

Attacks on SIDH and applications

2024/07/18 — PQC Summer School, China

Damien Robert

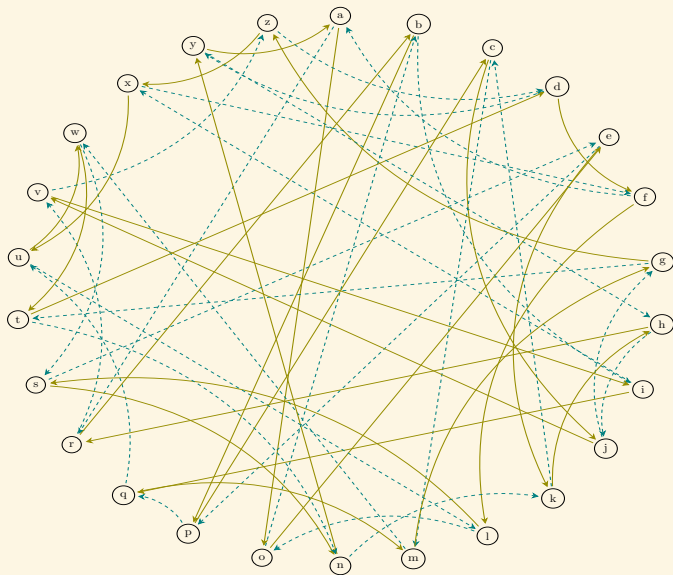
Équipe Canari, Inria Bordeaux Sud-Ouest



université
de BORDEAUX

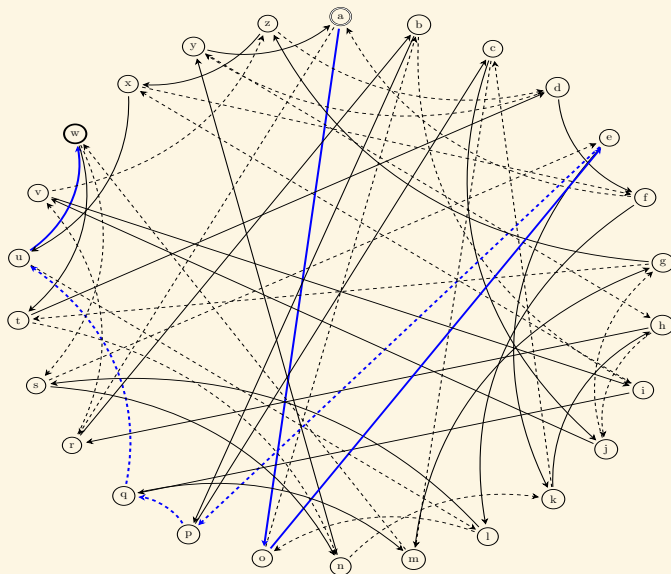
Inria

Key exchange on a (commutative) graph



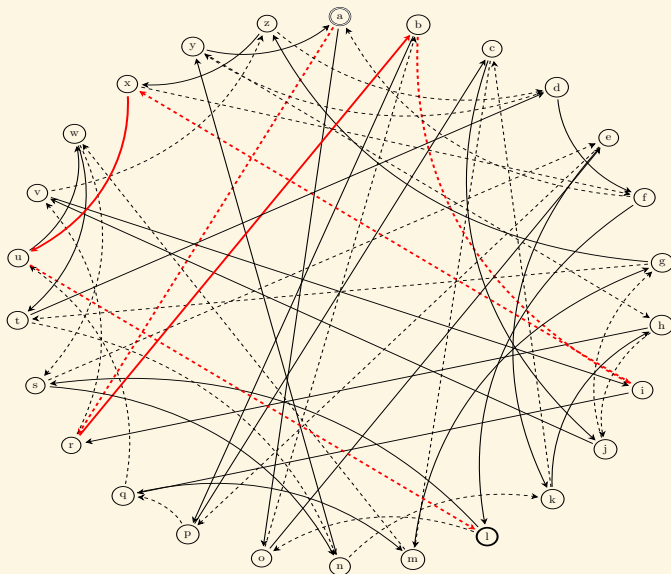
Key exchange on a (commutative) graph

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



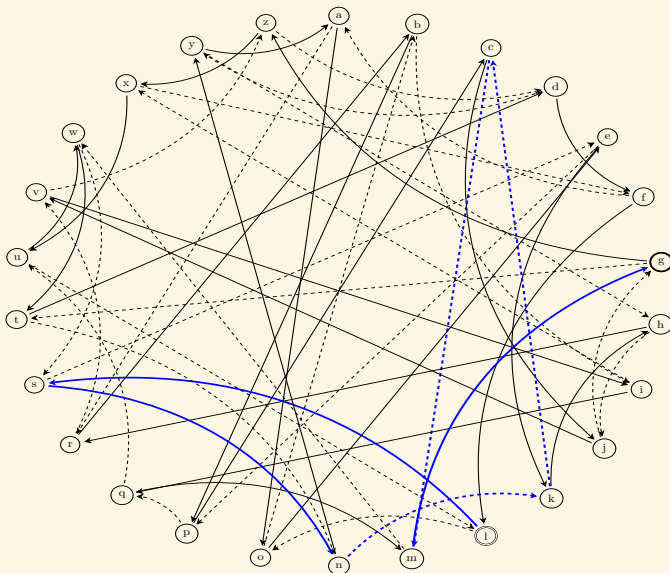
Key exchange on a (commutative) graph

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



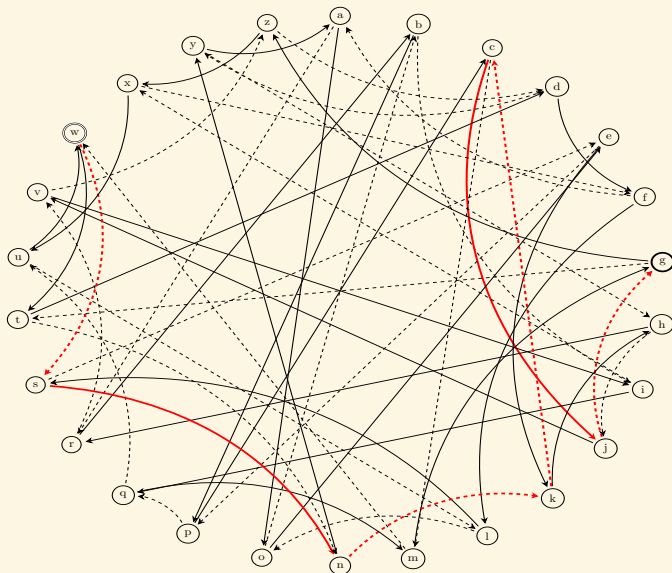
Key exchange on a (commutative) graph

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



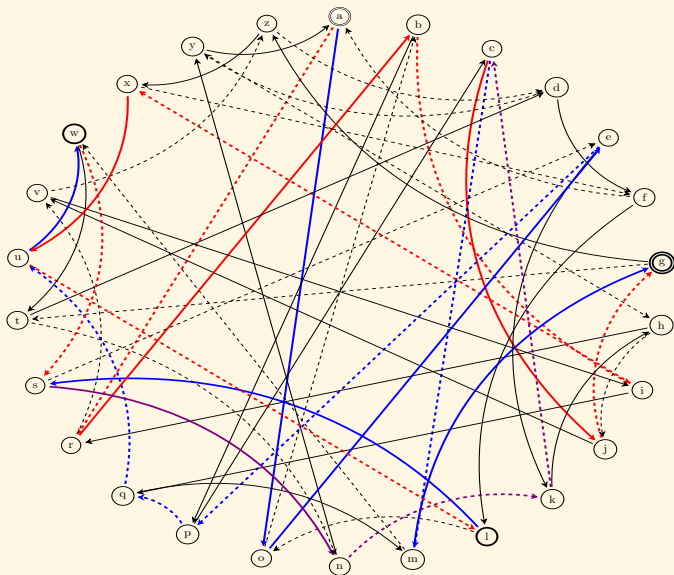
Key exchange on a (commutative) graph

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



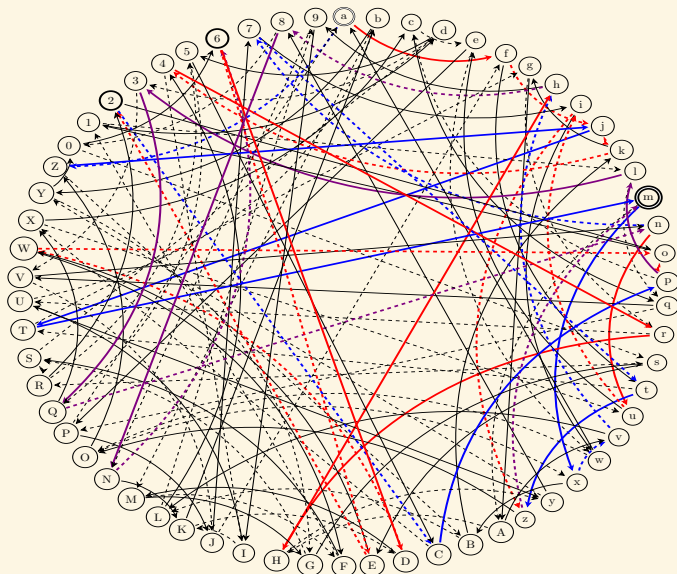
Key exchange on a (commutative) graph

The full exchange:



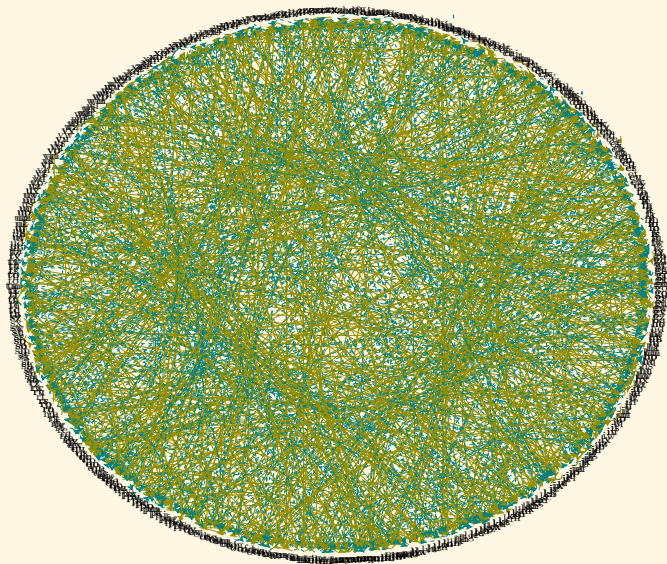
Key exchange on a (commutative) graph

Bigger graph (62 nodes)



Key exchange on a (commutative) graph

Even bigger graph (676 nodes)



Graphs for key exchange

- Needs a graph with good mixing properties:
A path of length $O(\log N)$ gives a uniform node \Rightarrow Ramanujan/expander graph.
- The graph does not fit in memory ($N = 2^{256}$).
- Needs an algorithm taking a node as input and giving the neighbour nodes as output.
- Isogeny graphs of elliptic curves

Isogenies

- Elliptic curve: $E/k : y^2 = x^3 + ax + b$. Algebraic group law!
- Isogeny: $\phi : E_1 \rightarrow E_2$ with $\phi(0_{E_1}) = 0_{E_2}$
- $\phi(P + Q) = \phi(P) + \phi(Q)$

$$\phi(x, y) = \left(\frac{g(x)}{h(x)}, cy \left(\frac{g(x)}{h(x)} \right)' \right)$$

- Isogeny $\phi \Leftrightarrow$ Kernels $K = \text{Ker } \phi$

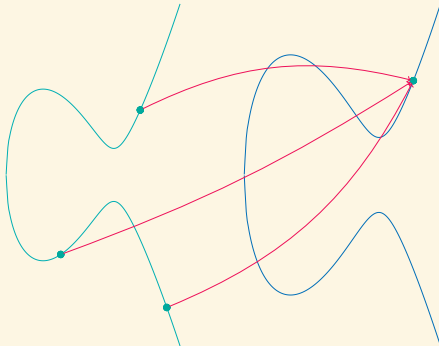
Isogeny based cryptography:

- Computing an isogeny $\phi : E_1 \rightarrow E_2$: **Easy!**
 - Given (E_1, E_2) , find an isogeny path $\phi : E_1 \rightarrow E_2$: **Hard!** (Even for quantum computers!)
- \Rightarrow Post quantum cryptosystems

Isogenies

$$E_1 : y^2 = x^3 + a_1x + b_1$$

$$E_2 : y^2 = x^3 + a_2x + b_2$$



Isogeny graphs for key exchange

- Isogeny graph of **ordinary elliptic curves** E/\mathbb{F}_p
[Couveignes (1997)], [Rostovtsev–Stolbunov (2006)]

- Graph of size $N \approx \sqrt{p}$.

☺ Commutative graph!

☺ Group action framework! (By $\text{Cl}(\text{End}(E_0))$)

$$\begin{array}{ccc} E_0 & \xrightarrow{\phi_a} & E_a \\ \downarrow \phi_b & & \downarrow \phi_b \\ E_b & \xrightarrow{\phi_a} & E_{ab} \end{array}$$

☹ 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} ($N \approx p$).

Isogeny graphs for key exchange

Meme: Gru's plan

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

SIDH in practice

- $p = 2^a 3^b - 1$. $N_A = 2^a, N_B = 3^b$
- $E_0 : y^2 = x^3 + x$ (supersingular when $a \geq 2$)
- $E_0[N_A] = \langle P_A, Q_A \rangle, E_0[N_B] = \langle P_B, Q_B \rangle$.
- 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 $\langle \phi_B(P_A + s_A Q_A) \rangle$, ϕ'_B has kernel $\langle \phi_A(P_B + s_B Q_B) \rangle$.
- 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".)
- $\text{Ker } \phi'_A = \langle P'_A + s_A Q'_A \rangle, \text{Ker } \phi'_B = \langle P'_B + s_B Q'_B \rangle$.

Isogeny evaluation and interpolation

- **Evaluation**: given an n -isogeny ϕ and a point $Q \in E(\mathbb{F}_q)$, evaluate $\phi(Q)$.
- n -evaluation problem: ϕ is an n -isogeny = $\text{Ker } \phi$ is of degree n .
- **Interpolation**: given a tuple $(P, \phi(P))$, recover ϕ .
- (n, N) -interpolation problem: given ϕ an n -isogeny and P a point of N -torsion, from $(P, \phi(P))$ and $Q \in E(\mathbb{F}_q)$, evaluate $\phi(Q)$
- **Weak interpolation**: we are given $(P_1, \phi(P_1)), (P_2, \phi(P_2))$ for (P_1, P_2) a basis of $E[N]$.
- SIDH: the key exchange uses the N_A and N_B evaluation problems
- If we can solve the weak interpolation problem when $n = N_A, N = N_B$ are smooth in polylogarithmic time, we can **break SIDH**.

Meme: Anakin

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

Evaluation

- $\phi : E_1 \rightarrow E_2$ an n -isogeny, $\phi(x, y) = \left(\frac{g(x)}{h(x)}, cy \left(\frac{g(x)}{h(x)} \right)' \right)$, $\deg g, \deg h \leq n$
- $K : h(x) = 0, h(x) = \prod_{P \in K - 0_E} (x - x(P))$. If $E : y^2 = f(x)$, [Kohel 1996]:


$$\phi(x, y) = \left(\frac{g(x)}{h(x)}, y \left(\frac{g(x)}{h(x)} \right)' \right)$$
$$\frac{g(x)}{h(x)} = \#K.x - \sigma - f'(x) \frac{h'(x)}{h(x)} - 2f(x) \left(\frac{h'(x)}{h(x)} \right)'$$

- **Kernel representation: Linear time and linear space.**
- $\text{Ker } f = \langle T \rangle, T \in \mathbb{F}_{q^d}$, evaluate $\phi(Q)$ in $O(n)$ operations in \mathbb{F}_{q^d} [Vélu 1971]:

$$x(f(P)) = x(P) + \sum_{i=1}^{n-1} (x(P + iT) - x(iT))$$
$$y(f(P)) = y(P) + \sum_{i=1}^{n-1} (y(P + iT) - y(iT))$$

- $\sqrt{\text{élú}}$: $\widetilde{O}(\sqrt{n})$ (time/memory trade off)
- **Generator representation: Compact representation** if d small.

Decomposing a smooth degree isogeny

- $\phi : E_1 \rightarrow E_2, K = \text{Ker } \phi = \langle T \rangle$ of degree $n = 2^a, T \in \mathbb{F}_{q^d}$
- $\phi = \phi'_1 \circ \phi_1$
- $\phi_1 : E_1 \rightarrow E'_1$ of degree 2 with kernel $K_1 = \langle 2^{a-1}T \rangle$
- $\phi'_1 : E'_1 \rightarrow E_2$ of degree 2^{a-1} with kernel $K = \langle \phi_1(T) \rangle$
- Complexity: $O(a^2)$ arithmetic operations in \mathbb{F}_{q^d}
- [De Feo, Jao, Plût 2011]: $\widetilde{O}(a)$ operations in \mathbb{F}_{q^d}
-  d can be large, $d = \Theta(n)$ in the worst case \Rightarrow quasi-linear time
- In SIDH: $N_A = 2^a$ and $N_B = 3^b$ and the N_A, N_B -torsion points are rational, so the decomposition is fast!
- Can decompose isogenies of smooth degree N (if the N -torsion is accessible)

Interpolation

- Given $(P, \phi(P))$, P a point of order $N > 4n$, recover the rational function $\frac{g(x)}{h(x)}$ in $\tilde{O}(N)$ by interpolating the points $(x(mP), x(m\phi(P)))$, $m = 1, \dots, N - 1$.
- Can evaluate on \mathbb{Q} directly.
- Quasi-linear time.
- Faster algorithm when N is smooth?
- Yes if $\phi(P) = 0$. Then $n = N$ and $\text{Ker } \phi = \langle P \rangle$.
- If $n = N$, the weak interpolation problem reduces via the DLP to the N -evaluation problem.
- This is why the SIDH key exchange is fast: Bob uses the torsion point information published by Alice to find the kernel of his pushforward isogeny.
- No reason to expect a fast algorithm when N is prime to n .

Interpolation

- Given $(P, \phi(P))$, P a point of order $N > 4n$, recover the rational function $\frac{g(x)}{h(x)}$ in $\tilde{O}(N)$ by interpolating the points $(x(mP), x(m\phi(P)))$, $m = 1, \dots, N - 1$.
- Can evaluate on \mathbb{Q} directly.
- Quasi-linear time.
- Faster algorithm when N is smooth?
- Yes if $\phi(P) = 0$. Then $n = N$ and $\text{Ker } \phi = \langle P \rangle$.
- If $n = N$, the weak interpolation problem reduces via the DLP to the N -evaluation problem.
- This is why the SIDH key exchange is fast: Bob uses the torsion point information published by Alice to find the kernel of his pushforward isogeny.
- No reason to expect a fast algorithm when N is prime to n .

Revisiting isogeny evaluation

- Can an n -isogeny be evaluated faster than linear time when n has a large prime factor?
- If $\phi = [\ell]$ (so $n = \ell^2$): double and add in $O(\log \ell)$ to evaluate ℓQ .
- $\Phi : E^2 \rightarrow E^2, (P_1, P_2) \mapsto (P_1 + P_2, P_1 - P_2)$ is a 2-isogeny in dimension 2.
- $\Phi = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$
- Double: $\Phi(T, T) = (2T, 0)$.
- Add: $\Phi(T, Q) = (T + Q, T - Q)$.
- We can evaluate ℓQ as a composition of $O(\log \ell)$ evaluations of Φ , projections $E^2 \rightarrow E$ and embeddings $E \rightarrow E^2$.
- Double and add on $E = 2$ -isogenies in dimension 2

Kani's lemma [Kani 1997] ($g = 1$), [R. 2022] ($g > 1$)

- $\alpha : A \rightarrow B$ 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 $\beta' \alpha = \alpha' \beta$:

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

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

Using Kani's lemma for the interpolation problem

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ \downarrow \alpha & & \downarrow \alpha' \\ E'_1 & \xrightarrow{\phi'} & E'_2 \end{array}$$

- $\phi : E_1 \rightarrow E_2$ an n -isogeny.
- **Goal:** replace ϕ by Φ an N -isogeny.
- Find $\alpha : E_1 \rightarrow E'_1$ an m -isogeny, with $N = n + m$.
- Kani's lemma: $\Phi = \begin{pmatrix} \alpha & \widetilde{\phi'} \\ -\phi & \widetilde{\alpha'} \end{pmatrix} : E_1 \times E'_2 \rightarrow E'_1 \times E_2$ is an N -isogeny.
- We know $\phi(E[N])$ and we can evaluate α on $E[N] \Rightarrow$ recover $\text{Ker } \Phi$ (or $\text{Ker } \widetilde{\Phi}$)
- **Evaluate Φ , hence ϕ at any point:** $\Phi(P, 0) = (\alpha(P), -\phi(P))$.
- Evaluation is fast if N is (power) smooth.

Examples:

- m smooth [Castricky–Decru; Maino–Martindale (2022)]
- $m = \ell^2$: take $\alpha = [\ell]$
- $\text{End}(E)$ has an efficient endomorphism α of norm m [Castricky–Decru; Wesolowski (2022)].

Using Kani's lemma for the interpolation problem

Meme: disaster girl

- SIDH
- Higher dimensional isogenies

The general case: Zahrin's trick

- $\alpha = \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix}$ is always an endomorphism of norm $m = a_1^2 + a_2^2$ on E^2

- Gaussian integers $\mathbb{Z}[i]$

- $\alpha = \begin{pmatrix} a_1 & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 & a_4 & -a_3 \\ a_3 & -a_4 & a_1 & a_2 \\ a_4 & a_3 & -a_2 & a_1 \end{pmatrix}$ is always an endomorphism of norm $m = a_1^2 + a_2^2 + a_3^2 + a_4^2$ on E^4

- Hamilton's quaternion algebra
- Evaluating α : $O(\log m)$ arithmetic operations
- Every integer is a sum of four squares.

$$\begin{array}{ccc} E_1^4 & \xrightarrow{\phi} & E_2^4 \\ \downarrow \alpha & & \downarrow \alpha \\ E_1^4 & \xrightarrow{\phi} & E_2^4 \end{array}$$

- $\Phi : E_1^4 \times E_2^4 \rightarrow E_1^4 \times E_2^4$ is an N -isogeny.

Kani's lemma + Zahrin's trick = the embedding lemma [R. 2022]

- A n -isogeny $\phi : A \rightarrow B$ in dimension g can always be efficiently embedded into a N isogeny $\Phi : A' \rightarrow B'$ in dimension $8g$ (and sometimes $4g, 2g$) for any $N \geq n$.

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow & & \uparrow \\ A' & \xrightarrow{\Phi} & B' \end{array}$$

- Considerable flexibility (at the cost of going up in dimension).
 - Reduces the weak (n, N) -interpolation problem to the N -evaluation problem in higher dimension
 - Actually only need the image of ϕ on a subgroup of size $N, N > 4n$ (via further tricks by Castryck, De Feo, R., Wesolowski...)
- ⇒ Solves the interpolation problem when N is (power) smooth
- Amazing fact: does not require $\text{Ker } \phi$, works even if n is prime
 - Breaks SIDH: [Castryck–Decru], [Maino–Martindale] in dimension 2, [R.] in dimension 4 or 8

Kani's lemma + Zahrin's trick = the embedding lemma [R. 2022]

Meme: funeral

- SIDH
- 2011-2022

Castryck's invited talk at Eurocrypt 2024: "An attack became a tool: Isogeny based cryptography 2.0"

Meme: Buzz

- Higher dimensional isogenies
- Higher dimensional isogenies everywhere

Isogeny representations

- Before 2022: could only compute smooth degree isogenies $\phi : E_1 \rightarrow E_2$ (with accessible kernel points)
- Isogeny based cryptography: correspondance between ideals $I \subset R$ and certain isogenies $\phi_I : E_1 \rightarrow E_2$
- Supersingular isogeny graph over \mathbb{F}_{p^2} : R is a non commutative quaternionic order. Every isogeny comes from an ideal
Deuring's correspondance
- Ordinary isogeny graph or supersingular isogeny graph over \mathbb{F}_p : R is a (commutative) quadratic imaginary order.
😊 Class group action!

Translating an ideal I to an isogeny ϕ_I :

- Needs to find a smooth equivalent ideal $J \sim I$
- KLPT: heuristic polynomial smoothening algorithm for R quaternion algebra
- ☹ J has very large norm $\approx p^{4.5}$
- ☹ If R quadratic order, only subexponential time smoothening algorithms known
- ☹ Restricted group action

The HD representation

- Embed $\phi : E_1 \rightarrow E_2$ into an N -isogeny Φ in dimension g ($N \geq n$)

- Represent Φ by its kernel $\text{Ker } \Phi$:

$\text{Ker } \Phi$ is completely determined by n and the action of ϕ on $E_1[N]$

- CRT basis: $N = \prod_{i=1}^m N_i = \prod_{i=1}^m \ell_i^{e_i}$,

$$(P_i, Q_i, \phi(P_i), \phi(Q_i)), \quad \text{for } (P_i, Q_i) \text{ a basis of } E[\ell_i^{e_i}]$$

- Naive algorithm: reconstruct ϕ in $\widetilde{O}(n)$ via rational function interpolation
- HD approach: exploit the N -torsion structure by going to Φ in higher dimension

- Can take any $N \geq n$ (Example: N powersmooth)

- Ideal scenario: E_1 has rational $N = 2^m$ -torsion and Φ in dimension 2

- Compact and efficient isogeny representation

- Universal: can be efficiently recovered from any other efficient isogeny representation of ϕ

- Philosophy: if we know how ϕ act on sufficiently many nice points, we can efficiently compute $\phi(P)$ for any point P

Algorithms for N -isogenies in higher dimension

- Analogues of Vélu's formula: [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.
- 😊 Work in any dimension
- 😞 Exponential dependency 2^g in the dimension g .
- 😞 Need a rational level $\Gamma(2, 4)$ -structure (automatic for supersingular curves over \mathbb{F}_{p^2})
- Algorithm in $O(N^g)$ in the Jacobian model: [Couveignes, Ezome (2015)]
- 😊 Rational model
- 😞 Restricted to $g \leq 3$

Cost of a 2^m -isogeny in dimension g :

g	1	2	4	8
Relative cost	$\times 1$	$\times 4$	$\times 32$	$\times 1024$

Dedicated fast formulas in higher dimension

Dimension 2:

- Fast 2^m -isogenies in the Mumford Jacobian or Kummer model [Kunzweiler 2022] and in the theta model [Dartois, Maino, Pope, R. 2023]

$\log p$	m	Codomain			Evaluation		
		Theta Rust	Theta SageMath	Richelot SageMath	Theta Rust	Theta SageMath	Richelot SageMath
254	126	2.13 ms	108 ms	1028 ms	161 μ s	5.43 ms	114 ms
381	208	9.05 ms	201 ms	1998 ms	411 μ s	8.68 ms	208 ms
1293	632	463 ms	1225 ms	12840 ms	17.8 ms	40.8 ms	1203 ms

- Fast 3^m -isogenies in the Mumford Jacobian model [Decru, Kunzweiler 2023] and in the theta model [Corte-Real Santos, Costello, Smith 2024]

Dimension 4:

- Fast 2^m -isogenies in the theta model [Dartois 2024]

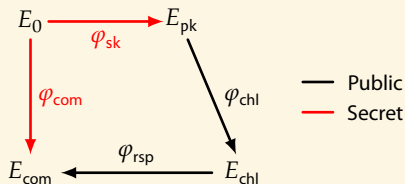
Cryptographic applications

- **New protocols** in isogeny based cryptography: SQIsignHD [DLRW24], FESTA [BMP23] and QFESTA [NO23], the Deuring VRF [Ler23b], SCALLOP-HD [CLP24] (efficient representation of orientations), IS-CUBE [Mor23], LIT-SiGamal [Mor24], SILBE [DFV24], POKE [Bas24], SQIsign2d (West and East) [BDD+24; NO24], SQIPrime [DF24]...
- **New or improved security reductions** in isogeny based cryptography, [MW23; ACD+23; PW24; ES24] and in classical elliptic curve cryptography [Gal24]
- **New methods** to convert ideals into isogenies [Ler23a; NO23; PR23; ON24; BDD+24]

Examples:

- **Clapoti(s)** [Page, R. 2023]: computing the class group action for an arbitrary orientation R in polynomial time
- No smoothening needed
- **Unrestricted effective group action!**
- **SQIsignHD, SQIsign2d-West**: bypass KLPT's smoothening algorithm for supersingular curves too
- KLPT: $\phi_f : E_1 \rightarrow E_2$, smoothened isogeny of degree $O(p^{4.5})$ (or $O(p^3)$ if E_1 is nice)
- HD representation: can use the smallest isogeny $\phi_f : E_1 \rightarrow E_2$ of degree $O(\sqrt{p})$ even if it is not smooth!

- Proves **knowledge** of a supersingular endomorphism ring
- Most compact PK+signature out of all PQ signature schemes
- NIST submission



SQLSign2d (West) and SQLSignHD

	SQLsign	SQLsign2d
Public key	66B	66B
Signatures	177B	148B
Clean security proof	☹️	😊
Keygen (Mcycles)	400	60
Sign (Mcycles)	1880	160
Verify (Mcycles)	29	9

- **SQLsign2D**: signature and verification in dimension 2

- **SQLsignHD**: signature in dimension 1, verification in dimension 4

New faster variant compared to the Eurocrypt 2024 version using techniques from SQLsign2d: signatures now use dimension 2 too. Bonus: same public key as in SQLsign2d!

- **Signature size**: 109B
- **Signature** $\approx 5\times$ faster than SQLsign2d
- **Verification** expected $\approx 8\times$ slower

Number theoretic applications

- E/\mathbb{F}_q ordinary elliptic curve, $K = \text{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. Given the factorisation of $[O_K : \mathbb{Z}[\pi]]$, compute $\text{End}(E)$ in polynomial time [R. 2022].
Factorisation: quantum polynomial time, classical subexponential time
- Previously: no quantum polynomial time algorithm known.
Classical algorithm in $L(1/2)$ under GRH [Bisson–Sutherland 2009].
- Compute the canonical lift \hat{E}/\mathbb{Z}_q of an ordinary elliptic curve in polynomial time [R. 2022]
Previously: $L(1/2)$ under GRH [Couveignes–Henocq 2002]
- Compute the modular polynomial Φ_ℓ by deformation [Kunzweiler, R. 2024]

Point counting for E/\mathbb{F}_q , $q = p^n$

- [Schoof 1985]: $\tilde{O}(n^5 \log^5 p)$ (Étale cohomology)
- [SEA 1992]: $\tilde{O}(n^4 \log^4 p)$ (Heuristic)
- [Kedlaya 2001]: $\tilde{O}(n^3 p)$ (Rigid cohomology)
- [Harvey 2007]: $\tilde{O}(n^{3.5} p^{1/2} + n^5 \log p)$
- [Sato 2000] (canonical lifts of ordinary curves): $\tilde{O}(n^2 p^2)$ (Crystalline cohomology)
- [Maiga – R. 2021]: $\tilde{O}(n^2 p)$
- [R. 2022]: $\tilde{O}(n^2 \log^8 p + n \log^{11} p)$

Use an HD representation of the Verschiebung $\hat{\pi}_p$ and canonical lifts

Example: divisions [R. 2022]

- Is an isogeny $\phi : E_1 \rightarrow E_2$ **divisible** by $[\ell]$?
- Prior art: test if $\phi(E[\ell]) = 0$
- Division polynomial ψ_ℓ : degree $O(\ell^2) \Rightarrow$ exponential time
- HD division algorithm [R. 2022]:
- Given an HD representation $(P_i, Q_i, \phi(P_i), \phi(Q_i))$ with $N_i \wedge \ell = 1$,

$$(P_i, Q_i, \frac{\phi(P_i)}{\ell}, \frac{\phi(Q_i)}{\ell})$$

is an HD representation of ϕ/ℓ if it exists

\Rightarrow polynomial time (in $\log \ell$) division algorithm

Corollary (Computing the endomorphism ring of ordinary elliptic curves)

If E/\mathbb{F}_q is an ordinary elliptic curve; point counting gives χ_π , hence $K := \mathbb{Q}(\pi_q)$, and we know $\mathbb{Z}[\pi] \subset \text{End}(E) \subset O_K$. Given the **factorisation** of the conductor $[O_K : \mathbb{Z}[\pi]]$ of $\mathbb{Z}[\pi]$, we can determine $\text{End}(E)$ in **polynomial time**, via efficient divisions.

Algorithms for the HD representation

$\phi/\mathbb{F}_q : E_1 \rightarrow E_2$ an n -isogeny with an efficient representation

- **Equality testing, Validity**
- **Composition and addition:** $\phi_2 \circ \phi_1, \phi_1 + \phi_2$
- **Dual isogeny:** $\tilde{\phi} : E_2 \rightarrow E_1$
- **Divisions:** Test if $\phi \stackrel{?}{=} \psi' \circ \psi$ is divisible by ψ , and if so return the HD representation of ψ'
- **Lifts and deformations:** deform ϕ to $\tilde{\phi}/R : \widetilde{E}_1 \rightarrow \widetilde{E}_2$ over $R = \mathbb{F}_q[\varepsilon]/\varepsilon^m$ or $R = \mathbb{Z}_q/p^m\mathbb{Z}_q$
- **Splittings:** If $n = n_1 n_2, n_1 \wedge n_2 = 1$, split ϕ as $\phi = \phi_2 \circ \phi_1$

$$\phi : E_1 \xrightarrow{\phi_1} E_{12} \xrightarrow{\phi_2} E_2$$

- **Pushforwards:** compute the pushforward of ϕ_1 and ϕ_2 if they are of coprime degrees

$$\begin{array}{ccc} E_0 & \xrightarrow{\phi_1} & E_1 \\ \downarrow \phi_2 & & \downarrow \phi'_2 \\ E_1 & \xrightarrow{\phi'_1} & E_{12} \end{array}$$

- **Kernel:** return an equation for $\text{Ker } \phi$ in $\widetilde{\mathcal{O}}(n)$

Efficient representation of isogenies

Past:

- Restricted to smooth degree isogenies
- Vélu's / $\sqrt{\text{él}}\text{u}$ formulas
- Ideal smoothening

Present:

- The **HD representation**: recent powerful tool with many applications in isogeny based cryptography and algorithmic number theory
- Use **abelian varieties** to speed up algorithms on elliptic curves
- Survey paper: [Rob25]

Future?

- Switch from **ideals** equivalences of categories to **modules** equivalences of categories
 - ▶ Handles the higher dimensional isogeny graphs of E^g
 - ▶ Handles level structures
 - ▶ Go beyond Kani's lemma
- Use cyclic isogenies?

Bibliography

- [ACD+23] S. Arpin, J. Clements, P. Dartois, J. K. Eriksen, P. Kutas, and B. Wesolowski. “Finding orientations of supersingular elliptic curves and quaternion orders”. In: [arXiv preprint arXiv:2308.11539](#) (2023) (cit. on p. 34).
- [Bas24] A. Basso. “POKE: A Framework for Efficient PKEs, Split KEMs, and OPRFs from Higher-dimensional Isogenies”. In: [Cryptology ePrint Archive](#) (2024) (cit. on p. 34).
- [BDD+24] A. Basso, L. De Feo, P. Dartois, A. Leroux, L. Maino, G. Pope, D. Robert, and B. Wesolowski. “SQLsign2D-West: The Fast, the Small, and the Safer”. In: [Advances in Cryptology – ASIACRYPT 2024, Part III](#). Vol. 15486, Lecture Notes in Computer Science. Springer Nature Switzerland, Dec. 2024, pp. 339–370. doi: [10.1007/978-981-96-0891-1_11](#) (cit. on p. 34).
- [BMP23] A. Basso, L. Maino, and G. Pope. “FESTA: fast encryption from supersingular torsion attacks”. In: [International Conference on the Theory and Application of Cryptology and Information Security](#). Springer. 2023, pp. 98–126 (cit. on p. 34).
- [CLP24] M. Chen, A. Leroux, and L. Panny. “SCALLOP-HD: group action from 2-dimensional isogenies”. In: [IACR International Conference on Public-Key Cryptography](#). Springer. 2024, pp. 190–216 (cit. on p. 34).
- [DLRW24] P. Dartois, A. Leroux, D. Robert, and B. Wesolowski. “SQLSignHD: New Dimensions in Cryptography”. In: [Lecture Notes in Computer Science 14651](#) (May 2024). Ed. by M. Joye and G. Leander, pp. 3–32. doi: [10.1007/978-3-031-58716-0_1](#) (cit. on p. 34).

- [DF24] M. Duparc and T. B. Fouotsa. “SQIPrime: A dimension 2 variant of SQISignHD with non-smooth challenge isogenies”. In: Cryptology ePrint Archive (2024) (cit. on p. 34).
- [DFV24] M. Duparc, T. B. Fouotsa, and S. Vaudenay. “Silbe: an updatable public key encryption scheme from lollipop attacks”. In: Cryptology ePrint Archive (2024) (cit. on p. 34).
- [ES24] K. Eisentraeger and G. Scullard. “Connecting Kani’s Lemma and path-finding in the Bruhat-Tits tree to compute supersingular endomorphism rings”. In: (2024). arXiv: [2402.05059](https://arxiv.org/abs/2402.05059) (cit. on p. 34).
- [Gal24] S. Galbraith. Climbing and descending tall volcanos. Cryptology ePrint Archive, Paper 2024/924. 2024. url: <https://eprint.iacr.org/2024/924> (cit. on p. 34).
- [Ler23a] A. Leroux. “Computation of Hilbert class polynomials and modular polynomials from supersingular elliptic curves”. In: Cryptology ePrint Archive (2023) (cit. on p. 34).
- [Ler23b] A. Leroux. “Verifiable random function from the Deuring correspondence and higher dimensional isogenies”. In: (2023) (cit. on p. 34).
- [MW23] A. H. L. Merdy and B. Wesolowski. “The supersingular endomorphism ring problem given one endomorphism”. In: arXiv preprint arXiv:2309.11912 (2023) (cit. on p. 34).
- [Mor23] T. Moriya. “IS-CUBE: An isogeny-based compact KEM using a boxed SIDH diagram”. In: Cryptology ePrint Archive (2023) (cit. on p. 34).
- [Mor24] T. Moriya. “LIT-SiGamal: An efficient isogeny-based PKE based on a LIT diagram”. In: Cryptology ePrint Archive (2024) (cit. on p. 34).
- [NO23] K. Nakagawa and H. Onuki. “QFESTA: Efficient Algorithms and Parameters for FESTA using Quaternion Algebras”. In: Cryptology ePrint Archive (2023) (cit. on p. 34).

- [NO24] K. Nakagawa and H. Onuki. “SQIsign2D-East: A New Signature Scheme Using 2-dimensional Isogenies”. In: [Cryptography ePrint Archive](#) (2024) (cit. on p. 34).
- [ON24] H. Onuki and K. Nakagawa. “Ideal-to-isogeny algorithm using 2-dimensional isogenies and its application to SQIsign”. In: [Cryptography ePrint Archive](#) (2024) (cit. on p. 34).
- [PR23] A. Page and D. Robert. “Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time”. Nov. 2023 (cit. on p. 34).
- [PW24] A. Page and B. Wesolowski. “The supersingular endomorphism ring and one endomorphism problems are equivalent”. In: [Annual International Conference on the Theory and Applications of Cryptographic Techniques](#) Springer. 2024, pp. 388–417 (cit. on p. 34).
- [Rob25] D. Robert. “On the efficient representation of isogenies (a survey)”. In: [Number-Theoretic Methods in Cryptology – NuTMiC 2024](#). Ed. by A. Dąbrowski, J. Pieprzyk, and J. Pomykała. Vol. 14966. Lecture Notes in Computer Science. Springer Nature Switzerland, Feb. 2025, pp. 3–84. doi: https://doi.org/10.1007/978-3-031-82380-0_1 (cit. on p. 40).

Polarisations and isogenies on an abelian variety

- Polarisation on A = a (symmetric) isogeny $\lambda_A : A \rightarrow \hat{A}$
- Principal polarisation: λ_A is an isomorphism.
- Warning: A may have several non equivalent principal polarisations if $g > 1$.

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.

Polarisations and isogenies on an abelian variety

- Polarisation on A = a (symmetric) isogeny $\lambda_A : A \rightarrow \hat{A}$
- Principal polarisation: λ_A is an isomorphism.
- Warning: A may have several non equivalent principal polarisations if $g > 1$.
- $\phi : (A, \lambda_A) \rightarrow (B, \lambda_B)$ N -isogeny between ppav: $\phi^* \lambda_B = N \lambda_A$.

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

- Dual isogeny: $\hat{\phi} : \hat{B} \rightarrow \hat{A}$
- Contragredient isogeny: $\tilde{\phi} = \lambda_A^{-1} \hat{\phi} \lambda_B : B \rightarrow A$
- ϕ N -isogeny $\Leftrightarrow \tilde{\phi} \circ \phi = N \Leftrightarrow \phi \tilde{\phi} = N$.
- $\text{Ker } \phi = \text{Im } (\tilde{\phi} \mid B[N])$.

N -isogenies and isotropic kernels

- $\phi : (A, \lambda_A) \rightarrow (B, \lambda_B)$ N -isogeny $\Rightarrow \text{Ker } \phi$ 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 $\phi : E_1 \rightarrow E_2$ is an N -isogeny $\Leftrightarrow \# \text{Ker } \phi = N$.
- 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 $\phi : (A, \lambda_A) \rightarrow (B, \lambda_B)$ has maximal isotropic kernel in $A[N]$, $N\lambda_A$ descends to a principal polarisation λ'_B on B .
- But we may have $\lambda'_B \neq \lambda_B$.
- $\tilde{\phi} \circ \phi = N$ is a stronger condition that ensures compatibility of ϕ 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.
- $F = \begin{pmatrix} a & c \\ b & d \end{pmatrix} : (A \times B, \lambda_A \times \lambda_B) \rightarrow (C \times D, \lambda_C \times \lambda_D)$.
- $\hat{F} = \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix} : \hat{C} \times \hat{D} \rightarrow \hat{A} \times \hat{B}$.
- $\tilde{F} = \begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix} : C \times D \rightarrow A \times B$.