

Breaking SIDH in polynomial time

2022/09/13 — LFANT seminar, Bordeaux

Damien Robert

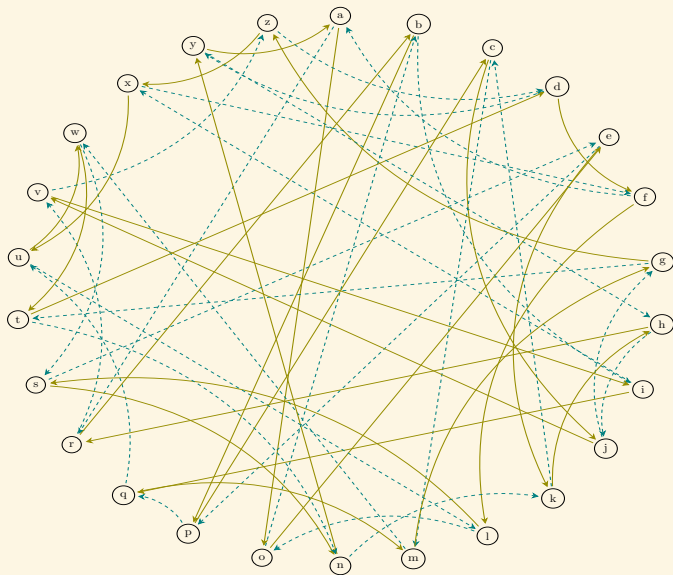
Équipe LFANT, Inria Bordeaux Sud-Ouest



université
de BORDEAUX

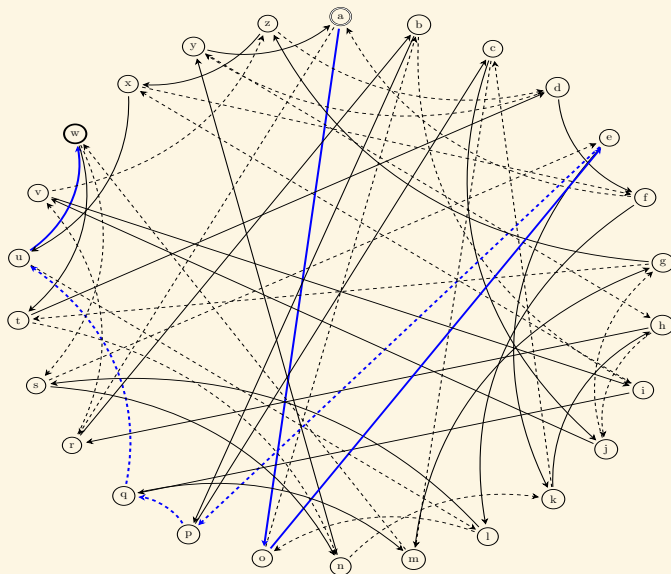


Key exchange on a (commutative) graph



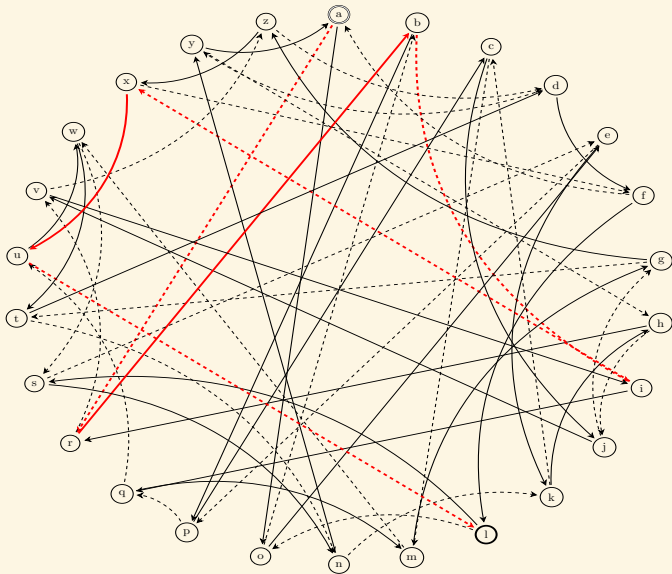
Key exchange on a (commutative) graph

Alice starts from 'a', follows the path 001110, and get 'w'.



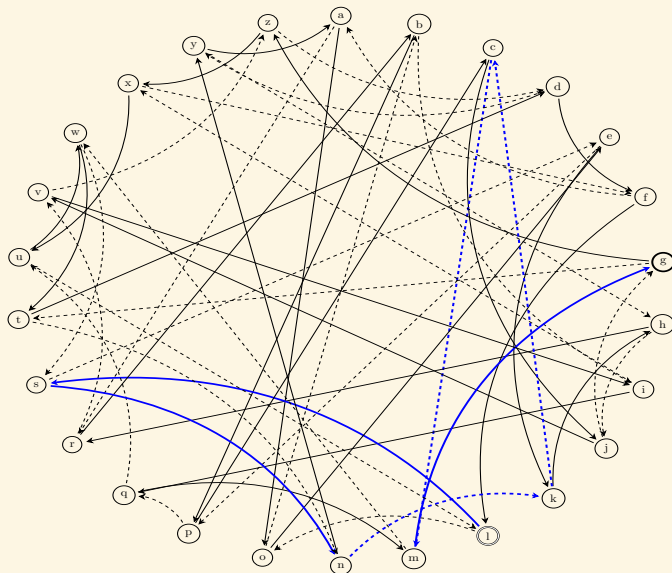
Key exchange on a (commutative) graph

Bob starts from 'a', follows the path 101101, and get 'l'.



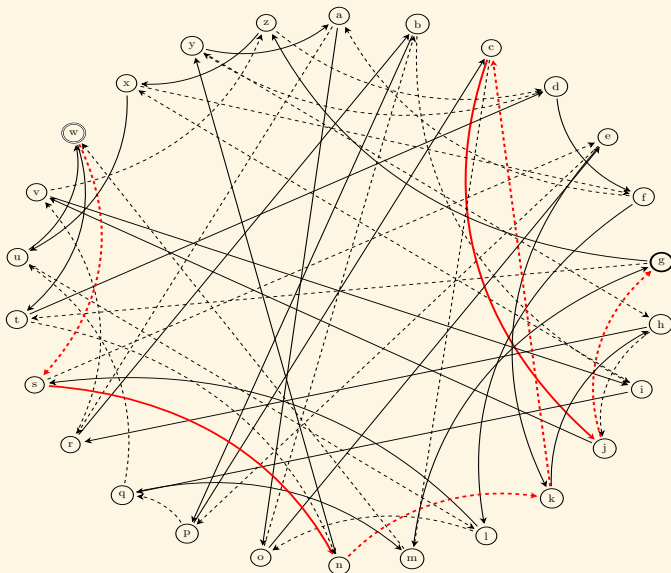
Key exchange on a (commutative) graph

Alice starts from 'l', follows the path 001110, and get 'g'.



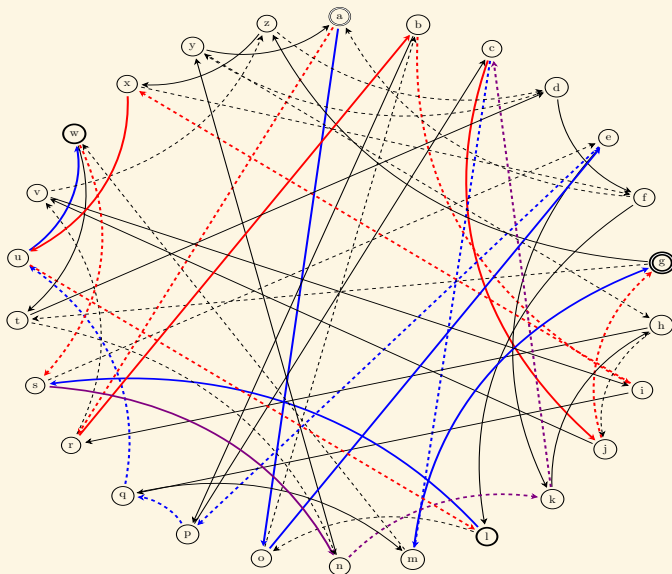
Key exchange on a (commutative) graph

Bob starts from 'w', follows the path 101101, and get 'g'.



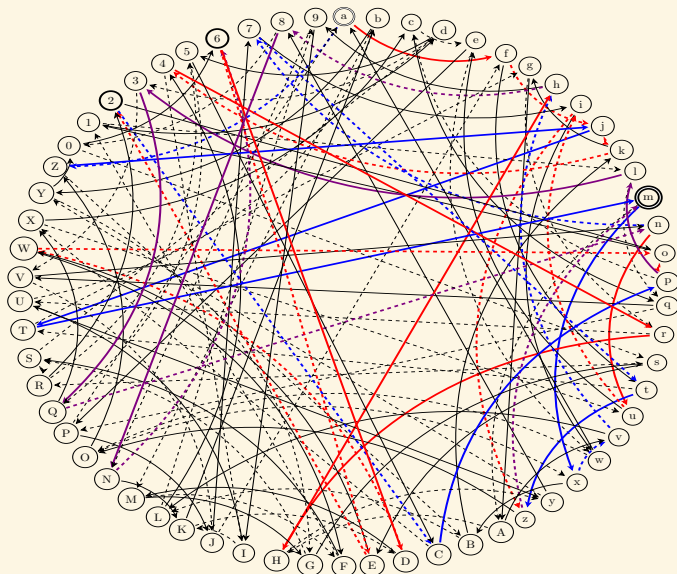
Key exchange on a (commutative) graph

The full exchange:



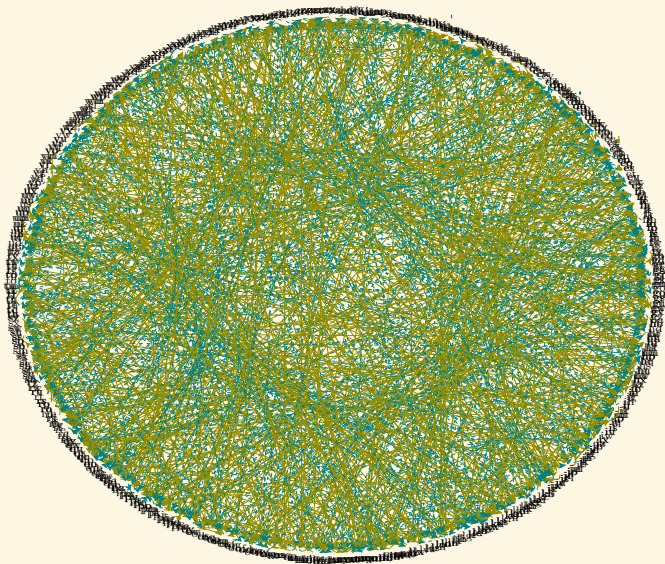
Key exchange on a (commutative) graph

Bigger graph (62 nodes)



Key exchange on a (commutative) graph

Even bigger graph (676 nodes)



Graph size for 128 bits of security (arbitrary graph)

- Need a graph with good mixing properties:
A path of length $O(\log N)$ gives a uniform node \Rightarrow Ramanujan/expander graph.
- Finding a path by exhaustive search: $O(N)$.
- Grover (quantum): $O(\sqrt{N})$.
- Meet in the middle: $\tilde{O}(\sqrt{N})$ and $O(\sqrt{N})$ memory.
- Time/Memory trade off: van Oorschot-Wiener Golden Collision Claw Finding.
 $\tilde{O}\left(\frac{N^{3/4}}{\sqrt{M}}\right)$ with $O(M)$ -memory ($M \leq \sqrt{N}$).
- Quantum claw finding: $\tilde{O}(N^{1/3})$ but needs $\tilde{O}(N^{1/3})$ memory.
- Tani's quantum claw finding algorithm:
find $g_1(x) = g_2(y)$ in $O(\#X^{2/3})$ where $g_1 : X \rightarrow Z, g_2 : Y \rightarrow Z, \#Z \gg \#X \approx \#Y$
(generalized Grover).
- Needs $N \approx 2^{256}$ or $N \approx 2^{384}$.
- The graph does not fit in memory.
- Need an algorithm taking a node as input and giving the neighbour nodes as output.



Isogeny graph of ordinary elliptic curves [Couveignes (1997)], [Rostovtsev–Stolbunov (2006)]

- Isogeny graph of an ordinary elliptic curve E/\mathbb{F}_p .
 - Graph of size $\approx \sqrt{p}$.
 - Torsor (principal homogeneous space) under the class group $\text{Cl}(\text{End}(E_0))$.
 - Hard to find good parameters.
 - CSIDH: supersingular elliptic curves over \mathbb{F}_p , torsor under $\text{Cl}(\mathbb{Z}[\sqrt{-p}])$.
- 😊 Commutative graph!
- ☹ Hidden shift problem solvable in quantum subexponential $L(1/2)$ time for an abelian group action via Kuperberg's algorithm.



SIDH: supersingular elliptic curve Diffie-Hellmann [De Feo, Jao (2011)][De Feo, Jao, Plût (2014)]

- Use the isogeny graph of a supersingular elliptic curve E over \mathbb{F}_{p^2} .
- There are $\approx p/12$ nodes and the graph is an expander graph.
- The endomorphism ring is a quaternion algebra (ramified at p and infinity), which is non commutative.
- The isogeny graph is a Cayley graph for the class groupoid.
- Non commutative graph.

- Practical parameters: $p + 1 = 2^a 3^b$ with $2^a \approx 3^b$
- $E(\mathbb{F}_{p^2}) \simeq \mathbb{Z}/(p+1)\mathbb{Z} \times \mathbb{Z}/(p+1)\mathbb{Z}$ has rational 2^a and 3^b -torsion.
- Paths given by 2^a and 3^b isogenies: $O(\sqrt{p})$ possible paths.
- Attacks: $p^{1/4}$ (classical) or $p^{1/6}$ (Tani's quantum claw algorithm).

⇒ For 128 bits of security, needs p of 512 bits or 768 bits.

- SIKE: supersingular isogeny key encapsulation (KEM).
- Short key size: $3.5 \log p$ via key compression.

Total key size: 1792 or 2688 bits



SIDH: supersingular elliptic curve Diffie-Hellmann [De Feo, Jao (2011)][De Feo, Jao, Plût (2014)]

Meme: Gru's plan

- Isogeny based key exchange
- Use supersingular curves
- The graph is non commutative
- The graph is non commutative

SIDH in practice

- $p = 2^a 3^b - 1$, $N_A = 2^a$, $N_B = 3^b$, N_A prime to N_B .
- $E_0 : y^2 = x^3 + x$ (supersingular when $a \geq 2$) or $E_0 : y^2 = x^3 + 6x^2 + x$.
- $E_0[N_A] = \langle P_A, Q_A \rangle$, $E_0[N_B] = \langle P_B, Q_B \rangle$.
- Alice's **secret** isogeny: ϕ_A of kernel $\langle P_A + s_A Q_A \rangle$.
- Bob's **secret** isogeny: ϕ_B of kernel $\langle P_B + s_B Q_B \rangle$.
- Key exchange:

$$\begin{array}{ccc}
 E_0 & \xrightarrow{\phi_B} & E_B \\
 \downarrow \phi_A & & \downarrow \phi'_A \\
 E_A & \xrightarrow{\phi'_B} & E_{AB}
 \end{array}$$

- E_{AB} is the **shared secret**.
- $\phi'_A \circ \phi_B = \phi'_B \circ \phi_A : E_0 \rightarrow E_{AB}$ has kernel $\text{Ker } \phi_A + \text{Ker } \phi_B$.
- ϕ'_A has kernel $\phi_B(P_A + s_A Q_A)$, ϕ'_B has kernel $\phi_A(P_B + s_B Q_B)$.
- Alice publishes: $P'_B = \phi_A(P_B)$, $Q'_B = \phi_A(Q_B)$.
Bob publishes: $P'_A = \phi_B(P_A)$, $Q'_A = \phi_B(Q_A)$. ("Torsion points".)
- $\text{Ker } \phi'_A = \langle P'_A + s_A Q'_A \rangle$, $\text{Ker } \phi'_B = \langle P'_B + s_B Q'_B \rangle$.
- Key exchange in $\tilde{O}(\log N_A \ell_A^{1/2} + \log N_B \ell_B^{1/2})$

(Via fast smooth isogeny computation [De Feo, Jao, Plût (2014)] and Velusqrt [Bernstein, De Feo, Leroux, Smith (2020)]).



SIDH in practice

- $p = 2^a 3^b - 1$, $N_A = 2^a$, $N_B = 3^b$, N_A prime to N_B .
- $E_0 : y^2 = x^3 + x$ (supersingular when $a \geq 2$) or $E_0 : y^2 = x^3 + 6x^2 + x$.
- $E_0[N_A] = \langle P_A, Q_A \rangle$, $E_0[N_B] = \langle P_B, Q_B \rangle$.
- Alice's **secret** isogeny: ϕ_A of kernel $\langle P_A + s_A Q_A \rangle$.
- Bob's **secret** isogeny: ϕ_B of kernel $\langle P_B + s_B Q_B \rangle$.
- Key exchange:

$$\begin{array}{ccc}
 E_0 & \xrightarrow{\phi_B} & E_B \\
 \downarrow \phi_A & & \downarrow \phi'_A \\
 E_A & \xrightarrow{\phi'_B} & E_{AB}
 \end{array}$$

- E_{AB} is the **shared secret**.
- $\phi'_A \circ \phi_B = \phi'_B \circ \phi_A : E_0 \rightarrow E_{AB}$ has kernel $\text{Ker } \phi_A + \text{Ker } \phi_B$.
- ϕ'_A has kernel $\phi_B(P_A + s_A Q_A)$, ϕ'_B has kernel $\phi_A(P_B + s_B Q_B)$.
- Alice publishes: $P'_B = \phi_A(P_B)$, $Q'_B = \phi_A(Q_B)$.
Bob publishes: $P'_A = \phi_B(P_A)$, $Q'_A = \phi_B(Q_A)$. ("Torsion points").
- $\text{Ker } \phi'_A = \langle P'_A + s_A Q'_A \rangle$, $\text{Ker } \phi'_B = \langle P'_B + s_B Q'_B \rangle$.
- Key exchange in $\tilde{O}(\log N_A \ell_A^{1/2} + \log N_B \ell_B^{1/2})$

(Via fast smooth isogeny computation [De Feo, Jao, Plût (2014)] and Velusqrt [Bernstein, De Feo, Leroux, Smith (2020)]).



SIDH in practice

- $p = 2^a 3^b - 1$, $N_A = 2^a$, $N_B = 3^b$, N_A prime to N_B .
- $E_0 : y^2 = x^3 + x$ (supersingular when $a \geq 2$) or $E_0 : y^2 = x^3 + 6x^2 + x$.
- $E_0[N_A] = \langle P_A, Q_A \rangle$, $E_0[N_B] = \langle P_B, Q_B \rangle$.
- Alice's **secret** isogeny: ϕ_A of kernel $\langle P_A + s_A Q_A \rangle$.
- Bob's **secret** isogeny: ϕ_B of kernel $\langle P_B + s_B Q_B \rangle$.
- Key exchange:

$$\begin{array}{ccc}
 E_0 & \xrightarrow{\phi_B} & E_B \\
 \downarrow \phi_A & & \downarrow \phi'_A \\
 E_A & \xrightarrow{\phi'_B} & E_{AB}
 \end{array}$$

- E_{AB} is the **shared secret**.
- $\phi'_A \circ \phi_B = \phi'_B \circ \phi_A : E_0 \rightarrow E_{AB}$ has kernel $\text{Ker } \phi_A + \text{Ker } \phi_B$.
- ϕ'_A has kernel $\phi_B(P_A + s_A Q_A)$, ϕ'_B has kernel $\phi_A(P_B + s_B Q_B)$.
- Alice publishes: $P'_B = \phi_A(P_B)$, $Q'_B = \phi_A(Q_B)$.
Bob publishes: $P'_A = \phi_B(P_A)$, $Q'_A = \phi_B(Q_A)$. ("Torsion points".)
- $\text{Ker } \phi'_A = \langle P'_A + s_A Q'_A \rangle$, $\text{Ker } \phi'_B = \langle P'_B + s_B Q'_B \rangle$.
- Key exchange in $\tilde{O}(\log N_A \ell_A^{1/2} + \log N_B \ell_B^{1/2})$

(Via fast smooth isogeny computation [De Feo, Jao, Plût (2014)] and Velusqrt [Bernstein, De Feo, Leroux, Smith (2020)]).



SIDH in practice

- $p = 2^a 3^b - 1$, $N_A = 2^a$, $N_B = 3^b$, N_A prime to N_B .
- $E_0 : y^2 = x^3 + x$ (supersingular when $a \geq 2$) or $E_0 : y^2 = x^3 + 6x^2 + x$.
- $E_0[N_A] = \langle P_A, Q_A \rangle$, $E_0[N_B] = \langle P_B, Q_B \rangle$.
- Alice's **secret** isogeny: ϕ_A of kernel $\langle P_A + s_A Q_A \rangle$.
- Bob's **secret** isogeny: ϕ_B of kernel $\langle P_B + s_B Q_B \rangle$.
- Key exchange:

$$\begin{array}{ccc}
 E_0 & \xrightarrow{\phi_B} & E_B \\
 \downarrow \phi_A & & \downarrow \phi'_A \\
 E_A & \xrightarrow{\phi'_B} & E_{AB}
 \end{array}$$

- E_{AB} is the **shared secret**.
- $\phi'_A \circ \phi_B = \phi'_B \circ \phi_A : E_0 \rightarrow E_{AB}$ has kernel $\text{Ker } \phi_A + \text{Ker } \phi_B$.
- ϕ'_A has kernel $\phi_B(P_A + s_A Q_A)$, ϕ'_B has kernel $\phi_A(P_B + s_B Q_B)$.
- Alice publishes: $P'_B = \phi_A(P_B)$, $Q'_B = \phi_A(Q_B)$.
Bob publishes: $P'_A = \phi_B(P_A)$, $Q'_A = \phi_B(Q_A)$. ("Torsion points").
- $\text{Ker } \phi'_A = \langle P'_A + s_A Q'_A \rangle$, $\text{Ker } \phi'_B = \langle P'_B + s_B Q'_B \rangle$.
- Key exchange in $\tilde{O}(\log N_A \ell_A^{1/2} + \log N_B \ell_B^{1/2})$

(Via fast smooth isogeny computation [De Feo, Jao, Plût (2014)] and Velusqrt [Bernstein, De Feo, Leroux, Smith (2020)]).



- Standardized KEM: Kyber (structured lattice)
- Standardized signatures: Dilithium, Falcon (structured lattices), SPHINCS (hash function)
- Fourth round KEM: BIKE, HQC (structured codes), Classic McEliece (code), SIKE (SIDH).

Meme: distracted boyfriend

- NIST PQC
- Isogeny based crypto
- Lattice based crypto



Torsion points attacks

- Eve knows $E_0, E_B, P'_A = \phi_B(P_A), Q'_A = \phi_B(Q_A), P_A, Q_A$ basis of the N_A -torsion.
- Goal: recover $\phi_B : E_0 \rightarrow E_B$, an N_B -isogeny.
- [Petit (2017)]: build an isogeny α on E_0 and combine it with ϕ_B (and/or $\widetilde{\phi_B}$) to get an N_A -isogeny F .
- Recover $\text{Ker } F \subset E_0[N_A]$: we know the action of ϕ_B on the N_A -torsion!
- We know the action of ϕ_B on $E_0[N_A]$ so we also know the action of $\widetilde{\phi_B}$ on $E_B[N_A]$, so we can also use $\widetilde{\phi_B}$ to build F .
- Compute F via an isogeny algorithm.
- Extract ϕ_B from F .



N-isogenies

- Polarised abelian variety (A, λ_A) : where $\lambda_A : A \rightarrow \widehat{A}$ is an isogeny
Technicality: the morphism λ_A needs to be induced from a divisor, $\Leftrightarrow \widehat{\widehat{\lambda_A}} : \widehat{\widehat{A}} \simeq A \rightarrow \widehat{A} = \lambda_A$.
- Principal polarisation: λ_A is an isomorphism \Rightarrow principally polarized abelian variety (ppav)
- $f : (A, \lambda_A) \rightarrow (B, \lambda_B)$ is an N -isogeny between ppav if $f^* \lambda_B = N \lambda_A$.
- Dual isogeny: $\widehat{f} : \widehat{B} \rightarrow \widehat{A}$
- Contragredient isogeny / Dual with respect to the principal polarisations: $\widetilde{f} = \lambda_A^{-1} \widehat{f} \lambda_B : B \rightarrow A$

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \lambda_A^{-1} \uparrow & & \downarrow \lambda_B \\ \widehat{A} & \xleftarrow{\widehat{f}} & \widehat{B} \end{array}$$

- f is an N -isogeny $\Leftrightarrow \widetilde{f} f = N \Leftrightarrow f \widetilde{f} = N$.
- $\text{Ker } f = \text{Im } \widetilde{f} \mid B[N]$.

Algorithms for N -isogenies

- [Cosset-R. (2014), Lubicz-R. (2012–2022)]: An N -isogeny in dimension g can be evaluated in linear time $O(N^g)$ arithmetic operations in the theta model given generators of its kernel.
- Warning: exponential dependency 2^g or 4^g in the dimension g .
- [Couveignes-Ezome (2015)]: Algorithm in $O(N^g)$ in the Jacobian model.
- Not hard to extend to product of Jacobians.
- Restricted to $g \leq 3$.



N -isogenies and isotropic kernels

- $f : (A, \lambda_A) \rightarrow (B, \lambda_B)$ N -isogeny $\Rightarrow \text{Ker } f$ is maximal isotropic in $A[N]$ for the Weil pairing
- Conversely, if $K \subset A[N]$ maximal isotropic, $N\lambda_A$ descends to a principal polarisation on $B = A/K$.
- An elliptic curve only has one principal polarisation ($NS(E) = \mathbb{Z}$).
- So $f : E_1 \rightarrow E_2$ is an N -isogeny $\Leftrightarrow \# \text{Ker } f = N$.
- But in higher dimension there may be many non equivalent principal polarisations.

Example (Superspecial abelian surfaces)

$A = E^2, E/\mathbb{F}_{p^2}$ supersingular. It admits $\approx p^2/288$ product polarisations $(E_1 \times E_2, \lambda_{E_1} \times \lambda_{E_2})$ where E_1, E_2 are supersingular and $\approx p^3/2880$ indecomposable polarisations $(\text{Jac } C, \Theta_C)$ where C is an hyperelliptic curve of genus 2.

- If $f : (A, \lambda_A) \rightarrow (B, \lambda_B)$ has maximal isotropic kernel in $A[N]$, $N\lambda_A$ descends to a principal polarisation λ'_B on B .
- But we may have $\lambda'_B \neq \lambda_B$.
- $\tilde{f} \circ f = N$ is a stronger condition that ensures compatibility of f with λ_B .



Composition and product polarisations

- **Composition:** $f : A \rightarrow B$ a N -isogeny, $g : B \rightarrow C$ a M -isogeny, $g \circ f : A \rightarrow C$.
- $\widehat{g \circ f} = \hat{f} \circ \hat{g} : \hat{C} \rightarrow \hat{A}$;
- $\widetilde{g \circ f} = \tilde{f} \circ \tilde{g} : C \rightarrow A$;
- $(\widetilde{g \circ f}) \circ (g \circ f) = \tilde{f} \circ \tilde{g} \circ g \circ f = NM$.
- The **composition** $g \circ f$ is an NM -isogeny.
- Conversely, if $g \circ f$ is an N -isogeny and f (resp. g) is an M -isogeny, then g (resp. f) is an N/M -isogeny.
- **Product polarisation:** $(A, \lambda_A) \times (B, \lambda_B) = (A \times B, \lambda_A \times \lambda_B)$ where $\lambda_A \times \lambda_B : A \times B \rightarrow \hat{A} \times \hat{B}$ is the product.
- $F = \begin{pmatrix} a & c \\ b & d \end{pmatrix} : (A \times B, \lambda_A \times \lambda_B) \rightarrow (C \times D, \lambda_C \times \lambda_D)$.
- $\hat{F} = \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix} : \hat{C} \times \hat{D} \rightarrow \hat{A} \times \hat{B}$.
- $\tilde{F} = \begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix} : C \times D \rightarrow A \times B$.



Dimension 1 torsion points attacks

Recall: construct α and combine it with ϕ_B to get an N_A -isogeny F .

- [Petit (2017)]: $F = \phi_B \circ \gamma \circ \widetilde{\phi_B} + [d]$.

$$E_B \begin{array}{c} \xrightarrow{\widetilde{\phi_B}} \\ \xleftarrow{\phi_B} \end{array} E_0 \curvearrowright \gamma$$

- γ a c -endomorphism of E_0 of “trace 0”: $\tilde{\gamma} = -\gamma$.
- $\tilde{F} = -\phi_B \circ \gamma \circ \widetilde{\phi_B} + [d]$.
- $\tilde{F}F = N_B^2 c + d^2$.
- Find parameters b, d such that $N_A = b^2 c N_B^2 + d^2$, $F = b\phi_B \gamma \widetilde{\phi_B} + [d]$ is then an N_A -endomorphism on E_B .
- Extract ϕ_B from F .

⇒ Needs a non trivial endomorphism γ on E_0 .

⇒ Needs unbalanced parameters $N_A > N_B^2$.



Non trivial endomorphisms

- On $E_0 : y^2 = x^3 + x$, endomorphism $\gamma = [i]$ over \mathbb{F}_{p^2} ,

$$[i](x, y) = (-x, iy).$$

- $\widetilde{[i]} = [-i]$: the Rosati involution is the complex conjugation

- $\text{End}(E_0) \supset \mathbb{Z}[i]$.

- If $\alpha = a_1 + a_2i$, $\tilde{\alpha} = a_1 - a_2i$, $\tilde{\alpha} \circ \alpha = a_1^2 + a_2^2$.

- Can construct a -isogenies whenever $a = a_1^2 + a_2^2$.

- [QKLMPPS (2021)]: dimension 1 attack when $N_A^2 = b^2 N_B^2 + a^2$ (and other variants).



Meme: balloons

- SIDH: small key size
- SIDH: small key size; Torsion points

Building N -isogenies in higher dimension?

- $f \mapsto \tilde{f}$ behaves like the complex conjugation $z \mapsto \bar{z}$,
(or like the $*$ operator in a \mathbb{C}^* -algebra)
- $f \mapsto \tilde{f} \circ f$ behaves like the complex norm $z \mapsto \|z\| = \bar{z}z = |z|^2$.
- Matrix representation of the Gaussian integers $z = \alpha + \beta i, \alpha, \beta \in \mathbb{Z}$:

$$M_z = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}.$$

- $\widetilde{M_z} := M_z^* = \overline{M_z}^T = M_{\bar{z}} = \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}, \quad \widetilde{M_z} M_z = \alpha^2 + \beta^2 = a + b, \quad a = \|\alpha\|, b = \|\beta\|.$
- M_z combines an " a -endomorphism" α and a " b -endomorphism" β into a " $a + b$ -endomorphism" M_z provided α, β are "symmetric" ($\tilde{\alpha} = \alpha, \tilde{\beta} = \beta$).
- Generalisation: $\alpha = \alpha_1 + \alpha_2 i \in \mathbb{Z}[i]$ of norm $a = \|\alpha\|, \beta = \beta_1 + \beta_2 i \in \mathbb{Z}[i]$ of norm $b = \|\beta\|$
- $F = \begin{pmatrix} \alpha & \bar{\beta} \\ -\beta & \bar{\alpha} \end{pmatrix} \in \text{Mat}_2(\mathbb{Z}[i]).$
- $\tilde{F} := F^* = \bar{F}^T = \begin{pmatrix} \bar{\alpha} & -\bar{\beta} \\ \beta & \alpha \end{pmatrix}, \quad \tilde{F}F = \bar{\alpha}\alpha + \bar{\beta}\beta = \|\alpha\| + \|\beta\| = a + b = \alpha_1^2 + \alpha_2^2 + \beta_1^2 + \beta_2^2.$
- Matrix representation of Hamilton's quaternions $\mathbb{Z}[i, j, k]$.
- F combines an " a -endomorphism" and a " b -endomorphism" into a " $a + b$ -endomorphism".



- $\alpha : A \rightarrow B$ a a -isogeny, $\beta : A \rightarrow C$ a b -isogeny.
- $\alpha' : C \rightarrow D$ a a -isogeny, $\beta' : C \rightarrow D$ a b -isogeny with $\beta'\alpha = \alpha'\beta$:

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \downarrow \beta & & \downarrow \beta' \\ C & \xrightarrow{\alpha'} & D \end{array}$$

- NB: If a prime to b , the pushforward α', β' of α, β by β, α satisfy these conditions.
- $F = \begin{pmatrix} \alpha & \widetilde{\beta'} \\ -\beta & \widetilde{\alpha'} \end{pmatrix} : A \times D \rightarrow B \times C.$
- $\tilde{F} = \begin{pmatrix} \tilde{\alpha} & -\tilde{\beta} \\ \beta' & \alpha' \end{pmatrix} : B \times C \rightarrow A \times D, \quad \tilde{F}F = a + b.$
- F is an $a + b$ -isogeny with respect to the product polarisations.
- $\text{Ker } F = \{\tilde{\alpha}(P), \beta'(P) \mid P \in B[N_A]\}$ (if a is prime to b)

Dimension 2 attacks [Castrick-Decru (2022-07-30)], [Maino-Martindale (2022-08-08)]

- if $\alpha : E_0 \rightarrow E'_0$ is an a -isogeny, combine α with $\phi_B : E_0 \rightarrow E_B$ an N_B -isogeny to build an $N_B + a$ -isogeny: $F = E'_0 \times E_B \rightarrow E_0 \times E_X$.

$$\begin{array}{ccc} E_0 & \xrightarrow{\phi_B} & E_B \\ \downarrow \alpha & & \downarrow \alpha' \\ E'_0 & \xrightarrow{\phi'_B} & E_X \end{array}$$

- $F = \begin{pmatrix} \tilde{\alpha} & \widetilde{\phi_B} \\ -\phi'_B & \alpha' \end{pmatrix}$.
- $\text{Ker } F = \{\alpha(P), \phi_B(P) \mid P \in E_0[N_A]\}$.
- ϕ_B can be directly extracted from F .
- Needs a $a := N_A - N_B$ isogeny on E_0 .
- Breaking SIDH then reduces to evaluating the isogeny F in dimension 2.
- Cost $\tilde{O}(\log N_A \ell_A^2)$ arithmetic operations.



Dimension 2 attacks [Castrick-Decru (2022-07-30)], [Maino-Martindale (2022-08-08)]

Meme: disaster girl

- SIDH
- Higher dimensional isogenies

Dimension 2 attacks: general case

- Easy to construct smooth isogenies from E_0 .
- Look for parameters $N_A = bN_B + a$ with a, b smooth.
- Parameter tweaks: $eN_A = bN_B/D_B + a$, e small integer, D_B small divisor of N_B .
- [De Feo (2022-08-25)]: (heuristic) subexponential $L(1/2)$ attack (tweaks of subexponential size).



Dimension 2 attacks: NIST's starting curve [Castryck-Decru]

- When $E_0 : y^2 = x^3 + x$, $\text{End}(E_0) \supset \mathbb{Z}[i]$.
- Can efficiently build a -isogenies if $a := N_A - N_B = a_1^2 + a_2^2$.
- Probability: $\Omega(1/\sqrt{\log N_A})$ (heuristic).
- [Castryck-Decru]: (heuristic) polynomial time attack.
- Require factorisation oracles to decompose a as a sum of two squares.
- [Wesolowski (2022-08-12)]: if $\text{End}(E_0)$ is known, can always build an a -isogeny in proven polynomial time.
- Polynomial time precomputation (depending on E_0), then attack in $\tilde{O}(\log N_A \ell_A^2)$ arithmetic operations.
- Sage implementation: <https://github.com/jack4818/Castryck-Decru-SageMath>
- [R.], [Oudompheng]: Look for $N_A = (b_1^2 + b_2^2)N_B/D_B + (a_1^2 + a_2^2)$.
- Heuristic precomputation of $O(\log^3 N_A)$ then attack (heuristically) in $\tilde{O}(\log^2 N_A \ell_A^2)$ arithmetic operations.
- Can be reduced to $\tilde{O}(\log^{3/2} N_A \ell_A^2)$ with $O(\log^{1/2} N_A)$ factorisation calls.



Revisiting the general case

Recall: we need to construct an $a := N_A - N_B$ isogeny on E_0 .

- If X is **generic**: can build smooth isogenies or the d^2 -endomorphism $[d]$.
- But on X^2 , for $a_1, a_2 \in \mathbb{Z}$, $\alpha = \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix}$ is an $a_1^2 + a_2^2$ -endomorphism.
- More generally, if α_1 is an a_1 -endomorphism, α_2 an a_2 -endomorphism of X and $\alpha_1\alpha_2 = \alpha_2\alpha_1$,
 $\alpha = \begin{pmatrix} \alpha_1 & \tilde{\alpha}_2 \\ -\alpha_2 & \tilde{\alpha}_1 \end{pmatrix}$ is an $a_1 + a_2$ -endomorphism on X^2 .
- So if $a = a_1^2 + a_2^2 + a_3^2 + a_4^2$, we can build an $a_1^2 + a_2^2$ endomorphism on X^2 , an $a_3^2 + a_4^2$ endomorphism on X^2 , and an a -endomorphism on X^4 .
- Decomposition of a as a **sum of four squares**: randomized polynomial time $\tilde{O}(\log^2 a)$.

\Rightarrow We can **always** build an a -endomorphism on E_0^4 !

Meme: Panik

- SIDH is broken (Panik)
- We can just start with a random curve (Kalm)
- It's still broken (Panik)

Dimension 8 attack in the general case [R. (2022-08-10)]

- Assume $N_A > N_B$.
- $a := N_A - N_B$. Decompose $a = a_1^2 + a_2^2 + a_3^2 + a_4^2$ to build α an a -endomorphism on E_0^4 .

$$\begin{array}{ccc} E_0^4 & \xrightarrow{\phi_B} & E_B^4 \\ \downarrow \alpha & & \downarrow \alpha \\ E_0^4 & \xrightarrow{\phi_B} & E_B^4 \end{array}$$

- $F = \begin{pmatrix} \alpha & \widetilde{\phi_B} \\ -\phi_B & \tilde{\alpha} \end{pmatrix} \in \text{End}(E_0^4 \times E_B^4)$.
- $\text{Ker } F = \{\tilde{\alpha}(P), \phi_B(P) \mid P \in E_0[N_A]\}$.
- **Breaking SIDH in the general case** reduces to evaluating the isogeny F in dimension 8.
- Precomputation: randomized $O(\log^2 N_A)$.
- Attack: $\widetilde{O}(\log N_A \ell_A^8)$ arithmetic operations.
- **Quasi-linear** if $\ell_A = O(1)$ (or $\ell_A = O(\log \log N_A)$).
- Actually only need $N_A^2 > N_B$: we can reconstruct the N_A^2 -isogeny F from its action on the N_A -torsion.



Dimension 4 attack in the general case [R. (2022-08-10)]

- If $N_A^2 = (b_1^2 + b_2^2)N_B + (a_1^2 + a_2^2)$, we can construct β a $b_1^2 + b_2^2$ -endomorphism, α a $a_1^2 + a_2^2$ -endomorphism on E_0^2 .
- F is a N_A^2 -endomorphism on $E_0^2 \times E_B^2$.
- Attack: $\tilde{O}(\log N_A \ell_A^4)$ arithmetic operations.
- Precomputation in (randomized heuristic) $\tilde{O}(\log^3 N_A)$.



- Publishing the image of the torsion points was a **key weakness**.

Meme: Anakin

- I have a nice key exchange protocol
- You don't use torsion points , right?
- ...
- Right?

Lessons learned

- Publishing the image of the torsion points was a **key weakness**.
- CSIDH, SQISign **still secure**.

Meme: new friend

- Friendship ended with supersingular curves
- Now ordinary elliptic curve is my best friend

Meme: left exit

- SIDH; SQISign
- Isogeny based crypto



Lessons learned

- Publishing the image of the torsion points was a *key weakness*.
- CSIDH, SQISign *still secure*.
- No post-quantum *isogeny based KEM* with exponential quantum security anymore.
(OSIDH, masking torsion points [*Moriya, Fouotsa*]?)

Meme: chosen one

- When SIDH gets broken
- No, you were supposed to keep elliptic curves quantum resistant, not betray them



- **Embedding lemma**: for any $N' > N$, a N -isogeny $f : A \rightarrow B$ in dimension g can always be efficiently embedded into a N' -isogeny in dimension $8g$ (and sometimes $4g$ or $2g$).
- ⇒ An N -isogeny f over a finite field always admit an **efficient representation** which allows for evaluation in **polylogarithmic time** [R. (2022-08-17)]. (Take N' power smooth.)



- Can we use this new toolbox to build new cryptosystems or break other existing ones?

Meme: Buzz

- Higher dimensional isogenies
- Higher dimensional isogenies everywhere

Meme: funeral

- SIDH
- 2011-2022