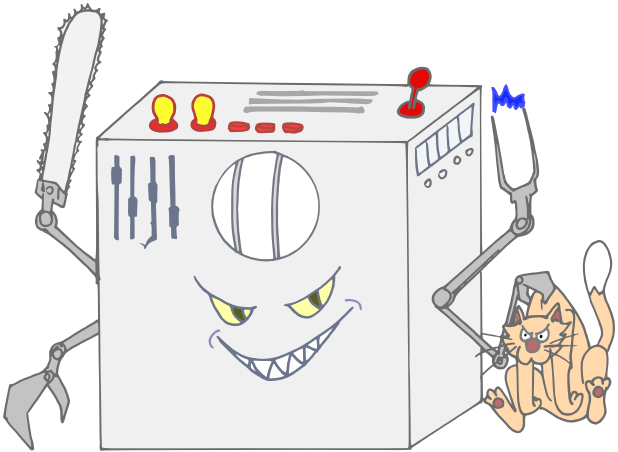
Isogeny-based Cryptography

Luca De Feo
IBM Research Zürich

December 14, 2025, Indocrypt

Are you quantum-safe?



Only two ways to Post-quantum Encryption

Noisy linear algebra:

Lattices, Codes

Far-fetched generalizations of the discrete logarithm:

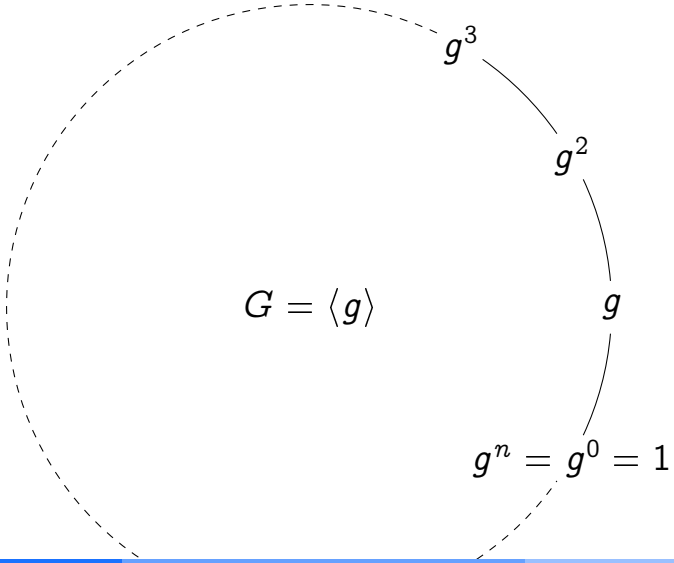
Isogenies

What crypto from isogenies?

	Key exchange / Encryption	Identification / Signature	Other
Quadratic (Group actions)	Couveignes–Rostovtsev–Stolbunov CSIDH SCALLOP	SeaSign CSI-FiSh PEGASIS	Threshold PAKE …
Quaternionic	—	SQIsign SIDH-like signatures	Ring signatures Adaptor signatures Chameleon hash …
Ad hoc	SIDH † SIDH fixes FESTA	SIDH-like signatures	Time-release crypto …

Cryptographic Group Actions

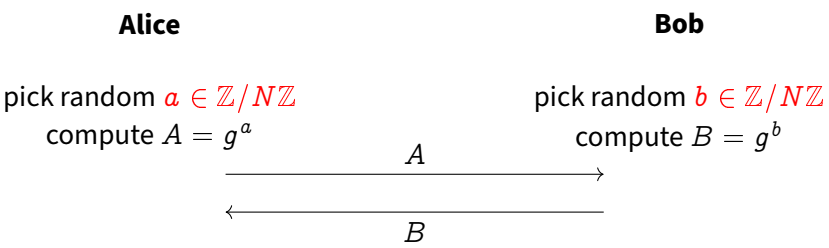
A cyclic group



Diffie–Hellman key exchange

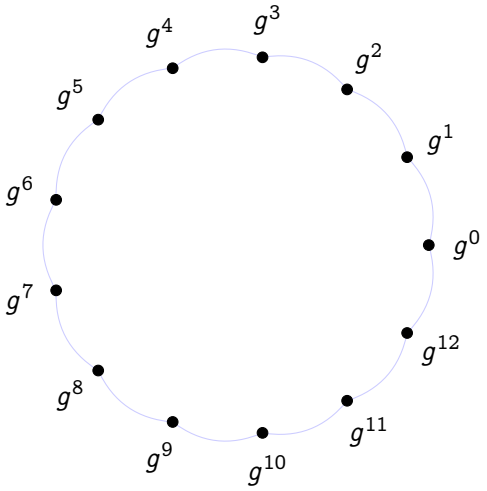
Goal: Alice and Bob have never met before. They are chatting over a public channel, and want to agree on a shared secret to start a private conversation.

Setup: They agree on a (large) cyclic group $G = \langle g \rangle$ of order N.



Shared secret is $B^a = g^{ab} = A^b$

What's needed for key exchange?



The axioms of a dlog group:

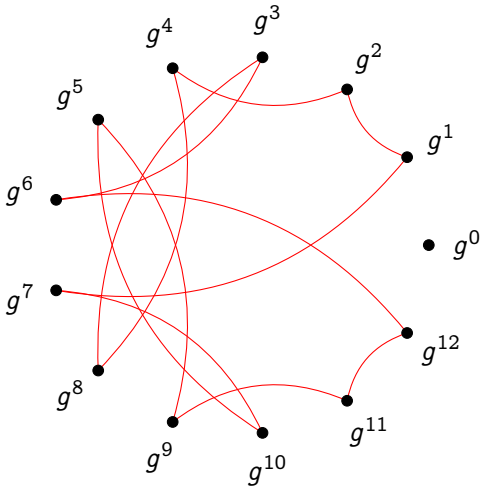
prod: ~~$g^a g^b = g^{a+b}$~~,

exp: $(g^a)^n = g^{na}$.

The hard problem:

dlog: $g^a \mapsto a$.

What's needed for key exchange?



The axioms of a dlog group:

prod: ~~$g^a g^b = g^{a+b}$~~,

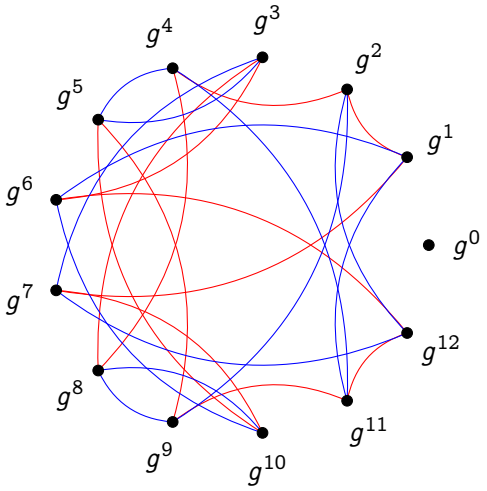
exp: $(g^a)^n = g^{na}$.

The hard problem:

dlog: $g^a \mapsto a$.

$g^a \longrightarrow g^{2a}$

What's needed for key exchange?



The axioms of a dlog group:

prod: ~~$g^a g^b = g^{a+b}$~~,

exp: $(g^a)^n = g^{na}$.

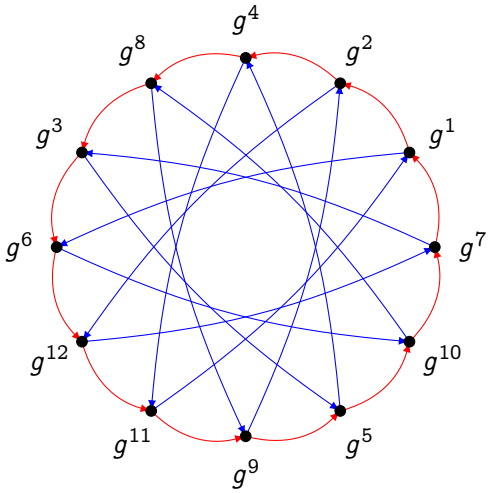
The hard problem:

dlog: $g^a \mapsto a$.

$g^a \longrightarrow g^{2a}$

$g^a \longrightarrow g^{6a}$

What's needed for key exchange?



The axioms of a dlog group:

prod: ~~$g^a g^b = g^{a+b}$~~,

exp: $(g^a)^n = g^{na}$.

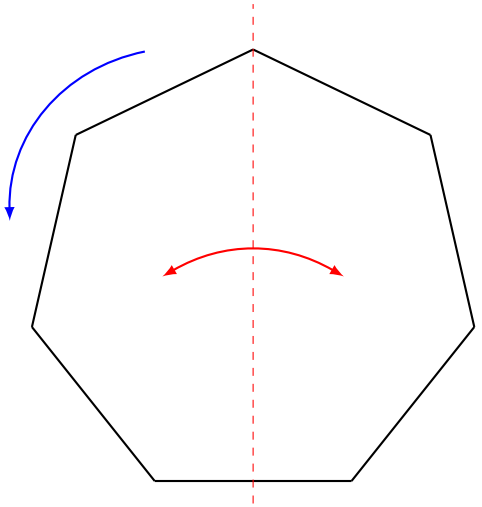
The hard problem:

dlog: $g^a \mapsto a$.

$g^a \longrightarrow g^{2a}$

$g^a \longrightarrow g^{6a}$

Symmetries = Group action



Group action

$\mathcal{G} \circlearrowright \mathcal{E}$: A (finite) set $\mathcal{E}$ acted upon by a group $\mathcal{G}$ freely and transitively:

$$\begin{aligned} * : \mathcal{G} \times \mathcal{E} &\longrightarrow \mathcal{E} \\ \mathfrak{g} * E &\longmapsto E' \end{aligned}$$

Compatibility: $\mathfrak{g}' * (\mathfrak{g} * E) = (\mathfrak{g}'\mathfrak{g}) * E$ for all $\mathfrak{g}, \mathfrak{g}' \in \mathcal{G}$ and $E \in \mathcal{E}$;

Identity: $\mathfrak{e} * E = E$ if and only if $\mathfrak{e} \in \mathcal{G}$ is the identity element;

Regularity: for all $E, E' \in \mathcal{E}$ there exist a unique $\mathfrak{g} \in \mathcal{G}$ such that $\mathfrak{g} * E' = E$.

Cryptographic Group Actions (Alamati, D., Montgomery, Patranabis 2021)

Hard Homogeneous Space (HHS) — Couveignes 1997 (eprint:2006/291)

$\mathcal{G} \circlearrowright \mathcal{E}$ such that $\mathcal{G}$ is commutative and:

- Evaluating $E' = \mathfrak{g} * E$ is easy;
- Inverting the action is hard.

Example

Let G be a group of order 13, then $(\mathbb{Z}/13\mathbb{Z})^\times \circlearrowright G$ defined by

$$a * g := g^a$$

is an HHS…

Cryptographic Group Actions (Alamati, D., Montgomery, Patranabis 2021)

Hard Homogeneous Space (HHS) — Couveignes 1997 (eprint:2006/291)

$\mathcal{G} \circlearrowright \mathcal{E}$ such that $\mathcal{G}$ is commutative and:

- Evaluating $E' = \mathfrak{g} * E$ is easy;
- Inverting the action is hard.

Example

Let G be a group of order 13, then $(\mathbb{Z}/13\mathbb{Z})^\times \circlearrowright G$ defined by

$$a * g := g^a$$

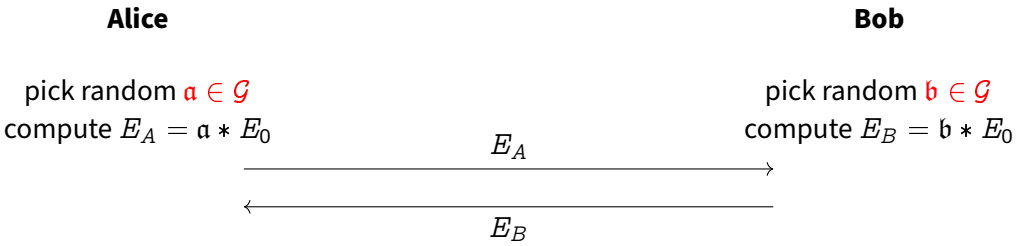
is an HHS… But

$$g^a \cdot g^b = g^{a+b}$$

has no interpretation as a group action!

Key exchange from group actions

Public parameters: A HHS $\mathcal{G} \circlearrowright \mathcal{E}$ of order N (large, but not necessarily prime).

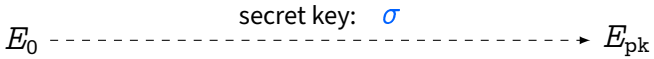


Shared secret is $\mathfrak{a} * E_B = (\mathfrak{a}\mathfrak{b}) * E_0 = \mathfrak{b} * E_A$

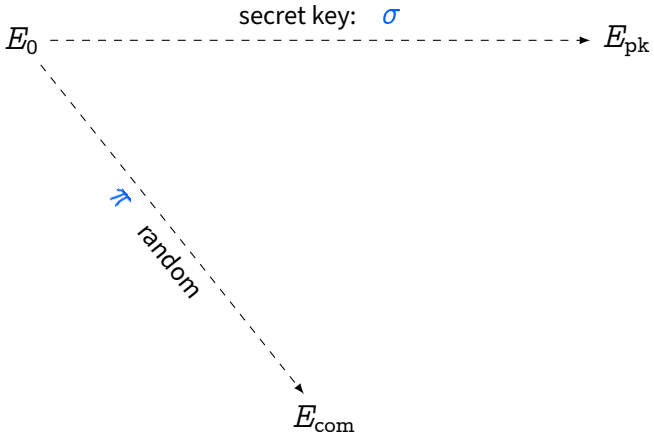
What crypto from isogenies?

	Key exchange / Encryption	Identification / Signature	Other
Quadratic (Group actions)	Couveignes–Rostovtsev–Stolbunov CSIDH SCALLOP	SeaSign CSI-FiSh PEGASIS	Threshold PAKE …
Quaternionic	—	SQIsign SIDH-like signatures	Ring signatures Adaptor signatures Chameleon hash …
Ad hoc	SIDH † SIDH fixes FESTA	SIDH-like signatures	Time-release crypto …

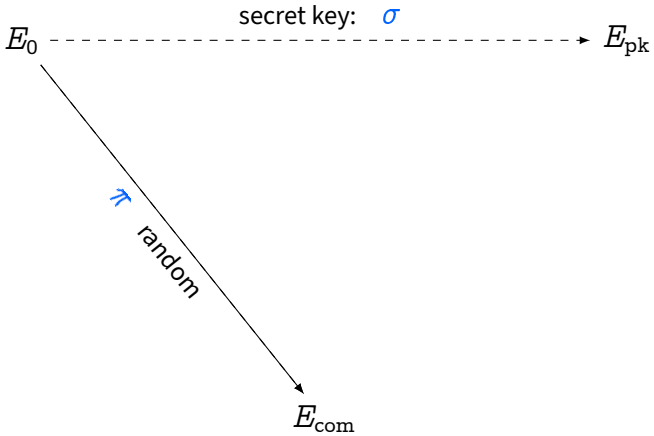
Identification scheme (Goldreich et al. 1992, Couveignes 1997, Stolbunov 2008)



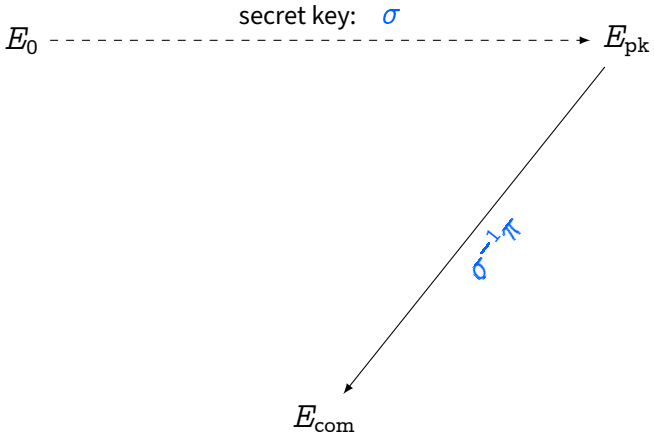
Identification scheme (Goldreich et al. 1992, Couveignes 1997, Stolbunov 2008)



Identification scheme (Goldreich et al. 1992, Couveignes 1997, Stolbunov 2008)



Identification scheme (Goldreich et al. 1992, Couveignes 1997, Stolbunov 2008)



Quantum security

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

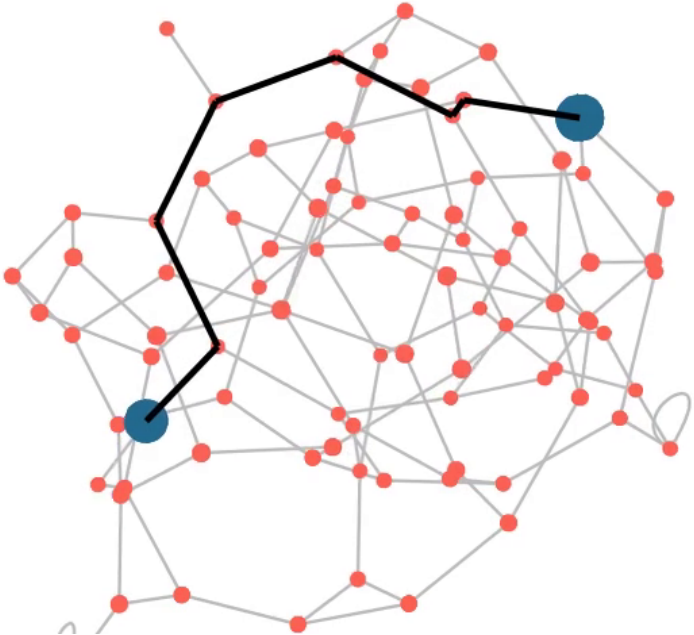
Subexponential attack $\exp(\sqrt{\log N \log\log N})$

- Reduction to the hidden shift problem by evaluating the group action in quantum superposition (subexponential cost);
- Well known reduction from the hidden shift to the dihedral (non-abelian) hidden subgroup problem;
- Kuperberg's algorithm solves the dHSP with a subexponential number of class group evaluations.
- Analyses suggest that 2^{64}-qbit security may be achieved somewhere around $\log N \approx 2048$.

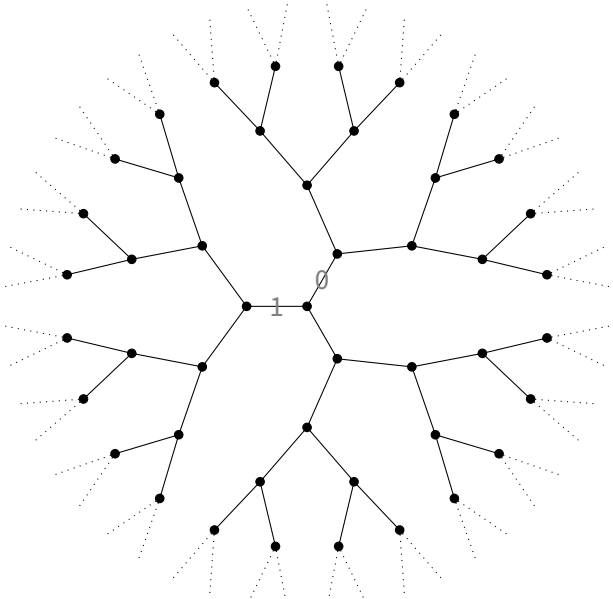
Expander graphs

The supersingular ℓ-isogeny graph

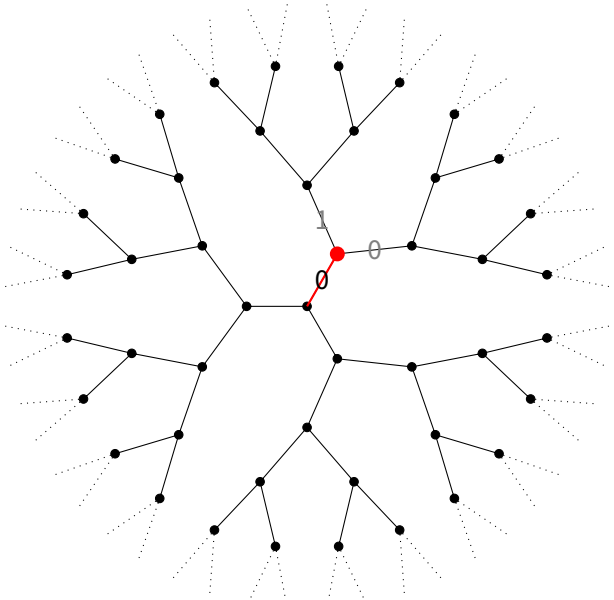
- Parameterized by primes p and $\ell \neq p$;
- $\approx p/12$ vertices;
- $(\ell + 1)$-regular;
- Connected;
- Optimal expander (in the sense of Ramanujan):
  - small diameter,
  - locally tree-like,
  - good mixing.



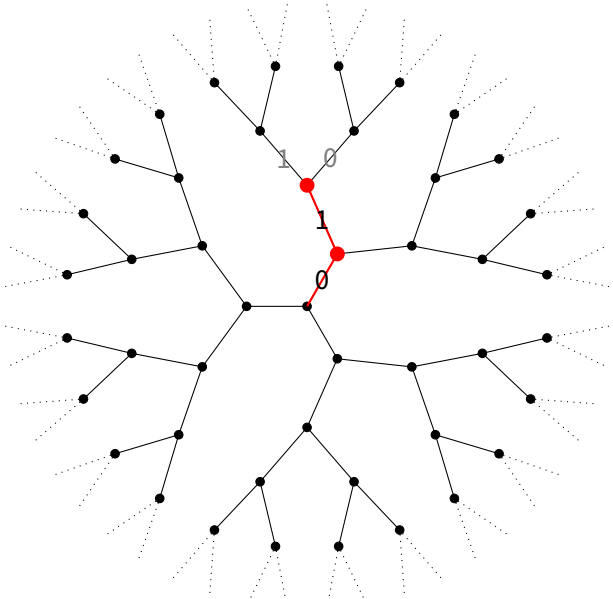
Random walks and Hash functions



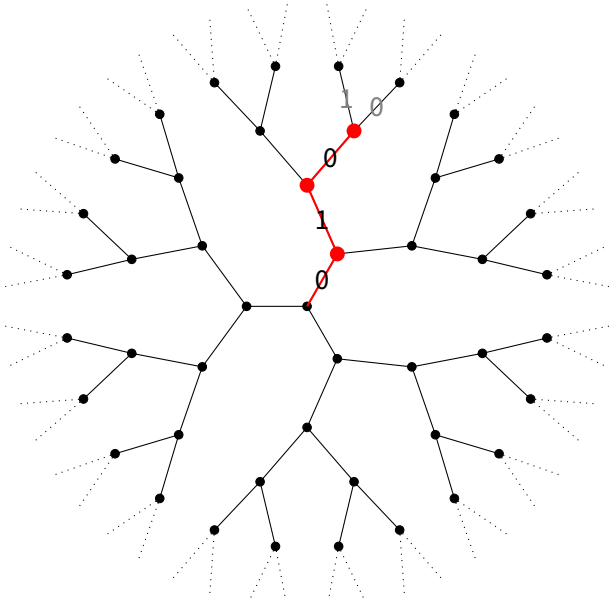
Random walks and Hash functions



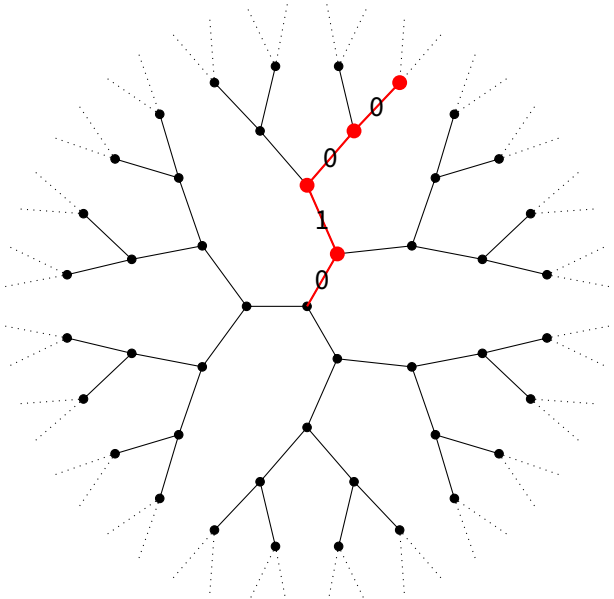
Random walks and Hash functions



Random walks and Hash functions



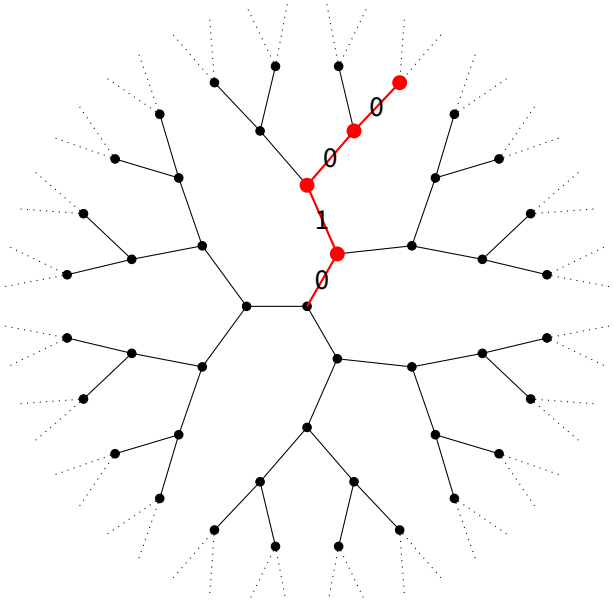
Random walks and Hash functions



Random walks and Hash functions

Collisions: finding cycles

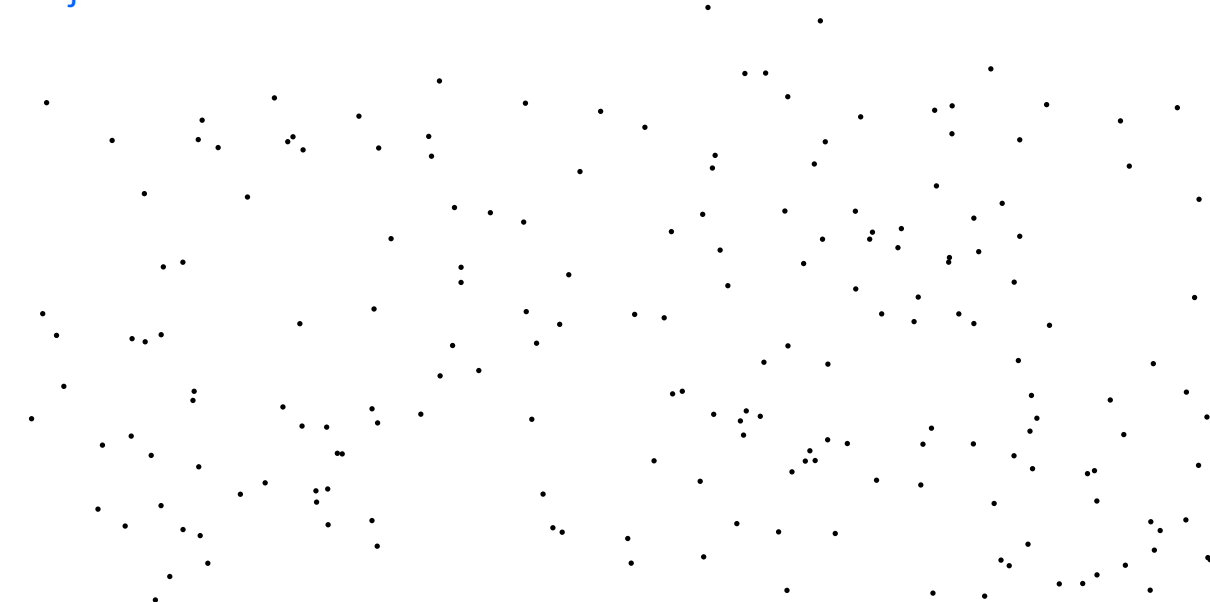
Preimages: finding paths



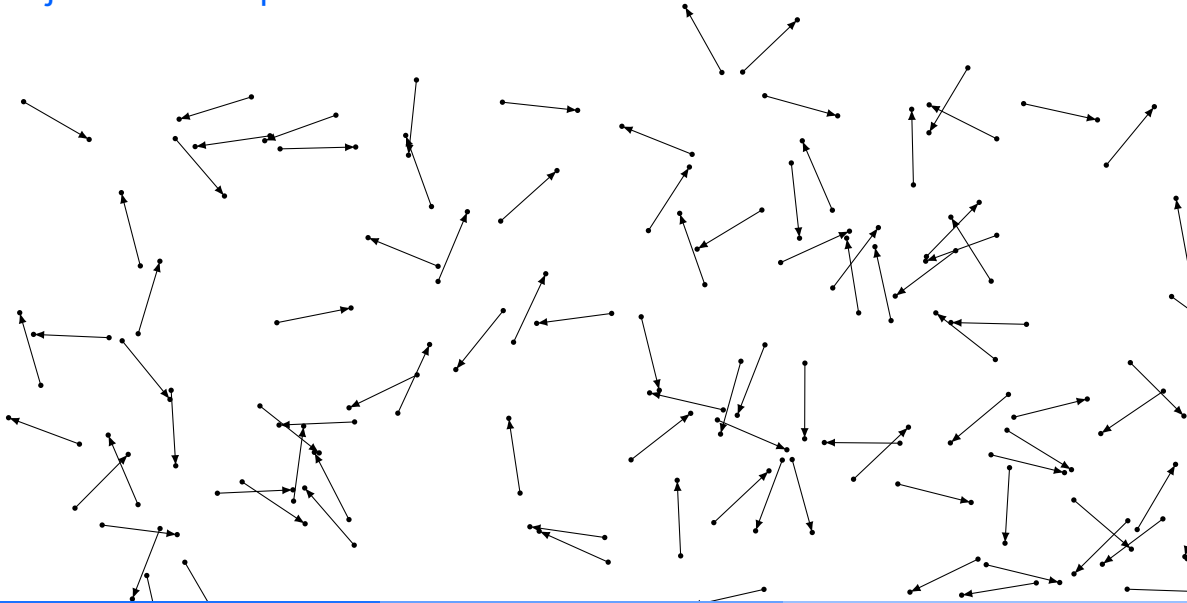
Forensic categories

(joint work with Basso, Patranabis, Radulescu, Wesolowski)

Objects

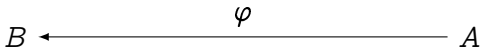


Objects and Morphisms



More than graphs…

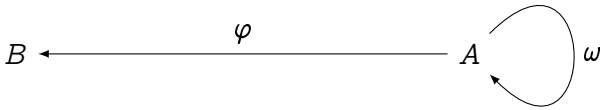
- A finite set of objects $\mathcal{E}$,
- For each pair $A, B \in \mathcal{E}$ a set of morphisms $\mathrm{Hom}(A, B)$



$$\varphi \in \mathrm{Hom}(A, B)$$

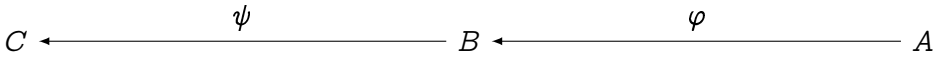
More than graphs…

- A finite set of objects $\mathcal{E}$,
- For each pair $A, B \in \mathcal{E}$ a set of morphisms $\mathrm{Hom}(A, B)$

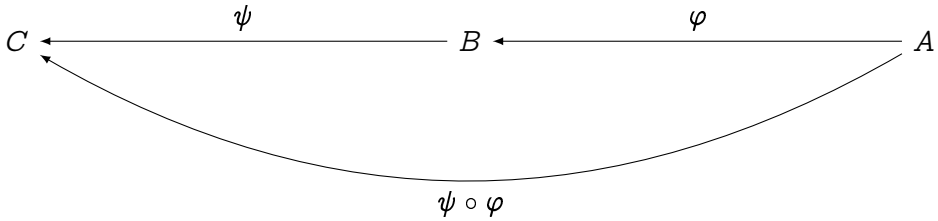


$\varphi \in \mathrm{Hom}(A, B)$ $\omega \in \mathrm{Hom}(A, A)$

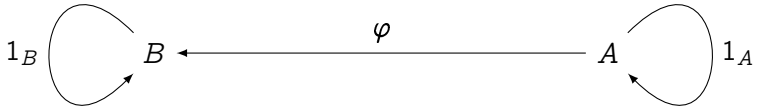
Transitively closed



Transitively closed



Identity morphisms



$$1_B \circ \varphi = \varphi = \varphi \circ 1_A$$

Computational axioms

- Every object and every morphism has a unique representation as a string;
- The representation of a morphism $\phi : A \to B$ identifies A and B;
- There exists efficient algorithms to verify that a string represents an object/morphism;
- There exists an origin object $O \in \mathcal{E}$ whose representation is known;
- …

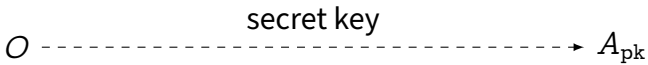
Axiom: *Walking*

Efficient algorithm for:

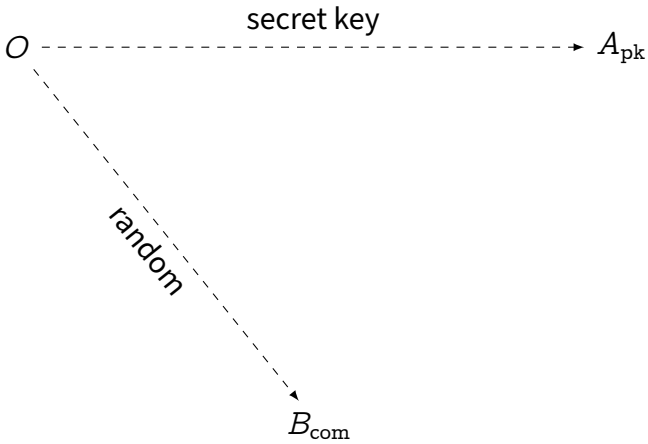
Input: Object A

Output:
- Uniformly random object B,
- Random morphism $\phi : A \to B$.

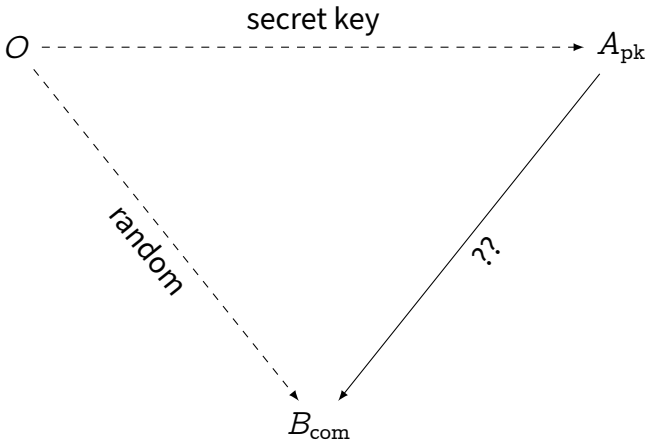
Identification scheme?



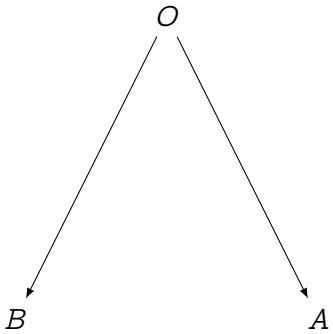
Identification scheme?



Identification scheme?

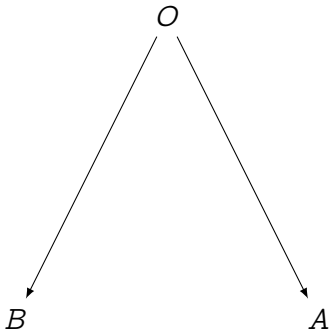


Axiom: Triangularizable



Input

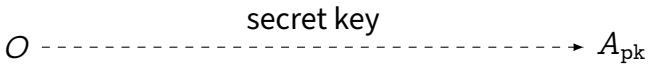
Axiom: Triangularizable



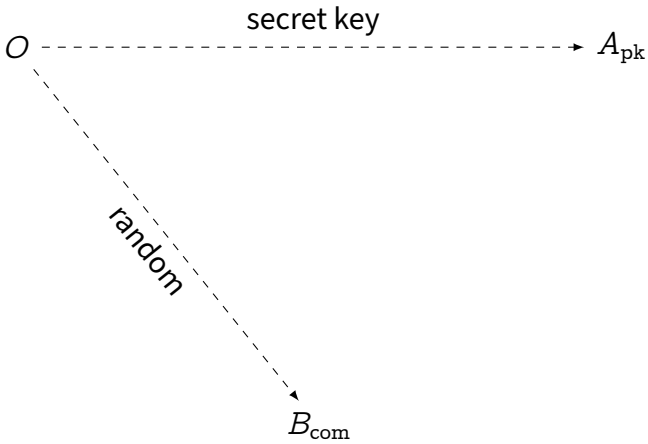
Input

Output

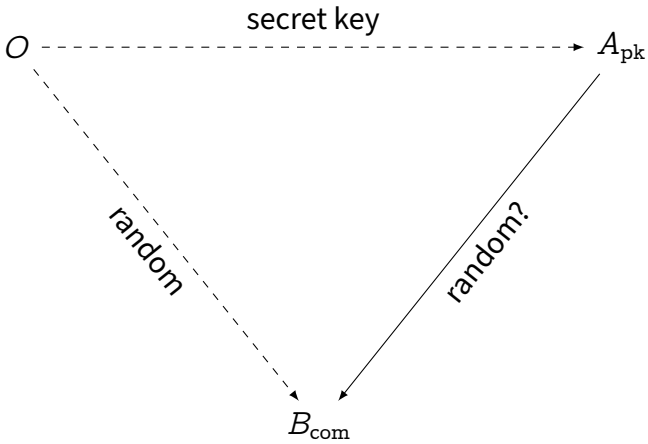
Identification scheme?



Identification scheme?



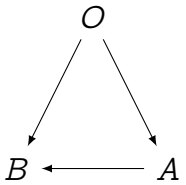
Identification scheme?



Hardness Assumption: *Walk-indistinguishable*

These two distributions are indistinguishable:

- Given A,
- *Walk* $\phi : A \to B$,



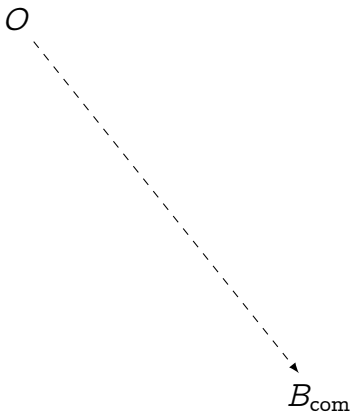
- Given $O \to A$,
- Sample random $O \to B$,
- *Triangularize* $\phi : A \to B$

Identification scheme?

O

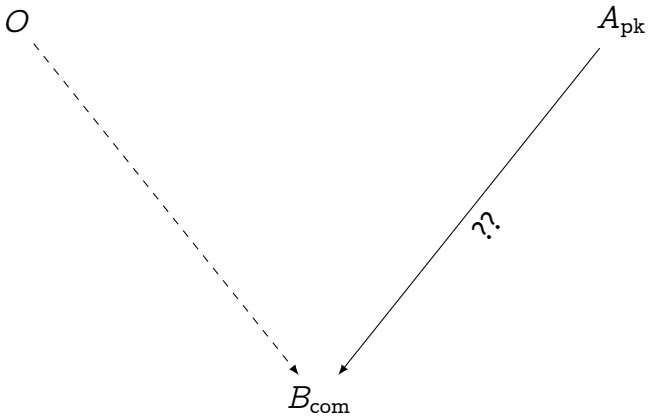
A_{pk}

Identification scheme?



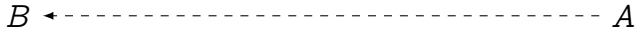
A_{pk}

Identification scheme?



Hardness assumption: *Morphism Finding*

Given two objects A, B, it is hard to find a morphism between them:



Summary

- *Effective* category,
- Origin object O,
- Walking,
- Triangularizable,
- Walk-indistinguishable,
- Hard to find morphisms.

GMW-style Identification scheme

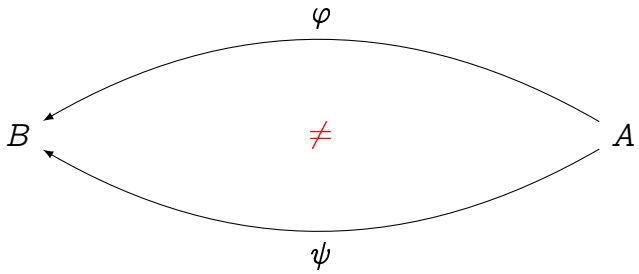
Summary

- *Effective* category,
- Origin object O,
- Walking,
- Triangularizable,
- Walk-indistinguishable,
- Hard to find morphisms.

GMW-style Identification scheme

Lame!

Towards a stronger hardness assumption



Fingerprints

- A finite set $\mathcal{M}$ with at least 2 elements
- Partial maps for any pair A, B:

$$\mathrm{fp} \quad : \quad \mathrm{Hom}(A, B) \quad \rightarrow \quad \mathcal{M} \cup \{\perp\}$$

Fingerprints

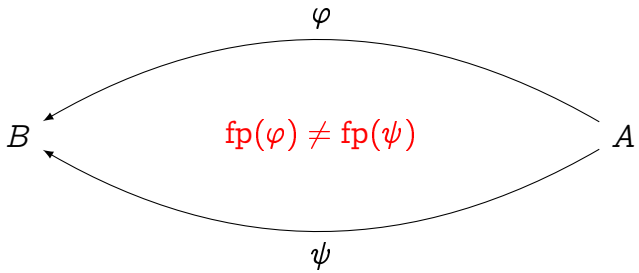
- A finite set $\mathcal{M}$ with at least 2 elements
- Partial maps for any pair A, B:

$$\mathrm{fp} \quad : \quad \mathrm{Hom}(A, B) \quad \to \quad \mathcal{M} \cup \{\perp\}$$

- Random walk $\to$ random fingerprint

Hardness assumption: Forensic hardness

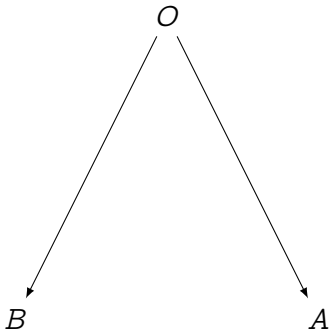
It is hard to find a pair of morphisms $A \to B$ with distinct fingerprints:



Easy corollary

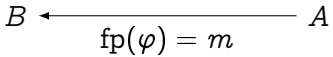
Forensic hardness $\Rightarrow$ Hard to find morphisms

Axiom: Triangularizable (reloaded)



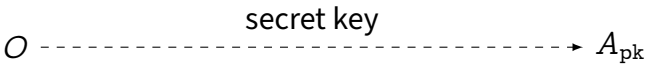
$m \in \mathcal{M}$

Input

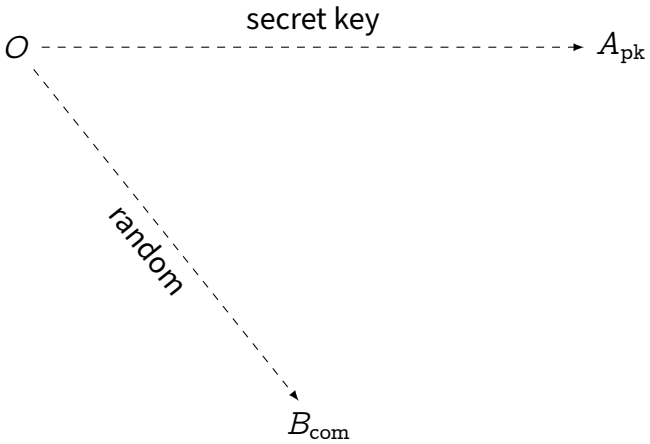


Output

SQIsign (in Forensic categories)

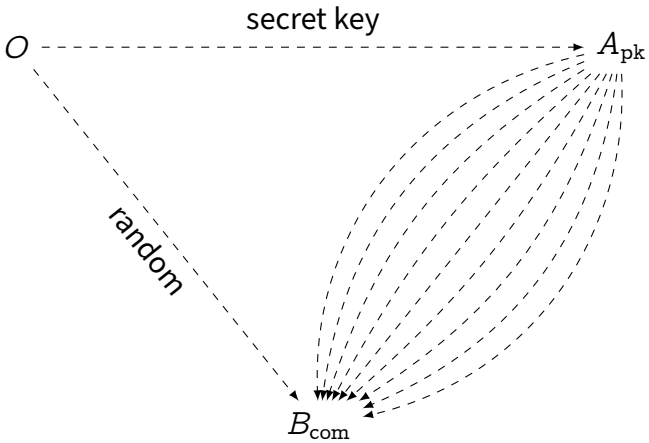


SQIsign (in Forensic categories)



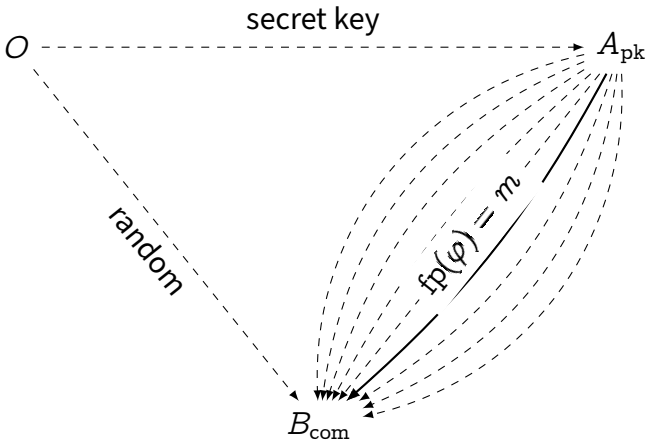
P: generate random commitment B_{com}

SQIsign (in Forensic categories)



P: generate random commitment B_{com}

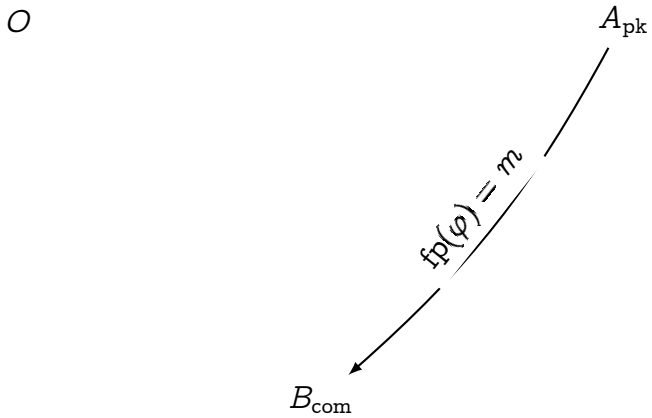
SQIsign (in Forensic categories)



P: generate random commitment B_{com}

V: challenge with random $m \in \mathcal{M}$

SQIsign (in Forensic categories)



P: generate random commitment B_{com}

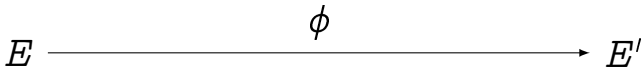
V: challenge with random $m \in \mathcal{M}$

P: respond with $\varphi : A_{\mathrm{pk}} \to B_{\mathrm{com}}$ such that $\mathrm{fp}(\varphi) = m$

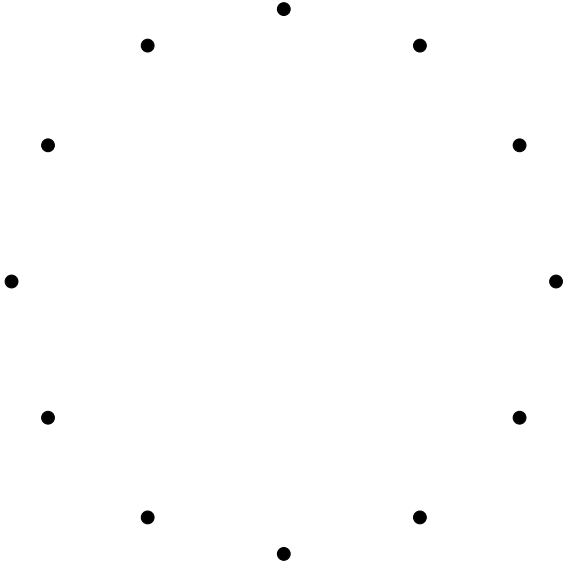
Isogenies, finally!

Isogenies = finite-kernel *algebraic* group morphisms: $E \to E'$

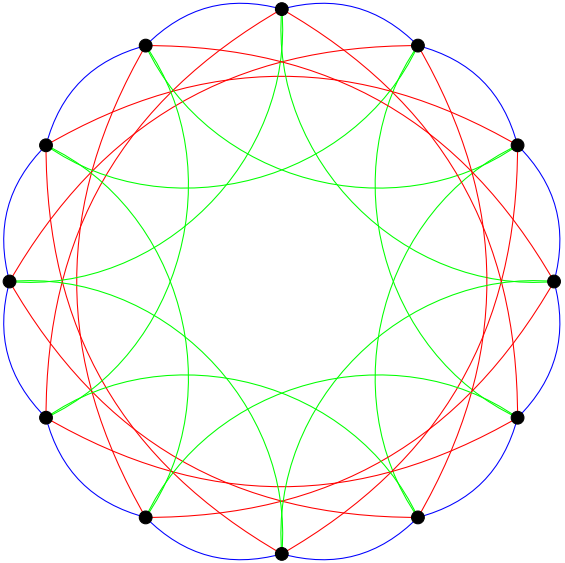
Endomorphisms = isogenies $E \to E$


E
ϕ
E'

Isogenous



Isogeny class



Isogeny class

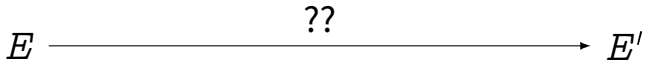
Isogeny graph

The isogeny problem

E

E'

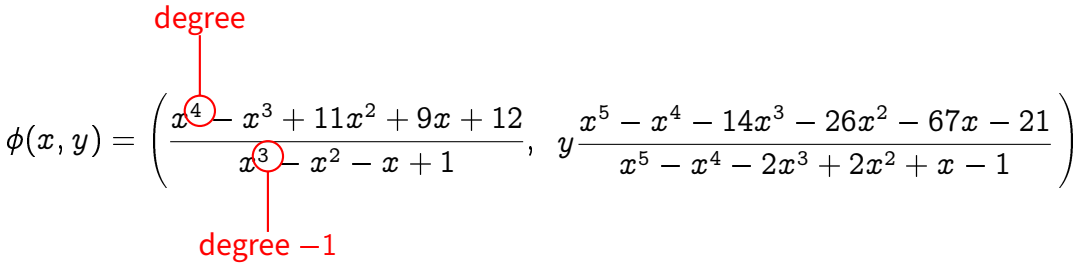
The isogeny problem



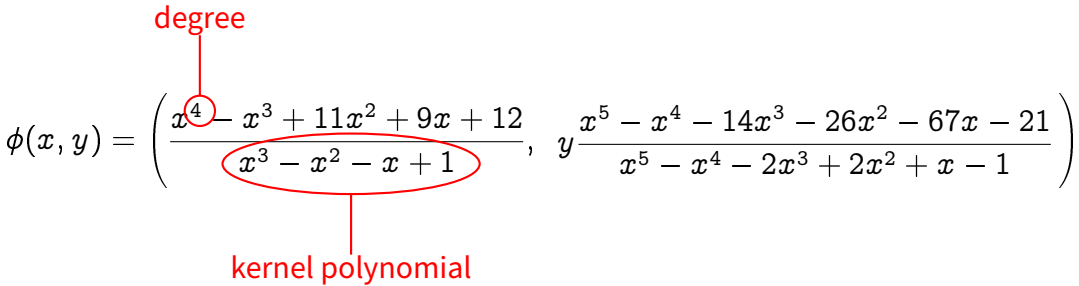
Anatomy of an isogeny

$$\phi(x,y) = \left(\frac{x^4 - x^3 + 11x^2 + 9x + 12}{x^3 - x^2 - x + 1},\ y\frac{x^5 - x^4 - 14x^3 - 26x^2 - 67x - 21}{x^5 - x^4 - 2x^3 + 2x^2 + x - 1} \right)$$

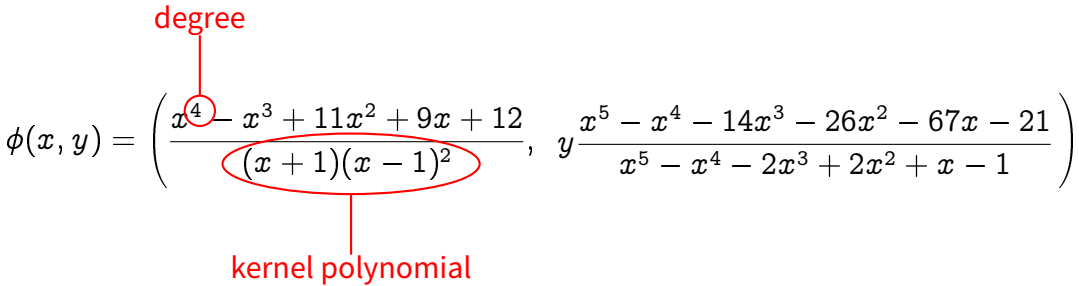
Anatomy of an isogeny



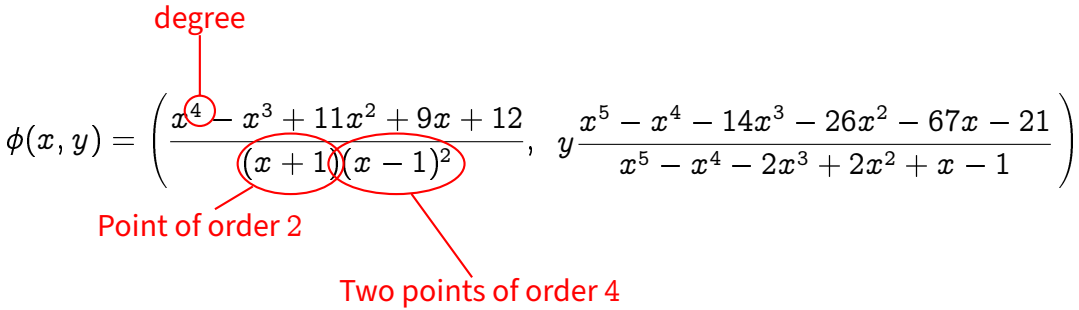
Anatomy of an isogeny



Anatomy of an isogeny



Anatomy of an isogeny



Anatomy of an isogeny

degree

$$\phi(x,y) = \left(\frac{x^4 - x^3 + 11x^2 + 9x + 12}{h(x)},\ y\frac{x^5 - x^4 - 14x^3 - 26x^2 - 67x - 21}{x^5 - x^4 - 2x^3 + 2x^2 + x - 1} \right)$$

$$h(x) = \prod_{P \in K \setminus \{0\}} \big(x - x(P)\big)$$

Anatomy of an isogeny

computed by Vélu–Elkies–Kohel formulas

$$\phi(x,y) = \left(\frac{g(x)}{h(x)}, \quad y\frac{x^5 - x^4 - 14x^3 - 26x^2 - 67x - 21}{x^5 - x^4 - 2x^3 + 2x^2 + x - 1} \right)$$

$$h(x) = \prod_{P \in K \setminus \{0\}} \big(x - x(P)\big)$$

Anatomy of an isogeny

computed by Vélu–Elkies–Kohel formulas

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

$$h(x) = \prod_{P \in K \setminus \{0\}} \big(x - x(P)\big)$$

Anatomy of an isogeny

computed by Vélu–Elkies–Kohel formulas

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

$$h(x) = \prod_{P \in K \setminus \{0\}} \big(x - x(P)\big)$$

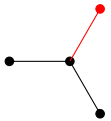
Input: Finite kernel $K \subset E$ of order d;

Output: Rational fractions $\phi(x,y)$;

Complexity: $\tilde{O}(d)$ operations.

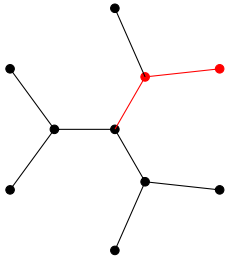
Isogeny graphs

$$\frac{x^2 + \cdots}{x + \cdots}$$



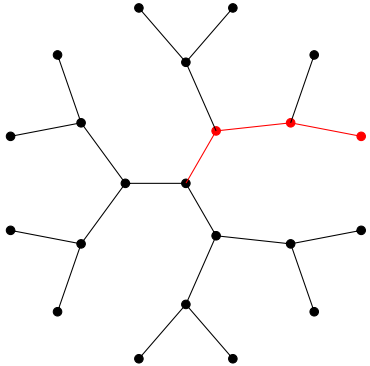
Isogeny graphs

$$\frac{x^2 + \cdots}{x + \cdots} \circ \frac{x^2 + \cdots}{x + \cdots}$$



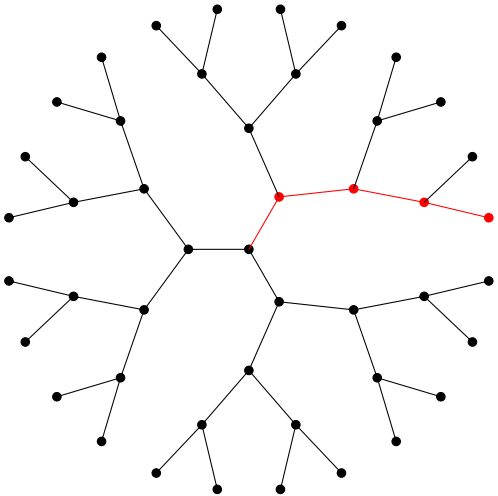
Isogeny graphs

$$\frac{x^2 + \cdots}{x + \cdots} \circ \frac{x^2 + \cdots}{x + \cdots} \circ \frac{x^2 + \cdots}{x + \cdots}$$



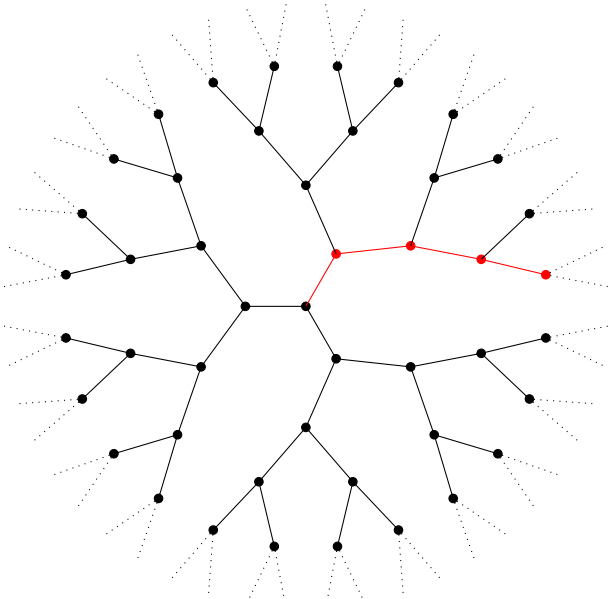
Isogeny graphs

$$\frac{x^2+\cdots}{x+\cdots} \circ \frac{x^2+\cdots}{x+\cdots} \circ \frac{x^2+\cdots}{x+\cdots} \circ \frac{x^2+\cdots}{x+\cdots}$$



Isogeny graphs

$$\frac{x^2+\cdots}{x+\cdots} \circ \frac{x^2+\cdots}{x+\cdots} \circ \frac{x^2+\cdots}{x+\cdots} \circ \frac{x^2+\cdots}{x+\cdots}$$



Two computational worlds

	Quadratic imaginary	Quaternionic
$\mathrm{rank}\,\mathrm{Hom}(E, E')$	2	4
Endomorphism algebra	number field	quaternion algebra
Maximal orders	one	many
Ideal class…	…group	…set
Find isogeny $E \to E'$	hard	hard
Convert isogenies $\leftrightarrow$ ideals	easy[1]	easy[1]
Compute $\mathrm{End}(E)$	easy	hard

[1] When $\mathrm{End}(E)$ is known

A cryptographic group action

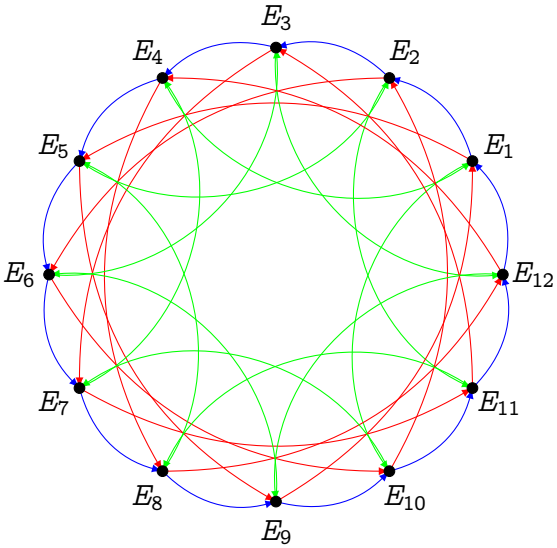
The quadratic imaginary case

Complex Multiplication

Fix an order $\mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$:

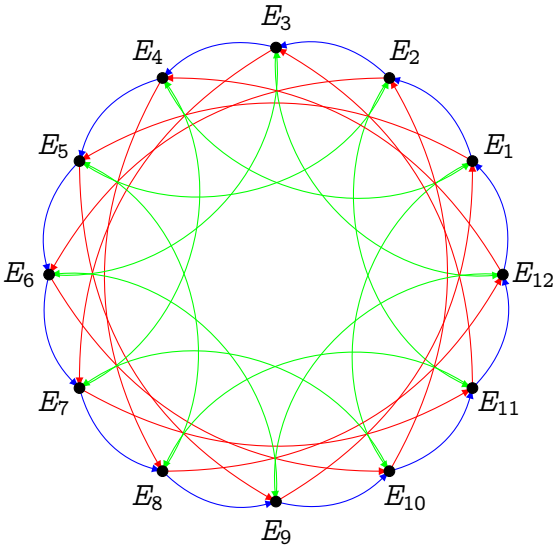
- Invertible ideal classes form a finite abelian group
- $\mathrm{Cl}(\mathcal{O})$ acts freely and transitively on the set of elliptic curves with $\mathrm{End}(E) \simeq \mathcal{O}$.

Class group action



Action $E_2 = E_1^{\bullet}$
$E_5 = E_1^{\bullet}$
$E_{10} = E_1^{\bullet}$

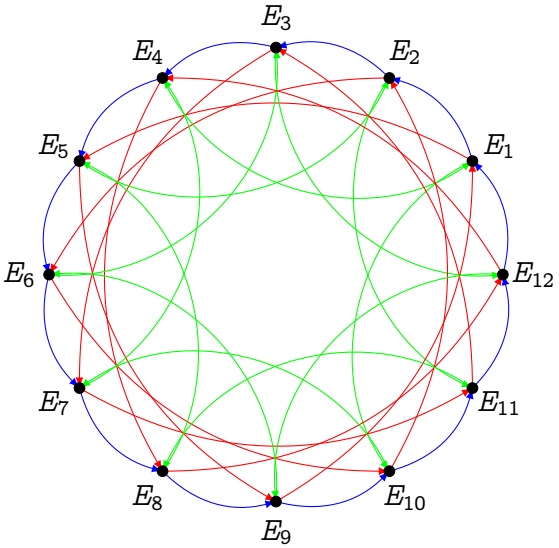
Class group action



Group $((E^{\bullet})^{\bullet})^{\bullet} = E^{(\bullet\bullet\bullet)} = E_1^{\bullet}$

Action $E_2 = E_1^{\bullet}$
$E_5 = E_1^{\bullet}$
$E_{10} = E_1^{\bullet}$

Class group action



Commutative $E^{(\bullet\bullet)} = E^{(\bullet\bullet)}$

Group $((E^{\bullet})^{\bullet})^{\bullet} = E^{(\bullet\bullet\bullet)} = E_1^{\bullet}$

Action $E_2 = E_1^{\bullet}$
$E_5 = E_1^{\bullet}$
$E_{10} = E_1^{\bullet}$

Two computational worlds

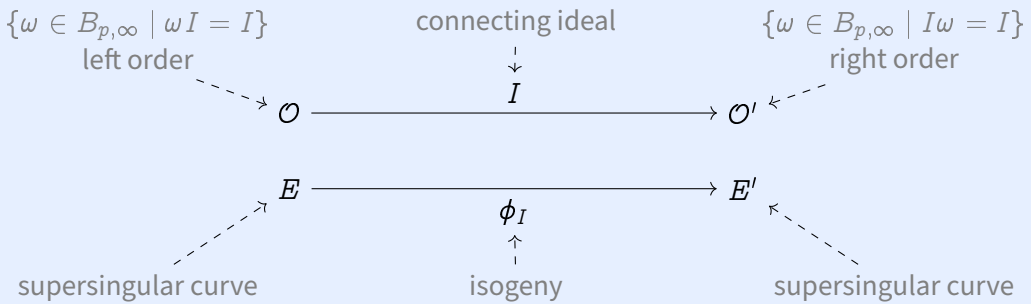
	Quadratic imaginary	Quaternionic
$\mathrm{rank}\,\mathrm{Hom}(E, E')$	2	4
Endomorphism algebra	number field	quaternion algebra
Maximal orders	one	many
Ideal class…	…group	…set
Find isogeny $E \to E'$	hard	hard
Convert isogenies $\leftrightarrow$ ideals	easy[1]	easy[1]
Compute $\mathrm{End}(E)$	easy	hard

[1] When $\mathrm{End}(E)$ is known

A forensic category

The Deuring correspondence (for supersingular curves)

An equivalence of categories (roughly)



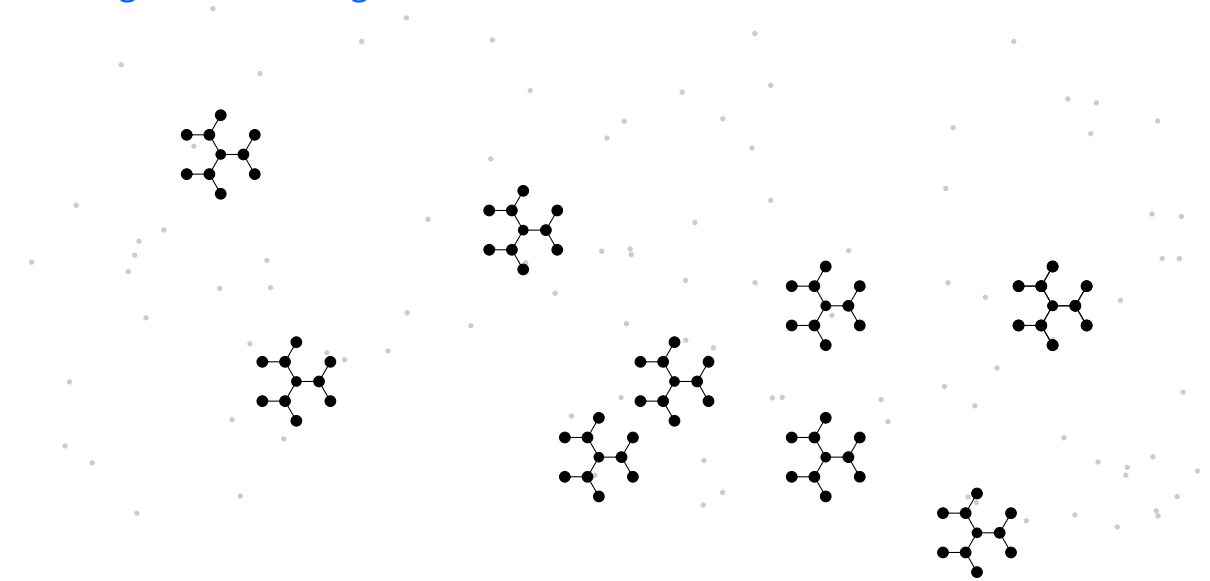
The endomorphism ring problem

Given a random supersingular curve E, compute $\mathrm{End}(E)$

Contagious knowledge

Contagious knowledge

Contagious knowledge



$\mathrm{End}(E)$ as a trapdoor

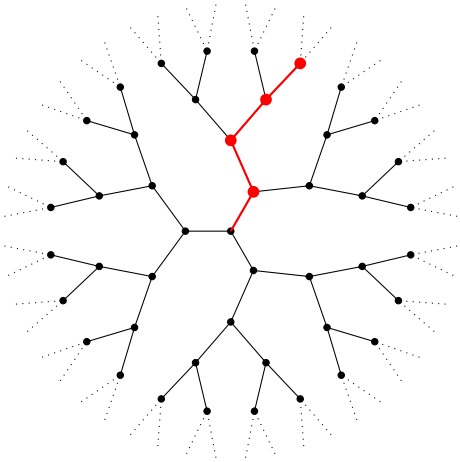
Input	Output	
random E	$\mathrm{End}(E)$	hard
random E	$\omega \in \mathrm{End}(E)$	hard
random E	$\phi : E_0 \to E$	hard
$\mathrm{End}(E)$	E	easy
$\mathrm{End}(E), \mathrm{End}(E')$	connecting ideal	easy
$I \subset \mathrm{End}(E)$	$\phi_I : E \to E'$	easy
$\mathrm{End}(E), \quad \phi : E \to E'$	$I_\phi \subset \mathrm{End}(E), \quad \mathrm{End}(E')$	easy

Axiom: *Walking*

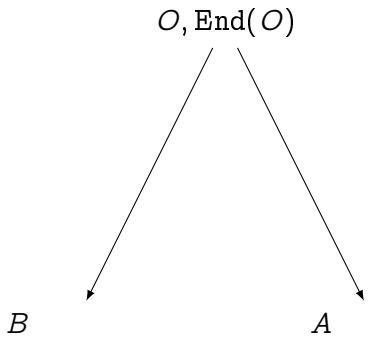
Efficient algorithm for:

Input: Curve A

Output:
- Uniformly random curve B,
- Random isogeny $\phi : A \to B$.

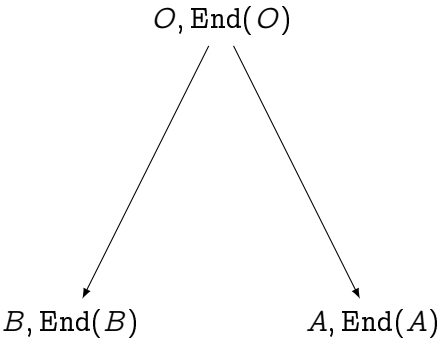


Axiom: Triangularizable



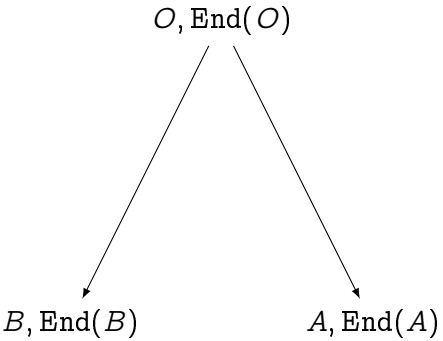
Input

Axiom: Triangularizable

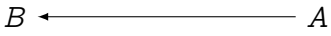


Input

Axiom: Triangularizable

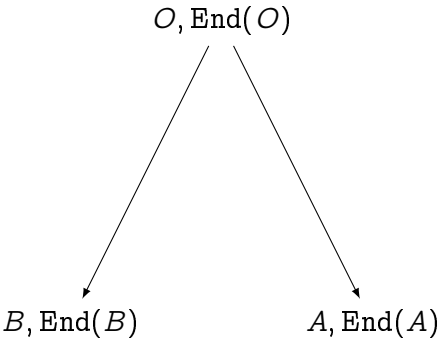


Input



Output

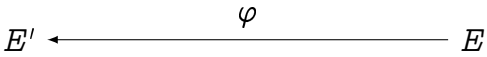
Axiom: Triangularizable



Input

Output

Fingerprints



How the isogeny acts on points of order N:

Kernel fingerprint: $\ker \varphi \cap E[N]$

(OG SQIsign)

Level fingerprint: Action on fixed bases of $E[N]$ and $E'[N]$

(joint with Borin, Lido, Schaeffler)

Worth the effort?

SQIsign v2 (June 2025)

	Sizes (bytes)		Timings (ms)		
Security	Public Key	Signature	Keygen	Sign	Verify
NIST-1	66	148	25	60	3
NIST-3	98	222	67	161	9
NIST-5	130	294	119	300	18

What crypto from isogenies?

	Key exchange / Encryption	Identification / Signature	Other
Quadratic (Group actions)	Couveignes–Rostovtsev–Stolbunov CSIDH SCALLOP	SeaSign CSI-FiSh PEGASIS	Threshold PAKE …
Quaternionic (Forensic cat.)	—	SQIsign SIDH-like signatures	Ring signatures Adaptor signatures Chameleon hash …
Ad hoc (Level structures)	SIDH † SIDH fixes FESTA	SIDH-like signatures	Time-release crypto …

Thank you

https://defeo.lu/

@luca_defeo@ioc.exchange

@bsky.defeo.lu