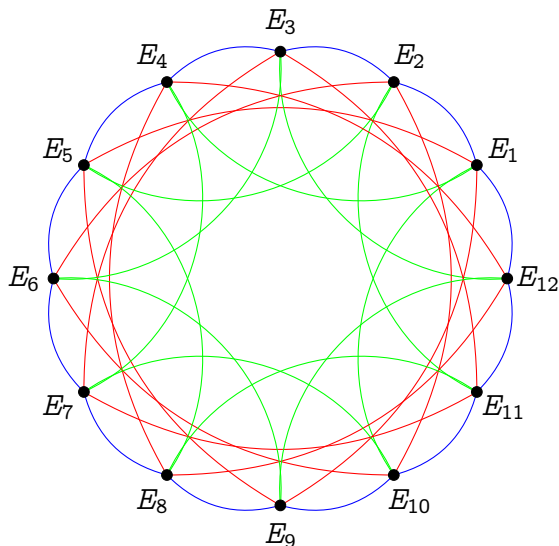
Vertices are elliptic curves with complex multiplication by \mathcal{O}_K (i.e., $\text{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

Edges are horizontal isogenies of bounded prime degree.

— degree 2

— degree 3

Complex multiplication graphs



Vertices are elliptic curves with complex multiplication by \mathcal{O}_K (i.e., $\text{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

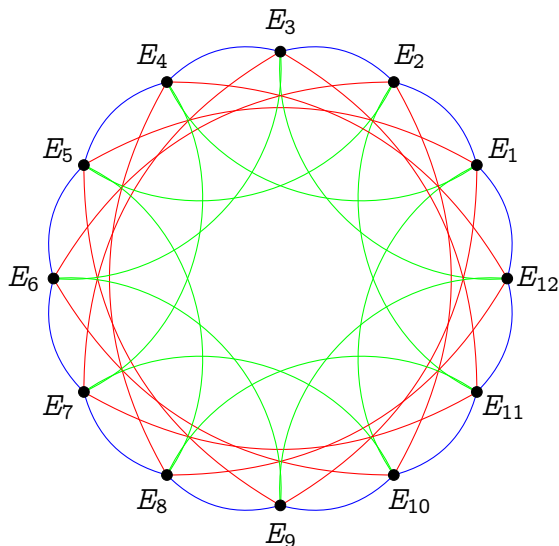
Edges are horizontal isogenies of bounded prime degree.

— degree 2

— degree 3

— degree 5

Complex multiplication graphs



Vertices are elliptic curves with complex multiplication by \mathcal{O}_K (i.e., $\text{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

Edges are horizontal isogenies of bounded prime degree.

— degree 2

— degree 3

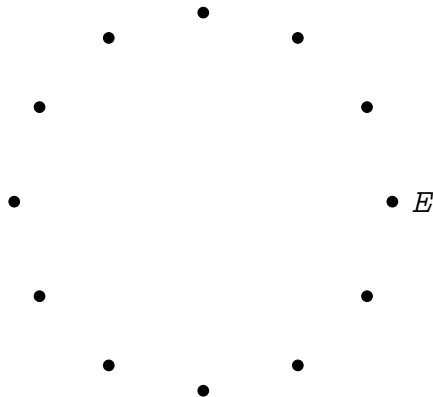
— degree 5

Isomorphic to a Cayley graph of $\text{Cl}(\mathcal{O}_K)$.

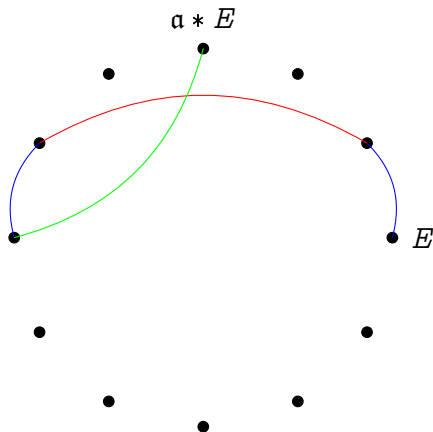
Rostovtsev & Stolbunov key exchange (CRS)

Public parameters:

- A starting curve E/\mathbb{F}_p with CM by \mathcal{O}_K ;
- A set of ideals of small norm $S \subset \text{Cl}(\mathcal{O}_K)$.



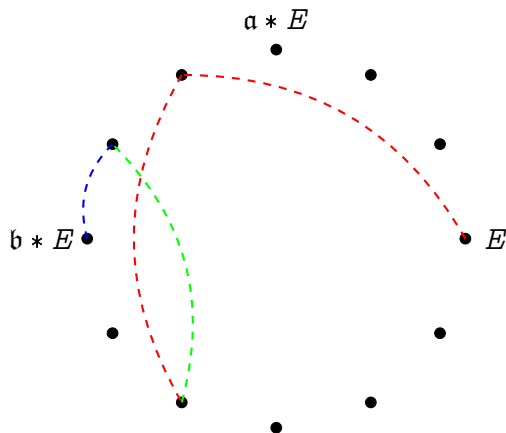
Rostovtsev & Stolbunov key exchange (CRS)



Public parameters:

- A starting curve E/\mathbb{F}_p with CM by \mathcal{O}_K ;
 - A set of ideals of small norm $S \subset \text{Cl}(\mathcal{O}_K)$.
- 1 **Alice** takes a **secret** random walk $\mathfrak{a} = \prod_{\mathfrak{s} \in S} \mathfrak{s}^{e_{\mathfrak{s}}}$ defining an isogeny $E \rightarrow \mathfrak{a} * E$;

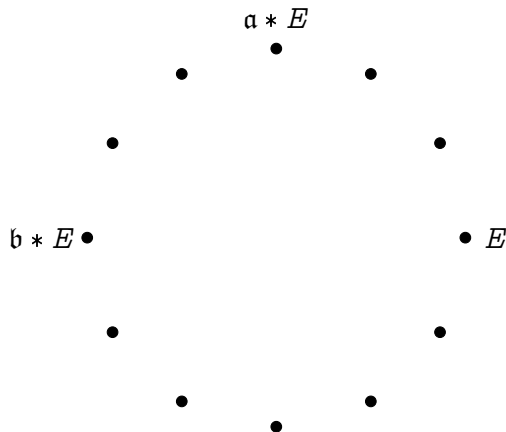
Rostovtsev & Stolbunov key exchange (CRS)



Public parameters:

- A starting curve E/\mathbb{F}_p with CM by \mathcal{O}_K ;
 - A set of ideals of small norm $S \subset \text{Cl}(\mathcal{O}_K)$.
- 1 **Alice** takes a **secret** random walk $\alpha = \prod_{\mathfrak{s} \in S} \mathfrak{s}^{e_{\mathfrak{s}}}$ defining an isogeny $E \rightarrow \alpha * E$;
 - 2 **Bob** does the same;

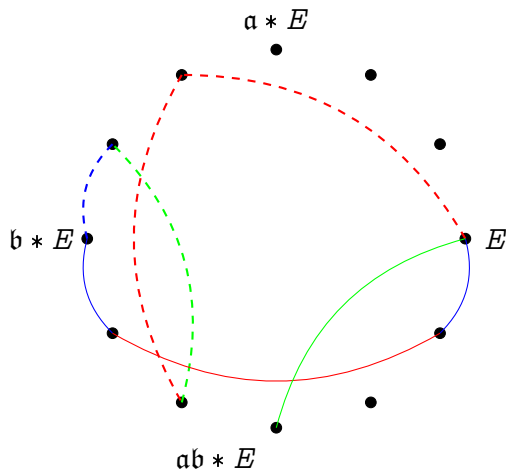
Rostovtsev & Stolbunov key exchange (CRS)



Public parameters:

- A starting curve E/\mathbb{F}_p with CM by \mathcal{O}_K ;
 - A set of ideals of small norm $S \subset \text{Cl}(\mathcal{O}_K)$.
- 1 **Alice** takes a **secret** random walk $\mathfrak{a} = \prod_{\mathfrak{s} \in S} \mathfrak{s}^{e_{\mathfrak{s}}}$ defining an isogeny $E \rightarrow \mathfrak{a} * E$;
 - 2 **Bob** does the same;
 - 3 They publish $\mathfrak{a} * E$ and $\mathfrak{b} * E$;

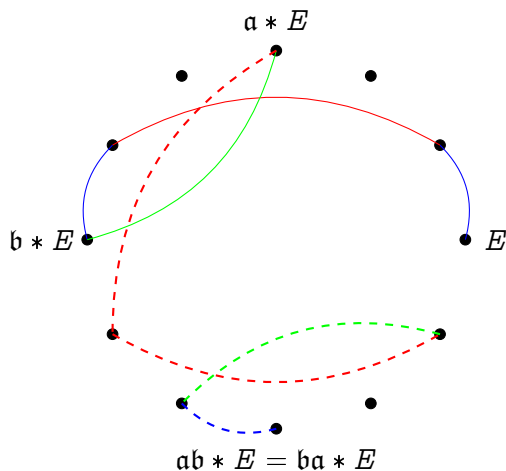
Rostovtsev & Stolbunov key exchange (CRS)



Public parameters:

- A starting curve E/\mathbb{F}_p with CM by \mathcal{O}_K ;
 - A set of ideals of small norm $S \subset \text{Cl}(\mathcal{O}_K)$.
- 1 **Alice** takes a **secret** random walk $\alpha = \prod_{s \in S} s^{e_s}$ defining an isogeny $E \rightarrow \alpha * E$;
 - 2 **Bob** does the same;
 - 3 They publish $\alpha * E$ and $b * E$;
 - 4 **Alice** repeats her secret walk α starting from $b * E$.

Rostovtsev & Stolbunov key exchange (CRS)



Public parameters:

- A starting curve E/\mathbb{F}_p with CM by \mathcal{O}_K ;
 - A set of ideals of small norm $S \subset \text{Cl}(\mathcal{O}_K)$.
- 1 **Alice** takes a **secret** random walk $\mathfrak{a} = \prod_{\mathfrak{s} \in S} \mathfrak{s}^{e_{\mathfrak{s}}}$ defining an isogeny $E \rightarrow \mathfrak{a} * E$;
 - 2 **Bob** does the same;
 - 3 They publish $\mathfrak{a} * E$ and $\mathfrak{b} * E$;
 - 4 **Alice** repeats her secret walk \mathfrak{a} starting from $\mathfrak{b} * E$.
 - 5 **Bob** repeats his secret walk \mathfrak{b} starting from $\mathfrak{a} * E$.

How to evaluate an isogeny action

Input: A degree ℓ , a *direction* (left/right/...), [a point $P \in E$];

Output: The curve E/H , [the image $\phi(P) \in E/H$].

Elkies' algorithm

- Applies to any curve/degree/kernel;
- Complexity $O(\ell^2)$, very costly in practice;
- Outputs:
 - ▶ A kernel polynomial such that $h(P) = 0$ iff $P \in H$;
 - ▶ The image curve E/H (using Vélu's formulas).

Direct application of Vélu's formulas

- Only possible if $H \subset E(\mathbb{F}_p)$; $(\Leftrightarrow \ell \mid \#E(\mathbb{F}_p))$
- Complexity $O(\ell)$, very efficient;
- Outputs:
 - ▶ The image curve E/H .

CSIDH (pron.: *sea-side*)

Speeding up the CRS key exchange (De Feo, Kieffer, and Smith 2018)

- Choose p such that $\ell \mid (p + 1)$ for many small primes ℓ ;
- Look for random ordinary curves such that:
 - ▶ $\ell \mid \#E(\mathbb{F}_p)$,
 - ▶ technical condition;
- Use Vélu's formulas for those primes ℓ .
- ~ 5 minutes for a 128-bit secure key exchange

HARD!



CSIDH (Castryck, Lange, Martindale, Panny, and Renes 2018)

- Choose p such that $\ell \mid (p + 1)$ for many small primes ℓ ;
- Select a supersingular curve E/\mathbb{F}_p , automatically
 - ▶ $\#E(\mathbb{F}_p) = p + 1$,
 - ▶ technical condition always satisfied;
- ~ 100 ms for a 128 bits secure key exchange

EASY!



Key exchange with full supersingular graphs (over \mathbb{F}_{p^2})

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.

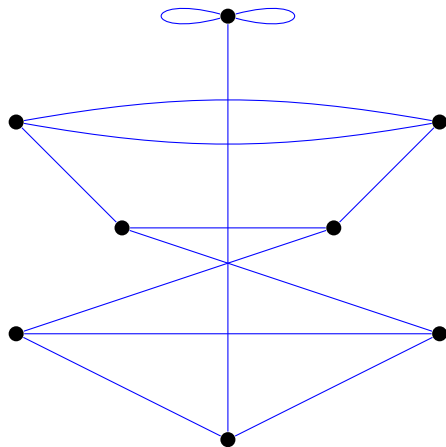


Figure: 2- and 3-isogeny graphs on \mathbb{F}_{97^2} .

Key exchange with full supersingular graphs (over \mathbb{F}_{p^2})

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.

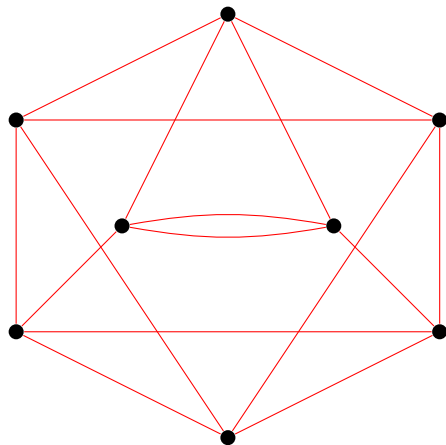


Figure: 2- and 3-isogeny graphs on \mathbb{F}_{97^2} .

Key exchange with full supersingular graphs (over \mathbb{F}_{p^2})

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.

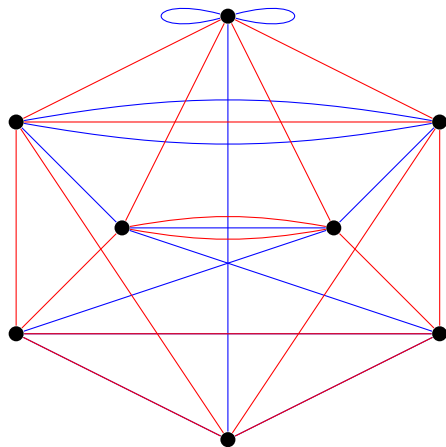


Figure: 2- and 3-isogeny graphs on \mathbb{F}_{97^2} .

Key exchange with full supersingular graphs (over \mathbb{F}_{p^2})

- 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 $l_A^{e_A}$
=
Kernel $\langle P \rangle \subset E[l_A^{e_A}]$

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

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

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

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

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E/\langle P \rangle \\ \psi \downarrow & & \downarrow \psi' \\ E/\langle Q \rangle & \xrightarrow{\phi'} & E/\langle P, Q \rangle \end{array}$$

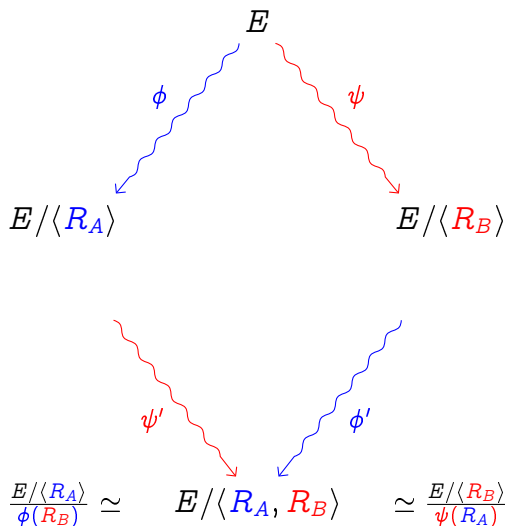
Supersingular Isogeny Diffie-Hellman¹

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:

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



¹Jao and De Feo 2011; De Feo, Jao, and Plût 2014.

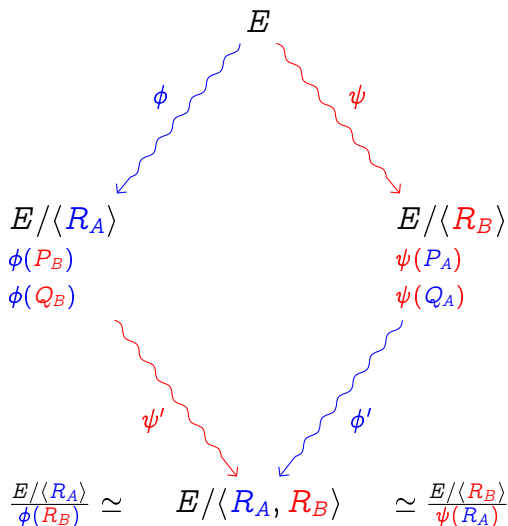
Supersingular Isogeny Diffie-Hellman¹

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:

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



¹Jao and De Feo 2011; De Feo, Jao, and Plût 2014.

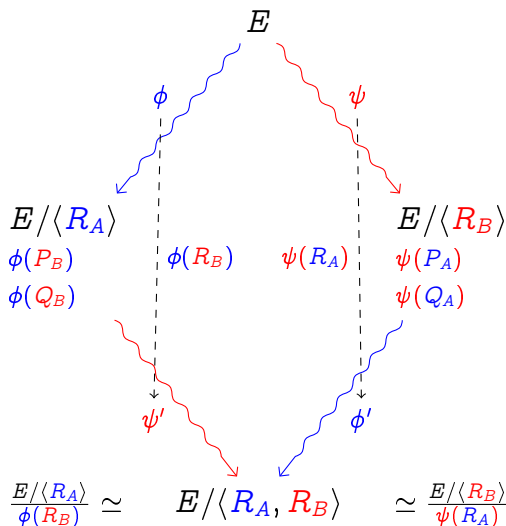
Supersingular Isogeny Diffie-Hellman¹

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:

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



¹Jao and De Feo 2011; De Feo, Jao, and Plût 2014.

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.
- Download the package [here](#).

	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

CSIDH vs SIDH

	CSIDH	SIDH
Speed (NIST 1)	<100ms	~ 10ms
Public key size (NIST 1)	64B	378B
Key compression ²		~ 15ms ³
↳ speed		222B
↳ size		yes
Constant time impl.	not yet	yes
Submitted to NIST	no	yes
Best classical attack	$p^{1/4}$	$p^{1/4}$
Best quantum attack	$\tilde{O}\left(3\sqrt{\log_3 p}\right)$	$p^{1/6}$
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	short but slooow!	big and slow

²Zanon, Simplicio, Pereira, Doliskani, and Barreto 2018.

³<https://twitter.com/PatrickLonga/status/1002313366466015232?s=20>

SIDH/SIKE: what's under the hood?

For efficiency: $p = 2^a 3^b - 1$, with a even;

For security:

$$a \sim (\log_2 3)b \geq \begin{cases} 2 \times \text{classical security parameter,} \\ 3 \times \text{quantum security parameter;} \end{cases}$$

For verifiability:

- Special starting curve $E_0 : y^2 = x^3 + x$;
- P_A, Q_A, P_B, Q_B chosen as the lexicographically first points satisfying the necessary conditions.

Implementation: finite field

Arithmetic in \mathbb{F}_p

- $p = 2^a 3^b - 1$ lends itself to optimizations:
 - ▶ Adapted Comba-based Montgomery reduction^a,
 - ▶ Adapted Barret reduction^b;
 - ▶ Assembly optimized.

^aCostello, Longa, and Naehrig 2016.

^bKarmakar, Roy, Vercauteren, and Verbauwhede 2016.

Arithmetic in \mathbb{F}_{p^2}

Because $p \equiv -1 \pmod{4}$, then -1 is not a quadratic residue in \mathbb{F}_p . We define $\mathbb{F}_{p^2} = \mathbb{F}_p[i] = \mathbb{F}_p[X]/(X^2 + 1)$.

- Arithmetic similar to $\mathbb{Q}[i]$;
- Karatsuba-like formulas for multiplication and squaring;
- Inversion only requires one inversion in \mathbb{F}_p ;
- Optimizations similar to pairing-base crypto (e.g., BN254).

Implementation: curves

Montgomery curves

Not a Weierstrass equation:

$$by^2 = x^3 + ax^2 + x$$

- Only possible for curves with a 4-torsion point (we're lucky);
- Very efficient arithmetic in XZ -coordinates: identify $\pm P$ by dropping the Y -coordinate

Doubling:

$$[2](X : \cdot : Z) = ((X^2 - Z^2)^2 : \cdot : 4XZ(X^2 + aXZ + Z^2))$$

Tripling:

$$[3](X : \cdot : Z) = (X(X^4 - 6X^2Z^2 - 4aXZ^3 - 3Z^4) : \cdot : Z(3X^4 + 4aX^3Z + 6X^2Z^3 - Z^4))$$

Implementation: curves

Computing $mP + nQ$

- Observe that $mP + nQ$ and $P + (n/m)Q$ generate the same isogeny kernel;
- Constant time Montgomery ladder tailored^a to $P + cQ$.
- For simplicity and constant-time sampling, SIKE secret keys are restricted to $P + cQ$ with $c \in [0, \dots, 2^x - 1]$.

^aFaz-Hernández, López, Ochoa-Jiménez, and Rodríguez-Henríquez 2017.

Input $P = (X_P : Z_P)$, $Q = (X_Q : Z_Q)$, $P - Q = (X_{P-Q} : Z_{P-Q})$,
a scalar c ;

Output $P + cQ$.

- 1 Set $R_0 = Q$, $R_1 = P$, $R_2 = Q - P$
- 2 For i from 0 to $\lfloor \log_2 c \rfloor$:
 - ▶ if $c_i = 0$, let $R_0, R_1 = 2R_0, R_0 + R_1$;
 - ▶ if $c_i = 1$, let $R_0, R_2 = 2R_0, R_0 + R_2$;
- 3 Return R_1 .

Implementation: isogenies

Vélu's formulas

Given a group $G \subset E$, the isogeny $\phi : E \rightarrow E/G$ is defined by:

$$\phi(P) = \left(x(P) + \sum_{Q \in G \setminus \{\mathcal{O}\}} x(P+Q) - x(Q), y(P) + \sum_{Q \in G \setminus \{\mathcal{O}\}} y(P+Q) - y(Q) \right).$$

3-isogenies of Montgomery curves

Let $P = (X_3 : Z_3)$ be a point of order 3 on $by^2 = x^3 + ax^2 + x$. The curve $E/\langle P \rangle$ has equation $by^2 = x^3 + a'x^2 + x$ where

$$a' = (aX_3Z_3 + 6(Z_3^2 - X_3^2))X_3/Z_3^3.$$

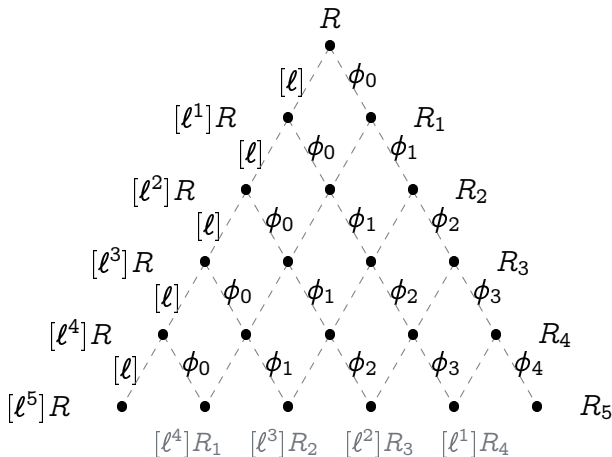
It is defined by the map

$$\phi(X : Z) = (X(X_3X - Z_3Z)^2 : Z(Z_3X - X_3Z)^2).$$

Similar formula for 4-isogenies.

Implementation: isogeny walks

$\text{ord}(R) = \ell^e$ and $\phi = \phi_0 \circ \phi_1 \circ \dots \circ \phi_{e-1}$, each of degree ℓ



For each i , one needs to compute $[\ell^{e-i}] R_i$ in order to compute ϕ_i .

Implementation: isogeny walks



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

- Right edges are ℓ -isogeny evaluation;
- Left edges are multiplications by ℓ (about twice as expensive);
- The best strategy can be precomputed offline and hardcoded.
- Evaluation is done in constant time!
- Pre-computed optimized strategies are given in the SIKE submission document.

Example

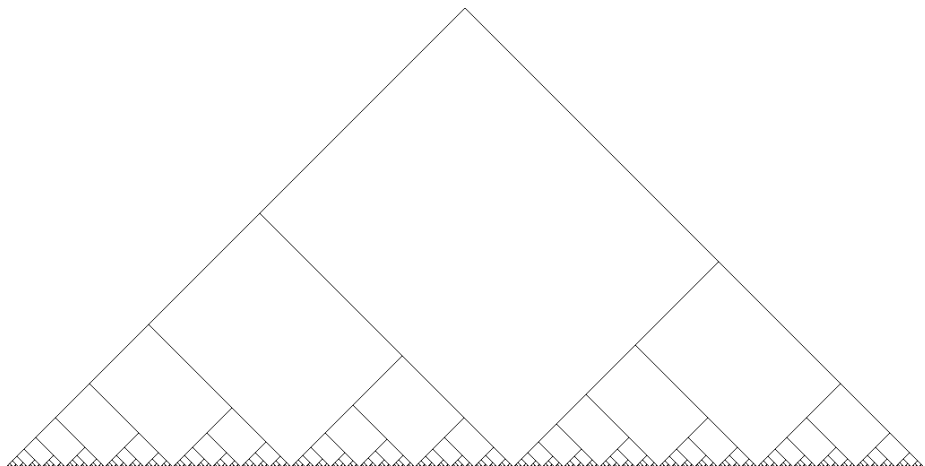


Figure: Optimal strategy for $e = 512, \ell = 2$.

Implementation: constant time

- Secret key sampling in constant time by restricting key space;
- $P + cQ$ in constant time via Montgomery ladder;
- Isogeny walk in constant time via any strategy.

Finite field operations in constant time

Only problem is to avoid inversions as much as possible, but Vélu's formulas require one inversion per curve on the walk.

Solution^a: projectivize curve equations

$$E : CB y^2 = Cx^3 + Ax^2 + Cx.$$

- Slightly increases operation counts of formulas;
- Delays all inversions to the very end;
- Only the value $(A : C)$ is needed in computations. Then:

$$j(E) = \frac{256(A^2 - 3C^2)}{C^4(A^2 - 4C^2)}.$$

^aCostello, Longa, and Naehrig 2016.

Summary

Public parameters:

- $p = 2^a 3^b - 1$,
- Staring curve $E : y^2 = x^3 + x$,
- Torsion generators

$$P_A = (X_{a1} : Z_{a1}), \quad Q_A = (X_{a2} : Z_{a2}), \quad P_A - Q_A = (X_{a3} : Z_{a3}),$$
$$P_B = (X_{b1} : Z_{b1}), \quad Q_B = (X_{b2} : Z_{b2}), \quad P_B - Q_B = (X_{b3} : Z_{b3}).$$

Secret keys:

- $R_A = P_A + cQ_A$ with $c \in [0, \dots, 2^a - 1]$,
- $R_B = P_B + cQ_B$ with $c \in [0, \dots, 2^{b \lceil \log_2 3 \rceil} - 1]$.

Public keys (curve equation can be interpolated from three points):

- $\phi(P_B), \phi(Q_B), \phi(P_B - Q_B)$,
- $\psi(P_A), \psi(Q_A), \psi(P_A - Q_A)$.


Shared secret:

- $j = 256(A^2 - 3C^2)/C^4(A^2 - 4C^2)$.



Thank you

<https://defeo.lu/>

 @luca_defeo

References I



De Feo, Luca, Jean Kieffer, and Benjamin Smith (2018).
“Towards practical key exchange from ordinary isogeny graphs.”
In: to appear in ASIACRYPT 2018.



Castricky, Wouter, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes (2018).
“CSIDH: An Efficient Post-Quantum Commutative Group Action.”
In: to appear in ASIACRYPT 2018.

References II



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 III



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 IV



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>.



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.