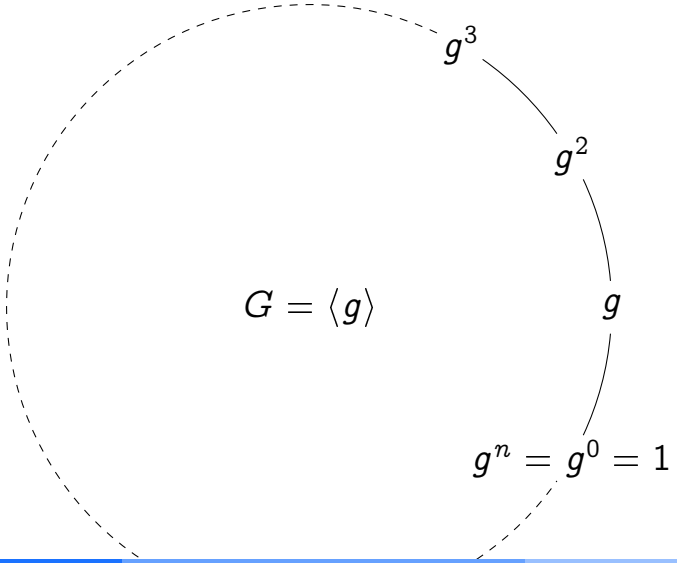
Group and Groupoid Actions
as a Foundation for Post-quantum Cryptography

Luca De Feo
IBM Research Zürich

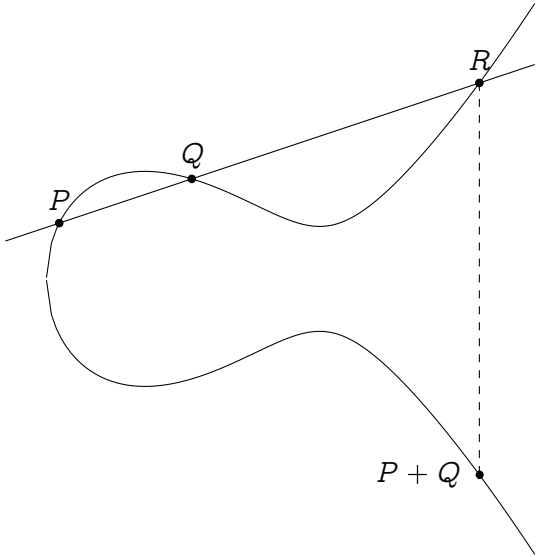
June 30, 2025
Summer School on real-world crypto and privacy Dubrovnik, Croatia

A cyclic group

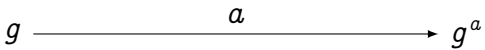


A cryptographer's favourite cyclic group

$$y^2 = x^3 + ax + b$$



The discrete logarithm one-way function



Setup: A cyclic group $G = \langle g \rangle$

Easy: $a \mapsto g^a$

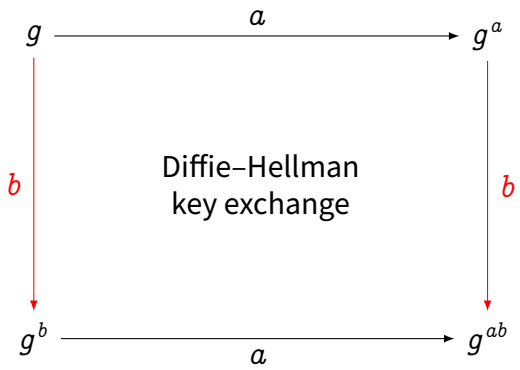
Hard: $g^a \mapsto a$

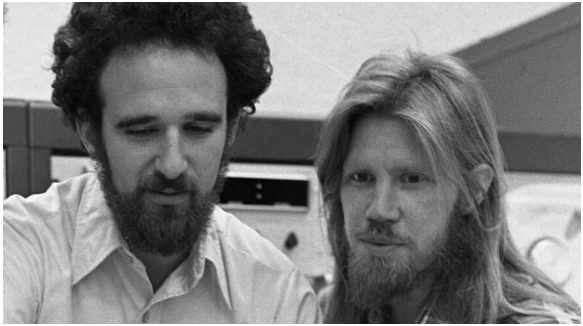
The discrete logarithm one-way function

Setup: A cyclic group $G = \langle g \rangle$

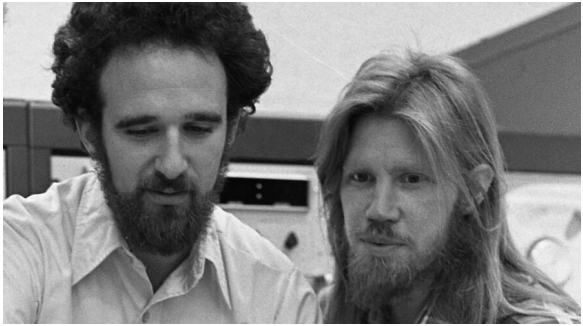
Easy: $a \mapsto g^a$

Hard: $g^a \mapsto a$





Diffie–Hellman key exchange



Diffie–Hellman key exchange

Shor's algorithm

Only two ways to Post-quantum Encryption

Noisy linear algebra:

Lattices, Codes

Far-fetched generalizations of the discrete logarithm:

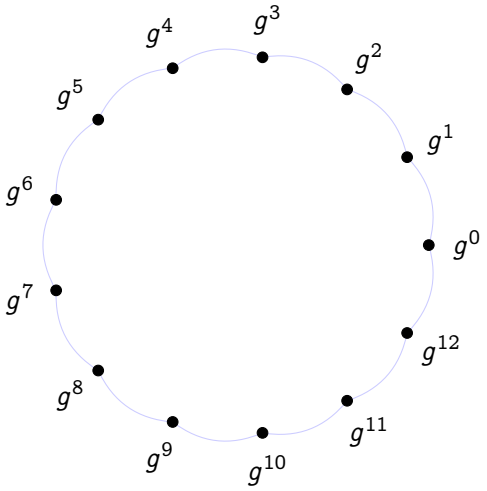
Isogenies

What crypto from isogenies?

	Key exchange/Encryption	Identification/Signature	Other
Group action	Couveignes–Rostovtsev–Stolbunov CSIDH SCALLOP	SeaSign CSI-FiSh PEGASIS	Threshold PAKE …
Groupoid action	—	Galbraith–Petit–Silva SQIsign SIDH-like signatures	Ring signatures Adaptor signatures …
Ad hoc[1]	SIDH † SIDH fixes FESTA	SIDH-like signatures	Time-release crypto …

[1] see D., Fouotsa, Panny, *"Isogeny problems with level structure"*, `https://ia.cr/2024/459`

What's needed for key exchange?



The axioms of a dlog group:

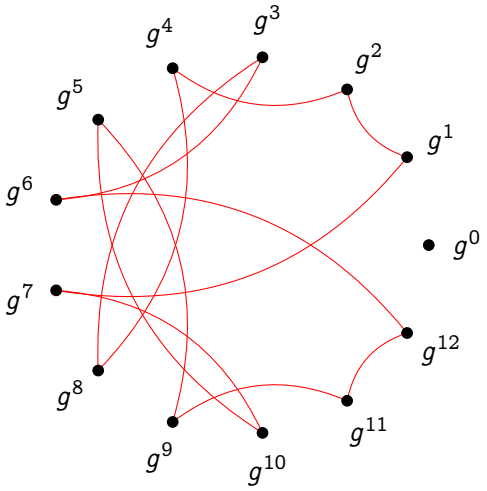
prod: ~~$g^a g^b = g^{a+b}$~~,

exp: $(g^a)^b = g^{ab} = (g^b)^a$.

The hard problem:

dlog: $g^a \mapsto a$.

What's needed for key exchange?



The axioms of a dlog group:

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

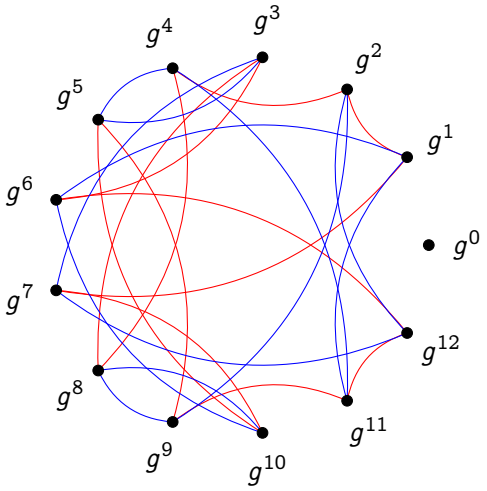
exp: $(g^a)^b = g^{ab} = (g^b)^a$.

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: $(g^a)^b = g^{ab} = (g^b)^a$.

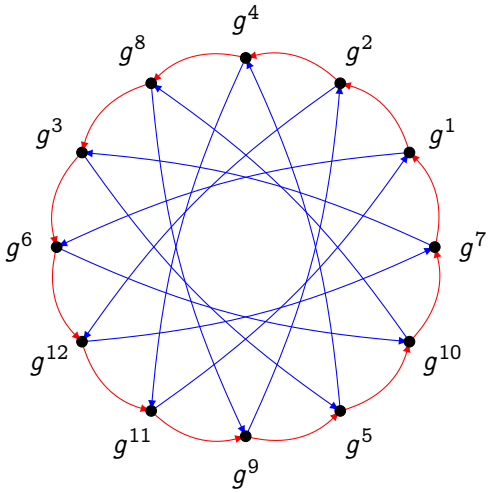
The hard problem:

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: $(g^a)^b = g^{ab} = (g^b)^a$.

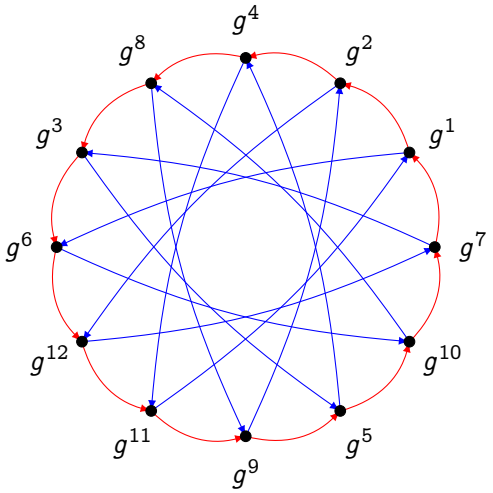
The hard problem:

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: $(g^a)^b = g^{ab} = (g^b)^a$.

The hard problem:

dlog: $g^a \mapsto a$.

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

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

Automorphism group: $(\mathbb{Z}/13\mathbb{Z})^\times$.

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 $\mathfrak{g} * E' = E$.

Group action

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

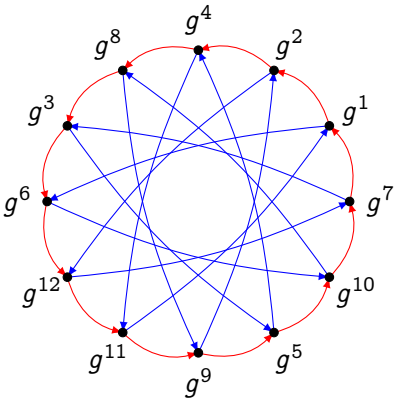
$$\begin{aligned} * : \mathcal{G} \times \mathcal{E} &\longrightarrow \mathcal{E} \\ \mathfrak{g} * E &\longmapsto E' \end{aligned}$$

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

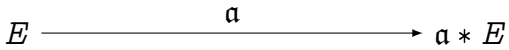
Identity: $\mathfrak{e} * E = E$ if and only if $\mathfrak{e} \in \mathcal{G}$ is the identity element;

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

Example: $(\mathbb{Z}/13\mathbb{Z})^* \quad \circlearrowright \quad (C_{13} \setminus \{1\})$



Cryptographic Group Actions



Setup: A group action $\mathcal{G} \circlearrowright \mathcal{E}$

Easy: $\mathfrak{g} \quad \mapsto \quad \mathfrak{g} * E$
(evaluation)

Hard: $\mathfrak{g} * E \quad \mapsto \quad \mathfrak{g}$
(inversion)

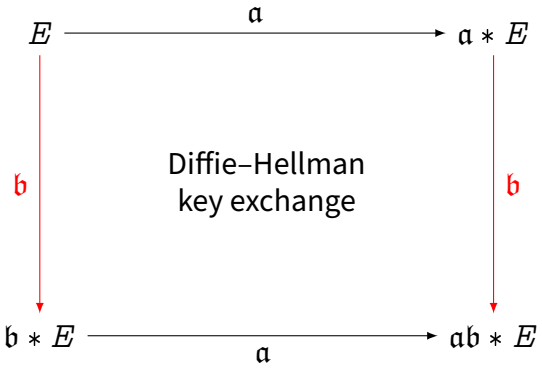
[1] Couveignes 1997. `https://ia.cr/2006/291`
[2] Alamati, D., Montgomery, Patranabis 2021. `https://ia.cr/2020/1188`

Cryptographic Group Actions

Setup: A group action $\mathcal{G} \curvearrowright \mathcal{E}$ with $\mathcal{G}$ commutative

Easy: $\mathfrak{g} \quad \mapsto \quad \mathfrak{g} * E$
(evaluation)

Hard: $\mathfrak{g} * E \quad \mapsto \quad \mathfrak{g}$
(inversion)



[1] Couveignes 1997. https://ia.cr/2006/291
[2] Alamati, D., Montgomery, Patranabis 2021. https://ia.cr/2020/1188

Cryptographic Group Actions in the Wild

Abelian

- Discrete logarithm
- Isogenies:
  - Complex multiplication (Couveignes–Rostovtsev–Stolbunov)
  - π-oriented (CSIDH)
  - Arbitrary orientations (SCALLOP, …)

Non-Abelian

- Isomorphism of Codes (PCE, LCE)
- Lattice Isomorphism
- Graph Isomorphism

Cryptographic Group Actions in the Wild

Abelian

- Discrete logarithm
- Isogenies:
  - Complex multiplication (Couveignes–Rostovtsev–Stolbunov)
  - π-oriented (CSIDH)
  - Arbitrary orientations (SCALLOP, …)

Non-Abelian

- Isomorphism of Codes (PCE, LCE)
- Lattice Isomorphism
- ~~Graph Isomorphism~~

Cryptographic Group Actions in the Wild

Abelian

- ~~Discrete logarithm~~
- Isogenies:
  - Complex multiplication (Couveignes–Rostovtsev–Stolbunov)
  - π-oriented (CSIDH)
  - Arbitrary orientations (SCALLOP, …)

Non-Abelian

- Isomorphism of Codes (PCE, LCE)
- Lattice Isomorphism
- ~~Graph Isomorphism~~

Quantum security

Group Action Inversion $\rightarrow$ Hidden Shift Problem

Abelian:

- Abelian Hidden Shift Problem $\rightarrow$ Dihedral Hidden Subgroup Problem
- Kuperberg's algorithm (quantum subexponential time)

Non-Abelian: no quantum speedup known

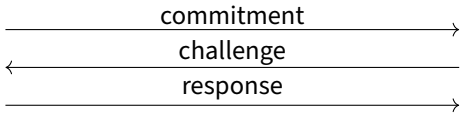
Zero-Knowledge Proofs of Knowledge (ZK-PoK)

Prover

NP statement, witness

Verifier

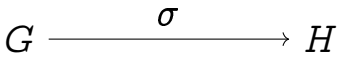
NP statement



Σ-protocols

"OK, I believe you!"

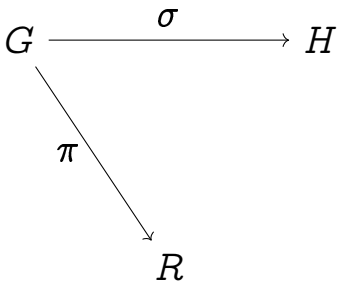
A ZK-PoK for Graph Isomorphism (after Goldwasser–Micali–Rackoff)



Prover

Verifier

A ZK-PoK for Graph Isomorphism (after Goldwasser–Micali–Rackoff)



Prover

Verifier

R

A ZK-PoK for Graph Isomorphism (after Goldwasser–Micali–Rackoff)

$$G \xrightarrow{\sigma} H$$

$$R$$

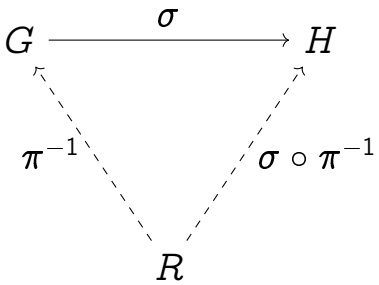
Prover

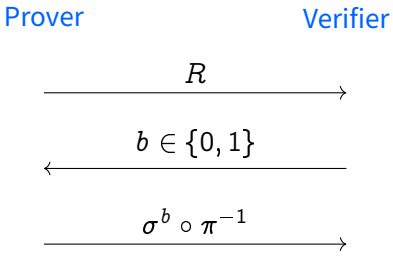
Verifier

$$\xrightarrow{R}$$

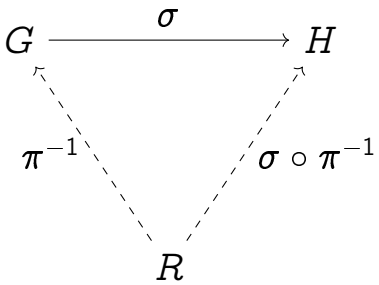
$$\xleftarrow{b \in \{0,1\}}$$

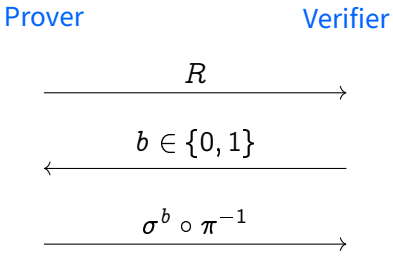
A ZK-PoK for Graph Isomorphism (after Goldwasser–Micali–Rackoff)





A ZK-PoK for Graph Isomorphism (after Goldwasser–Micali–Rackoff)





Basis for: SeaSign / CSI-FiSh (isogenies), LESS (codes)

Groupoids

A groupoid is a non-empty set $\mathcal{G}$ with two operations

Inverse: $^{-1} : \mathcal{G} \to \mathcal{G}$

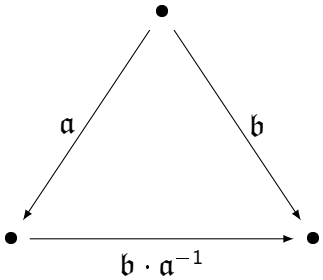
Product: a partial function $\cdot : \mathcal{G} \times \mathcal{G} \rightharpoonup \mathcal{G}$

And axioms

Associativity: $\mathfrak{a} \cdot (\mathfrak{b} \cdot \mathfrak{c}) = (\mathfrak{a} \cdot \mathfrak{b}) \cdot \mathfrak{c}$ if either is defined,

Inverse: $\mathfrak{a} \cdot \mathfrak{a}^{-1}$ and $\mathfrak{a}^{-1} \cdot \mathfrak{a}$ are always defined,

Identity: if $\mathfrak{a} \cdot \mathfrak{b}$ is defined $\mathfrak{a} \cdot \mathfrak{b} \cdot \mathfrak{b}^{-1} = \mathfrak{a}$ and $\mathfrak{a}^{-1} \cdot \mathfrak{a} \cdot \mathfrak{b} = \mathfrak{b}$.



Groupoid action

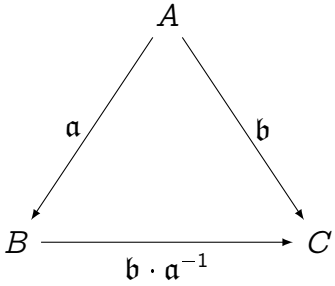
$\mathcal{G} \circlearrowright \mathcal{E}$: A (finite) set $\mathcal{E}$ acted upon by a groupoid $\mathcal{G}$ freely and transitively:

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

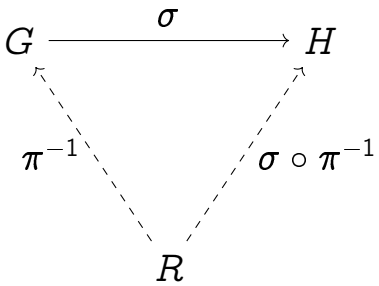
Compatibility: $\mathfrak{g}' * (\mathfrak{g} * E) = (\mathfrak{g}'\mathfrak{g}) * E$ whenever either is defined;

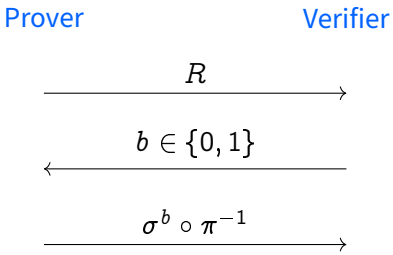
Identity: $(\mathfrak{g}^{-1}\mathfrak{g}) * E = E$ whenever $\mathfrak{g} * E$ is defined;

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



A ZK-PoK from Groupoid Actions





Galbraith–Petit–Silva 2016: it works!!! …in a very special case and with lots of quirks

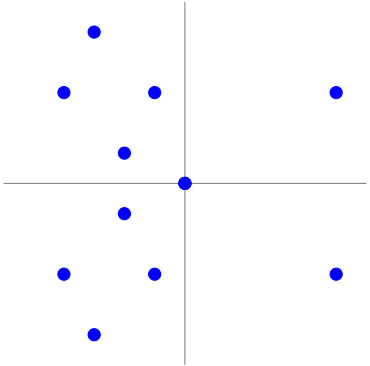
Morphisms of elliptic curves

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

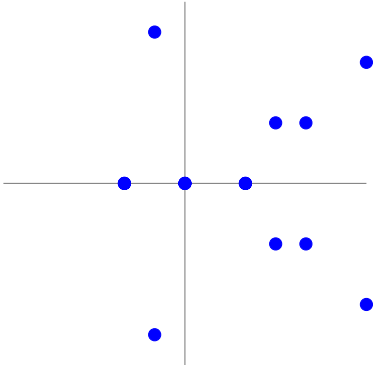
Endomorphisms = isogenies $E \to E$

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

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

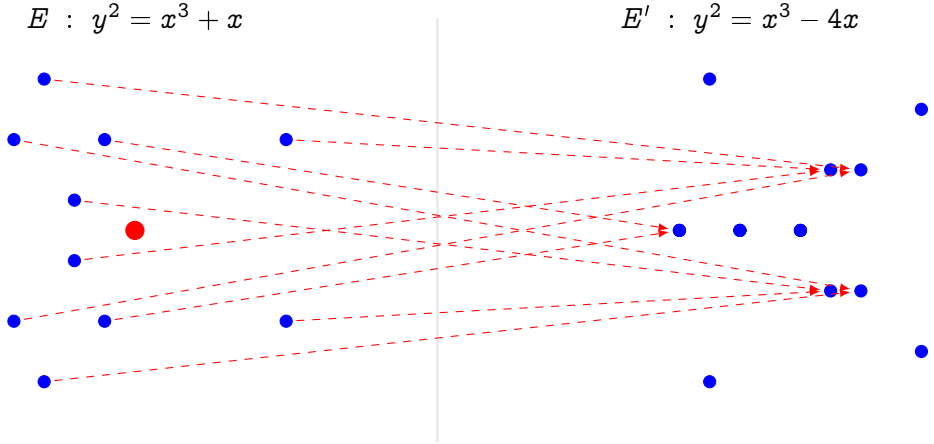


$E' : y^2 = x^3 - 4x$



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

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

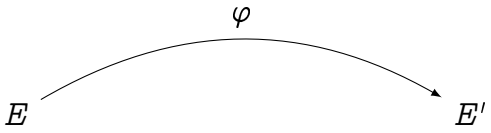


$$\phi(x, y) = \left(\frac{x^2 + 1}{x}, \quad y \frac{x^2 - 1}{x^2} \right)$$

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

Degree and dual

Let $\varphi : E \to E'$. There exist:

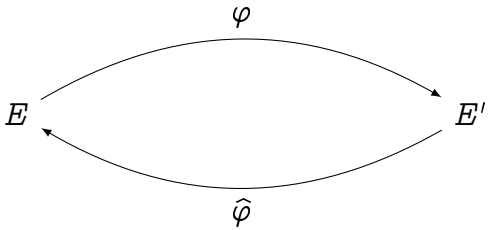


Degree and dual

Let $\varphi : E \to E'$. There exist:

Degree: a smallest integer $d > 0$, and

Dual: a unique isogeny $\widehat{\varphi} : E' \to E$,

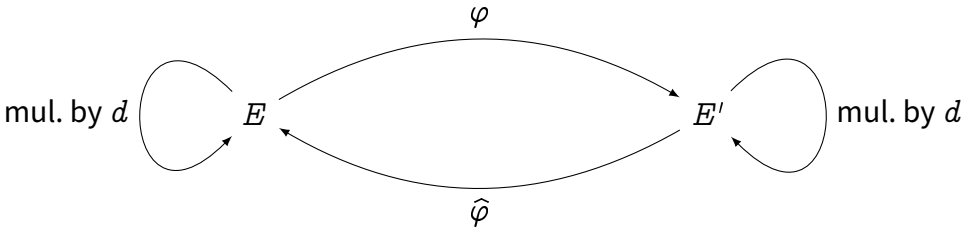


Degree and dual

Let $\varphi : E \to E'$. There exist:

Degree: a smallest integer $d > 0$, and

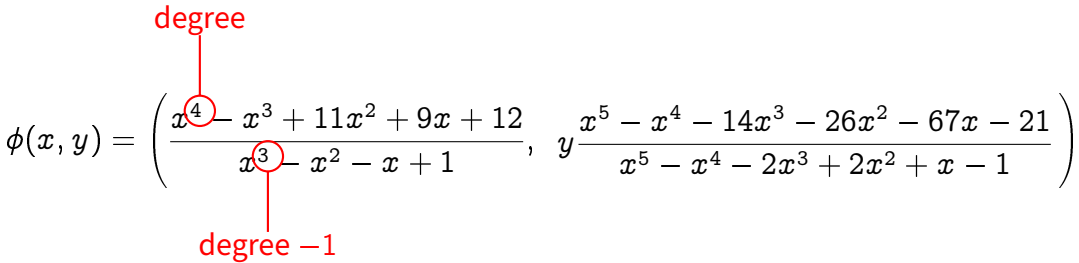
Dual: a unique isogeny $\widehat{\varphi} : E' \to E$,
such that:



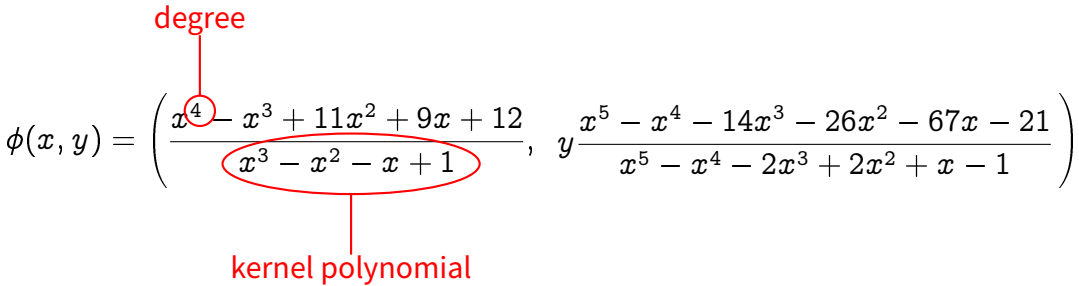
Anatomy of an isogeny

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

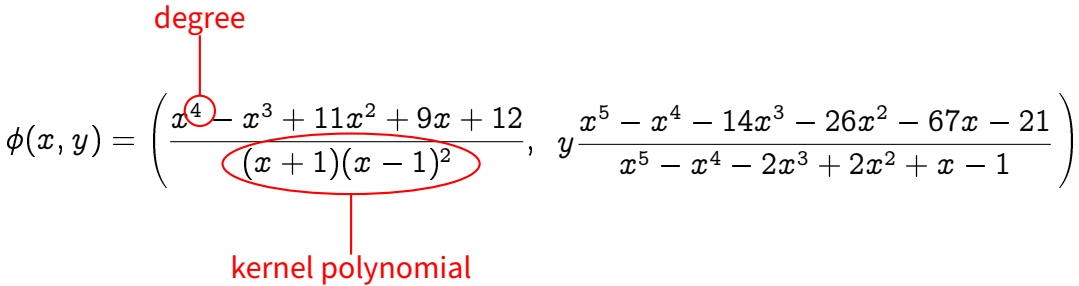
Anatomy of an isogeny



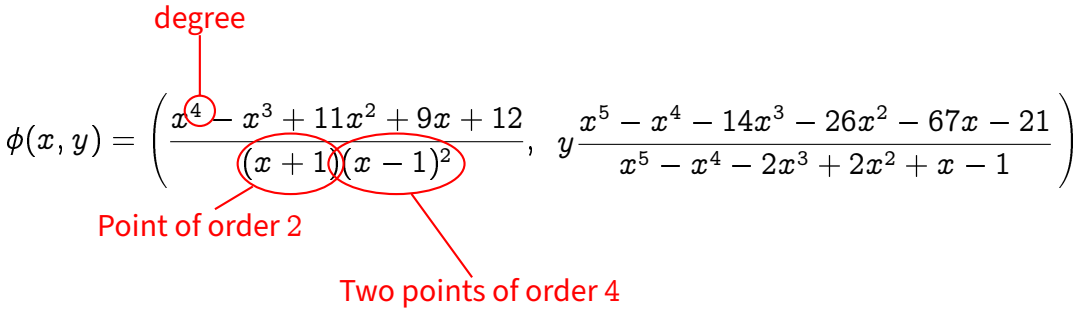
Anatomy of an isogeny



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.

How many isogenies?

Finite subgroups of order d

$K \subset E$

$\longleftrightarrow$

Isogenies of degree d

$\phi : E \to E/K$

(up to composing with isomorphism)

How many isogenies?

Finite subgroups of order d

$K \subset E$

$\longleftrightarrow$

Isogenies of degree d

$\phi : E \to E/K$

(up to composing with isomorphism)

Examples:

If d is prime $\quad \to$ at most $d + 1$ possible kernels,

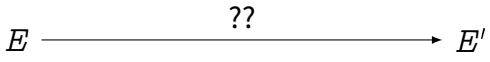
In general $\quad \to$ at most $\approx d$ possible kernels.

The isogeny one-way function

Setup: A class of isogenous curves

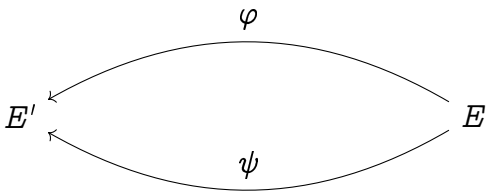
Easy: $E, K \quad \mapsto \quad E/K$

Hard: $E, E/K \quad \mapsto \quad K$



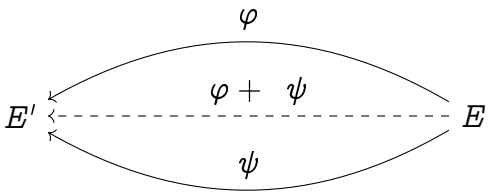
Do isogenies form a groupoid?

Lattices of isogenies



$$\varphi, \psi \in \mathrm{Hom}(E, E')$$

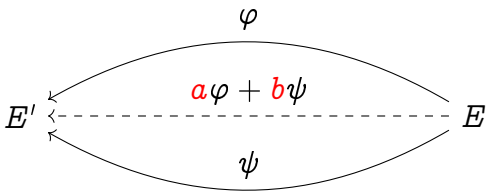
Lattices of isogenies



$$\varphi, \psi \in \mathrm{Hom}(E, E')$$

$$(\varphi + \psi)(P) := \varphi(P) + \psi(P)$$

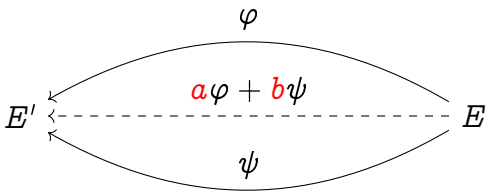
Lattices of isogenies



$$\varphi, \psi \in \mathrm{Hom}(E, E') \qquad a, b \in \mathbb{Z}$$

$$(a\varphi + b\psi)(P) := [a]\varphi(P) + [b]\psi(P)$$

Lattices of isogenies



$$\varphi, \psi \in \mathrm{Hom}(E, E') \qquad a, b \in \mathbb{Z}$$

$$(a\varphi + b\psi)(P) := [a]\varphi(P) + [b]\psi(P)$$

- $\deg(a\varphi) = a^2 \deg(\varphi)$,
- $\left|\deg(\varphi + \psi) - \deg(\varphi) - \deg(\psi)\right| \leq 2\sqrt{\deg(\varphi)\deg(\psi)}$,
- deg is a positive definite quadratic form.

Endomorphism rings

- $\mathrm{Hom}(A, B)$: additive group
- Distributivity:

$$\varphi \circ (\psi + \chi) = (\varphi \circ \psi) + (\varphi \circ \chi)$$

$$(\psi + \chi) \circ \varphi = (\psi \circ \varphi) + (\chi \circ \varphi)$$

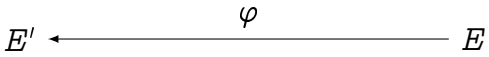
- It follows that $\mathrm{End}(A) := \mathrm{Hom}(A, A)$ is a ring.

Endomorphism rings

$\mathrm{End}(E)$ is a free $\mathbb{Z}$-module of rank 1, 2 or 4. As a ring:

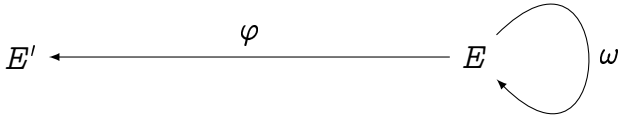
1) $\mathrm{End}(E) \simeq \mathbb{Z}$;
2) $\mathrm{End}(E) \subset$ quadratic imaginary field;
4) $\mathrm{End}(E) \subset$ quaternion algebra.

Isogenies = $\mathrm{End}(E)$-Ideals



$$\varphi \in \mathrm{Hom}(E, E')$$

Isogenies = $\mathrm{End}(E)$-Ideals



$$\varphi \circ \omega \in \mathrm{Hom}(E, E')$$

Isogenies = $\mathrm{End}(E)$-Ideals

$$\omega' \circ \varphi \in \mathrm{Hom}(E, E')$$

The Deuring correspondence: Isogenies $\longleftrightarrow$ Ideals

$\mathrm{Hom}(E, E')$ is a free $\mathbb{Z}$-module of rank 1, 2 or 4.

It is a rank-1 projective $\mathrm{End}(E)$-module, isomorphic to:

1) an ideal of $\mathbb{Z}$;
2) an invertible ideal of a quadratic imaginary field;
4) an invertible ideal of a quaternion algebra.

As a quadratic module: degree $\longleftrightarrow$ norm

The Deuring correspondence: Isogenies $\longleftrightarrow$ Ideal classes

Equivalent ideals:

$$I \simeq J \quad \iff \quad I = J\alpha$$

Deuring correspondence:

$$\mathrm{Hom}(E, E') \quad \longleftrightarrow \quad \mathrm{cls}(I)$$

Fact: the ideal classes $\mathrm{cls}(I)$ form a groupoid!

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	…groupoid
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

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 $\mathrm{End}(E) \simeq \mathcal{O}$.

What crypto from isogenies?

	Key exchange/Encryption	Identification/Signature	Other
Group action	Couveignes–Rostovtsev–Stolbunov CSIDH SCALLOP	SeaSign CSI-FiSh PEGASIS	Threshold PAKE …
Groupoid action	—	Galbraith–Petit–Silva SQIsign SIDH-like signatures	Ring signatures Adaptor signatures …
Ad hoc[2]	SIDH † SIDH fixes FESTA	SIDH-like signatures	Time-release crypto …

[2] see D., Fouotsa, Panny, *"Isogeny problems with level structure"*, `https://ia.cr/2024/459`

Performance of SQIsign

SQIsign v1 (June 2023)

	Sizes (bytes)		Timings (ms)		
Security	Public Key	Signature	Keygen	Sign	Verify
NIST-1	64	177	1,864	2,890	54
NIST-3	96	263	11,867	21,880	327
NIST-5	128	335	45,525	79,272	1,089

SQIsign v2 (June 2025)

NIST-1	66	148	25	60	3
NIST-3	98	222	67	161	9
NIST-5	130	294	119	300	18

Thank you

https://defeo.lu/

@luca_defeo@ioc.exchange

@bsky.defeo.lu