Isogeny-based Crypto
Coming of Age

Luca De Feo
IBM Research Zürich

May 13, 2026, Eurocrypt, Rome


When does one become an adult?

A brief history of ECC

1976 Diffie–Hellman key exchange

1977 RSA

A brief history of ECC

1976 Diffie–Hellman key exchange

1977 RSA

1985 Miller and Koblitz introduce elliptic curves to cryptography

A brief history of ECC

1976 Diffie–Hellman key exchange

1977 RSA

1985 Miller and Koblitz introduce elliptic curves to cryptography

1999 NIST standardizes its first elliptic curves

A brief history of ECC

1976 Diffie–Hellman key exchange
1977 RSA
1985 Miller and Koblitz introduce elliptic curves to cryptography
1994 Shor's quantum algorithm

1999 NIST standardizes its first elliptic curves

A brief history of ECC

1976 Diffie–Hellman key exchange
1977 RSA
1985 Miller and Koblitz introduce elliptic curves to cryptography
1994 Shor's quantum algorithm

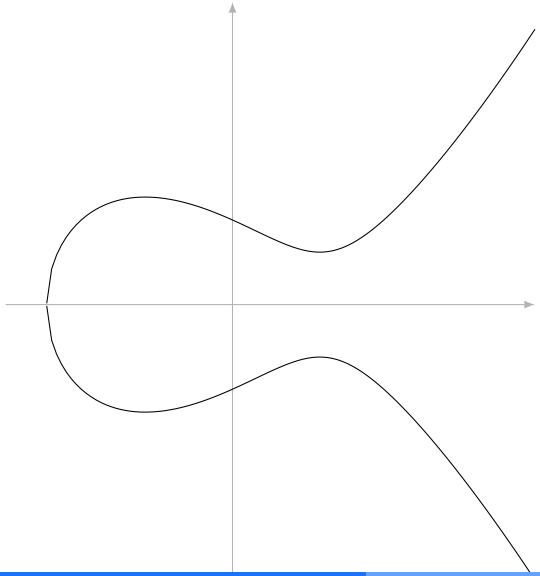
1999 NIST standardizes its first elliptic curves
2017 NIST calls for post-quantum algorithms

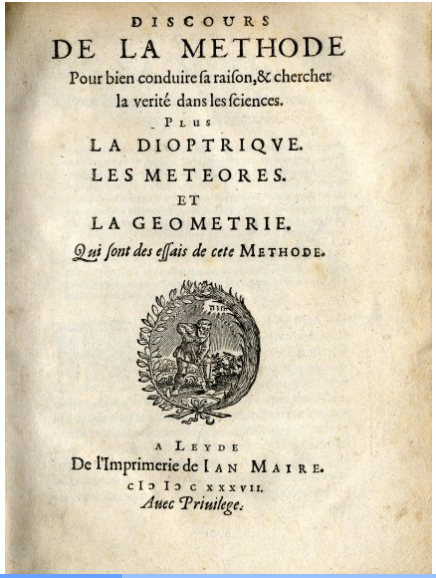
A brief history of ECC

1976 Diffie–Hellman key exchange
1977 RSA
1985 Miller and Koblitz introduce elliptic curves to cryptography
1994 Shor's quantum algorithm
1997 Couveignes' isogeny-based key exchange
1999 NIST standardizes its first elliptic curves
2017 NIST calls for post-quantum algorithms

High school isogenies

Geometry

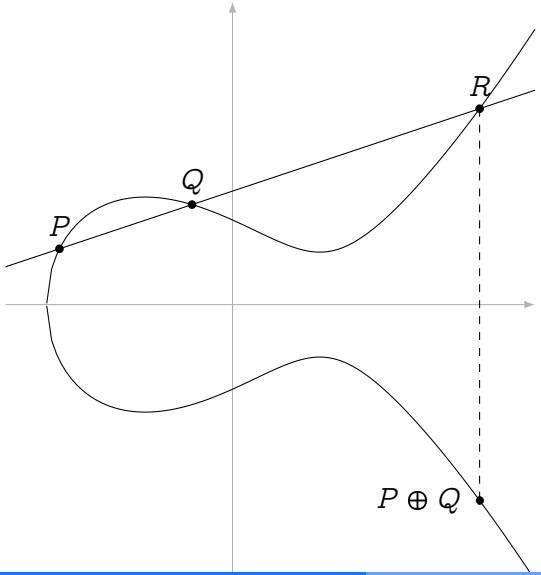




DISCOURS
DE LA METHODE
Pour bien conduire sa raison, & chercher
la verité dans les sciences.
Plus
LA DIOPTRIQVE.
LES METEORES.
ET
LA GEOMETRIE.
Qui sont des essais de cette METHODE.

A LEYDE
De l'Imprimerie de IAN MAIRE.
clɔ Iɔ c xxxvii.
Avec Privilege.

Groups


R
Q
P
P ⊕ Q


REPUBLIQUE FRANÇAISE
Evariste Galois
1811-1832
postes 1984
2,10+0,40
révolutionnaire et géomètre


NORGE
NIELS HENRIK ABEL
5 50
1802-1829

Isogenies

Algebraic morphisms: $\left(\dfrac{5x^2 + 5x + 4}{x + 1}, \quad y \dfrac{2x^2 + 4x - 4}{x^2 + 2x + 1} \right)$

Group morphisms: $\varphi(P + Q) = \varphi(P) + \varphi(Q)$

Isogenies

Algebraic morphisms: $\left(\dfrac{5x^2+5x+4}{x+1}, \quad y\dfrac{2x^2+4x-4}{x^2+2x+1}\right)$

→ Interpolation

Group morphisms: $\varphi(P+Q) = \varphi(P) + \varphi(Q)$

→ Groups **of** morphisms

Degree

$$\deg(\varphi) \in \mathbb{N}^+$$

- A measure of “size”;

Degree

$$\deg(\varphi) \in \mathbb{N}^+$$

- A measure of “size”;
- Multiplicative;

$$\deg(\psi \circ \varphi) = \deg(\psi)\deg(\varphi)$$

Degree

$$\deg(\varphi) \in \mathbb{N}^+$$

- A measure of “size”;
- Multiplicative;

$$\deg(\psi \circ \varphi) = \deg(\psi)\deg(\varphi)$$

- A measure of “complexity”:

  only isogenies of small degree fit into a computer!

The isogeny problem*

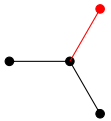
*Decisional problem **is easy**.

The isogeny problem*

*Decisional problem **is easy**.

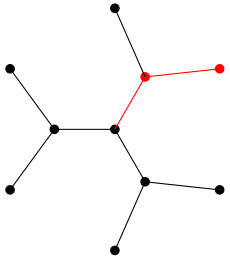
Isogeny graphs

degree 2



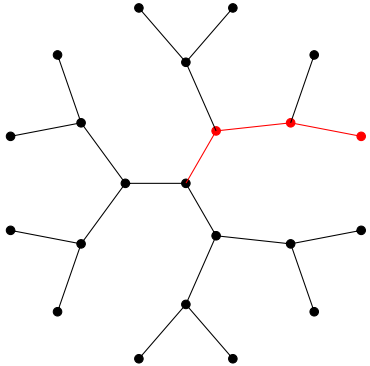
Isogeny graphs

degree 4



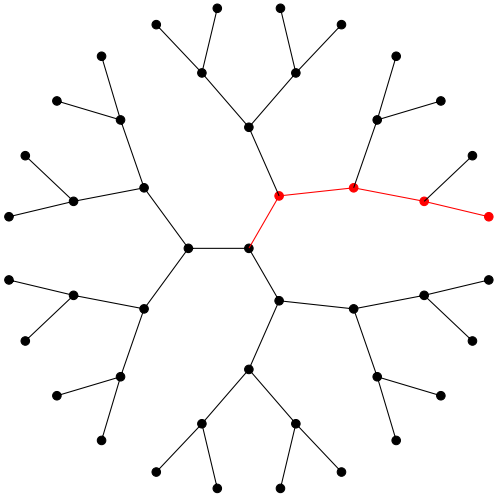
Isogeny graphs

degree 8



Isogeny graphs

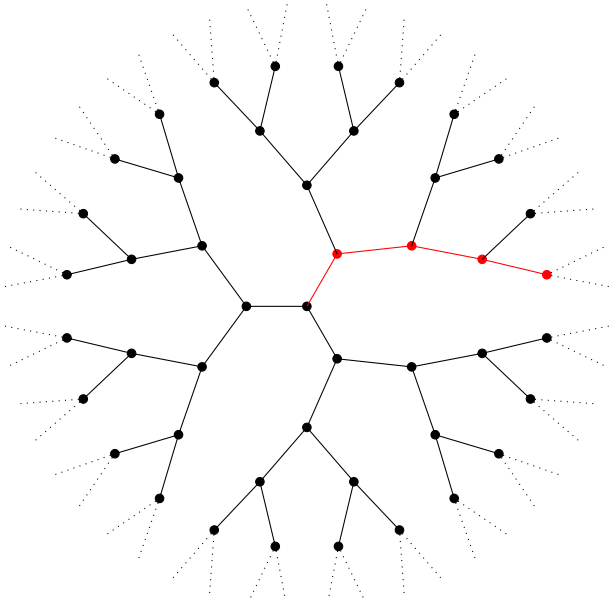
degree 16



Isogeny graphs

degree 2^x

$\rightarrow$ Isogeny **path** problem

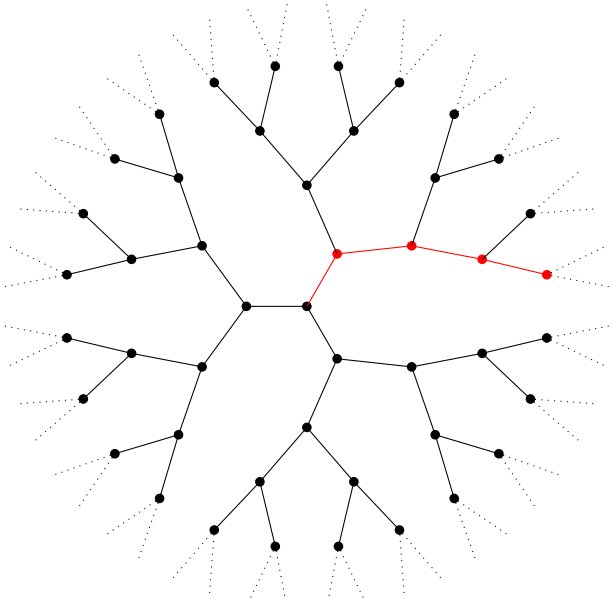


Isogeny graphs

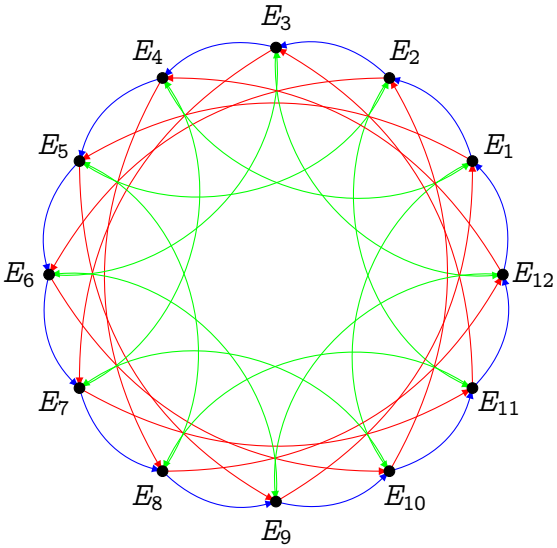
degree 2^x

$\rightarrow$ Isogeny **path** problem

$\rightarrow$ Hash functions
(Charles, Goren, Lauter '09)

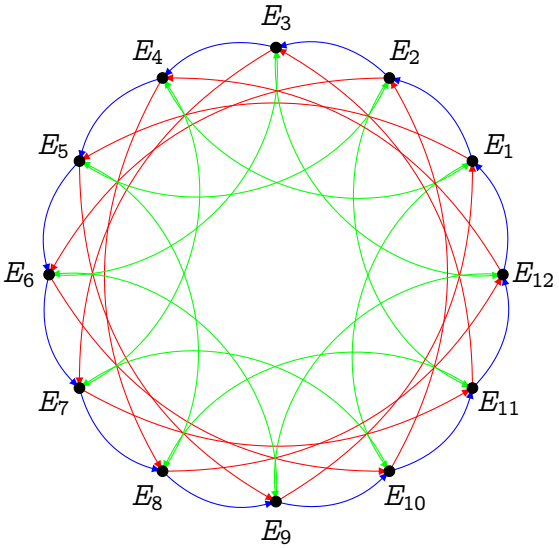


Couveignes ’97-’06 / Rostovtsev–Stolbunov ’06 / CSIDH ’19



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

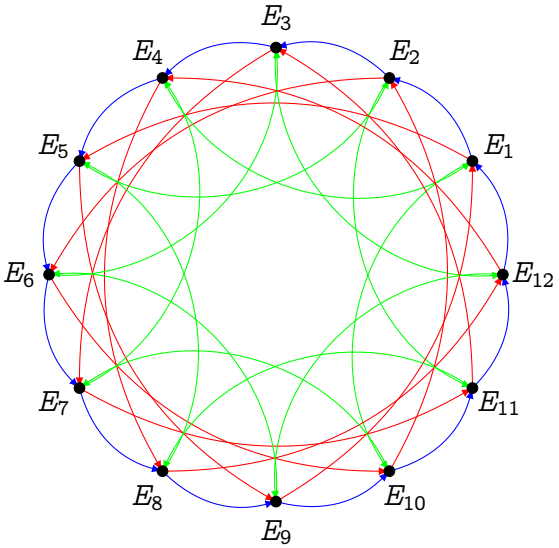
Couveignes ’97-’06 / Rostovtsev–Stolbunov ’06 / CSIDH ’19



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

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

Couveignes ’97-’06 / Rostovtsev–Stolbunov ’06 / CSIDH ’19

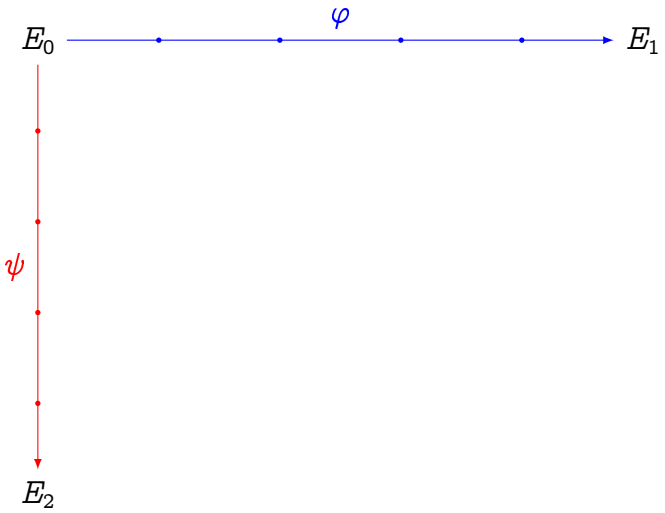


Commutative $E^{(\bullet\bullet)} = E^{(\bullet\bullet)}$

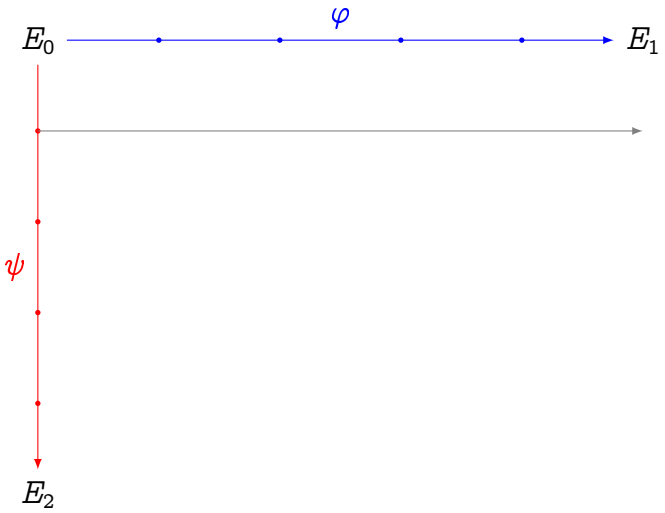
Group $((E^{\bullet})^{\bullet})^{\bullet} = E^{(\bullet\bullet\bullet)} = E_1^{\bullet}$

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

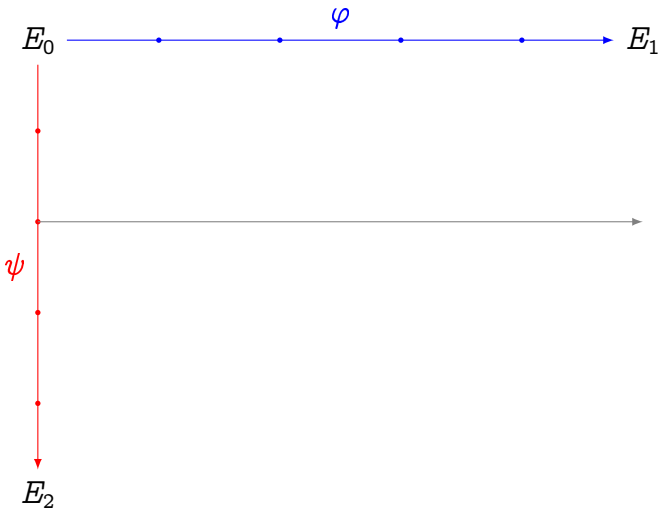
SIDH ’11 / SIKE ’17



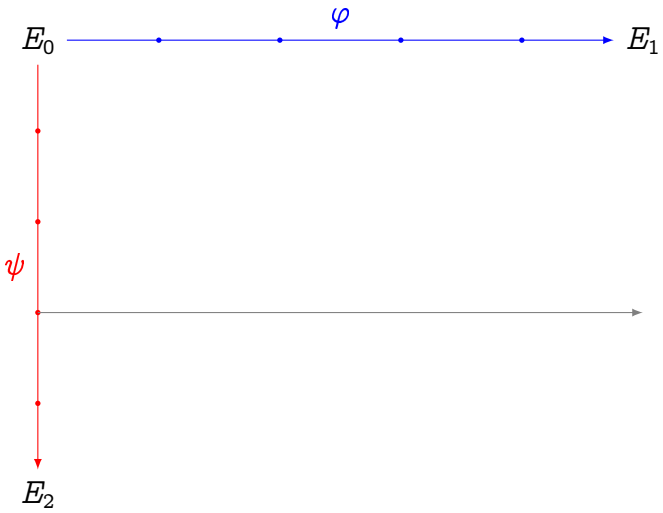
SIDH ’11 / SIKE ’17



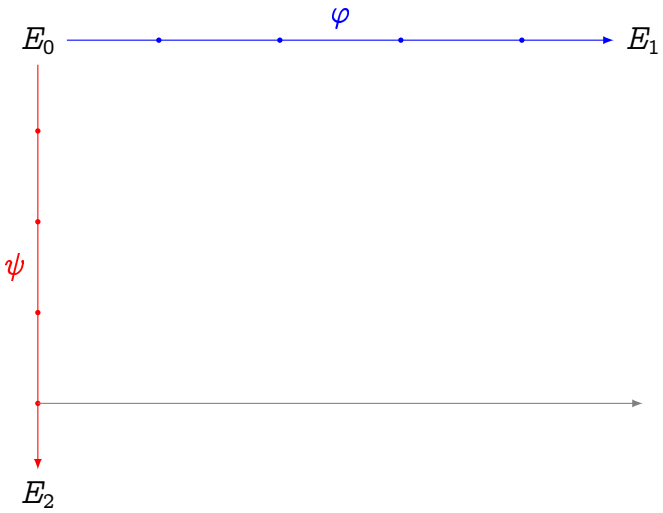
SIDH ’11 / SIKE ’17



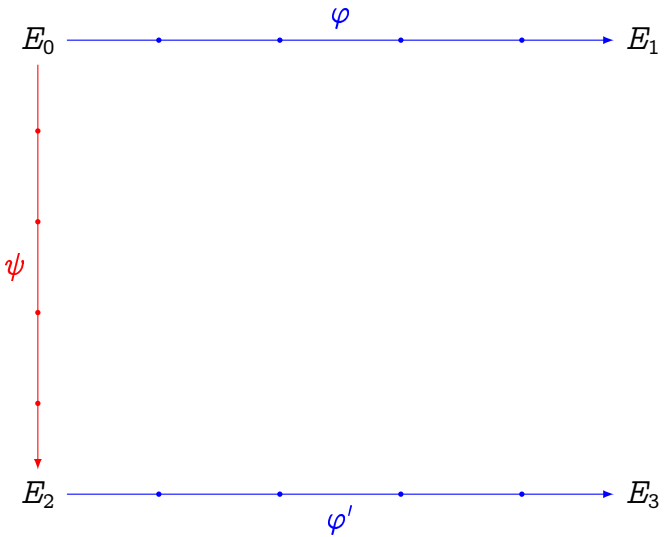
SIDH ’11 / SIKE ’17



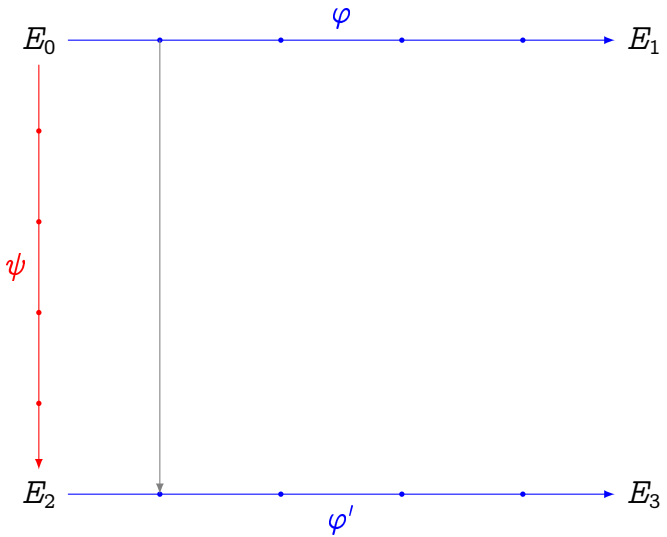
SIDH ’11 / SIKE ’17



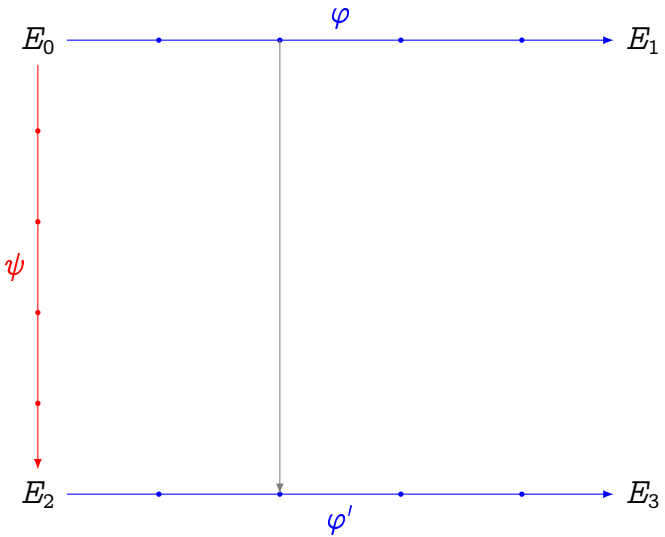
SIDH ’11 / SIKE ’17



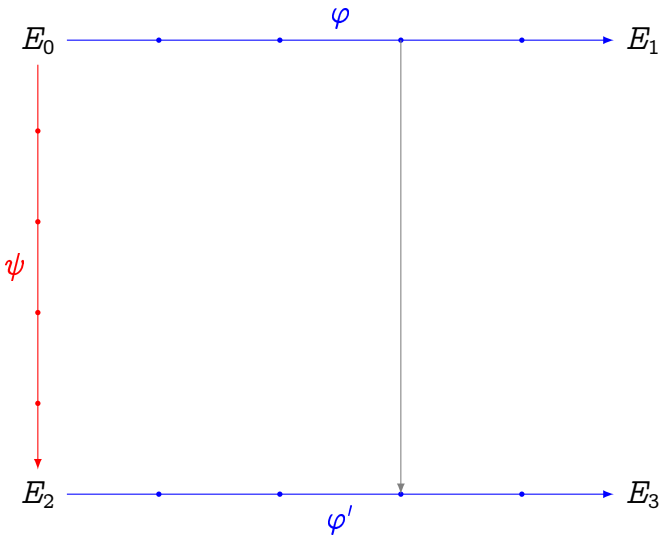
SIDH ’11 / SIKE ’17



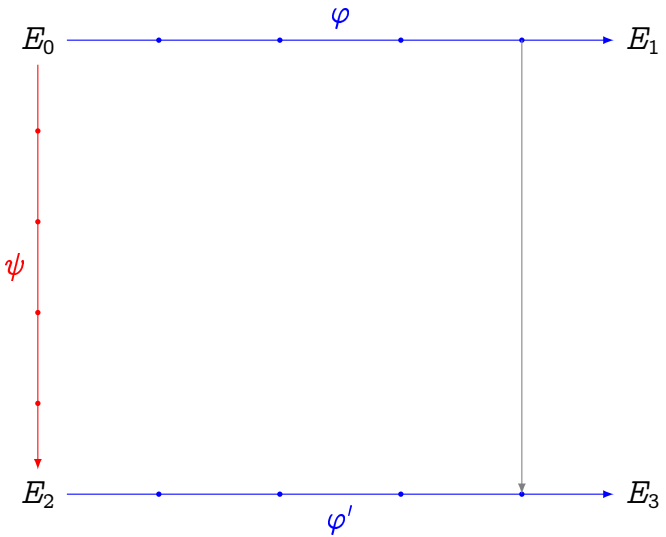
SIDH ’11 / SIKE ’17



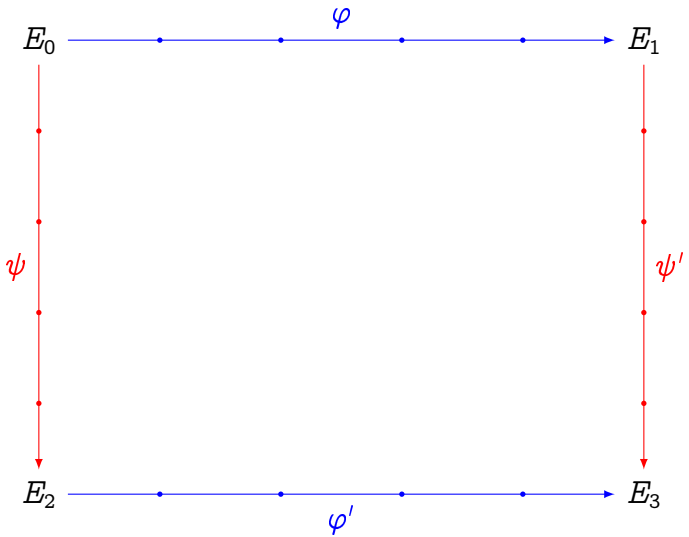
SIDH ’11 / SIKE ’17



SIDH ’11 / SIKE ’17

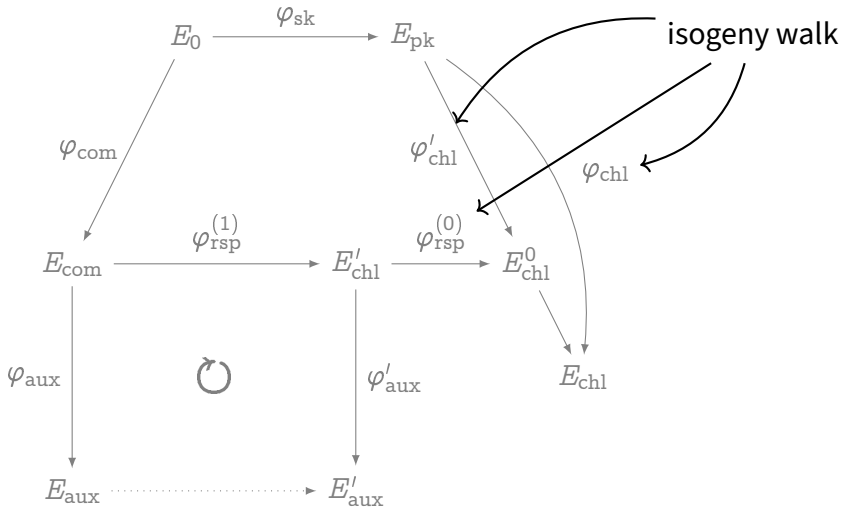


SIDH ’11 / SIKE ’17



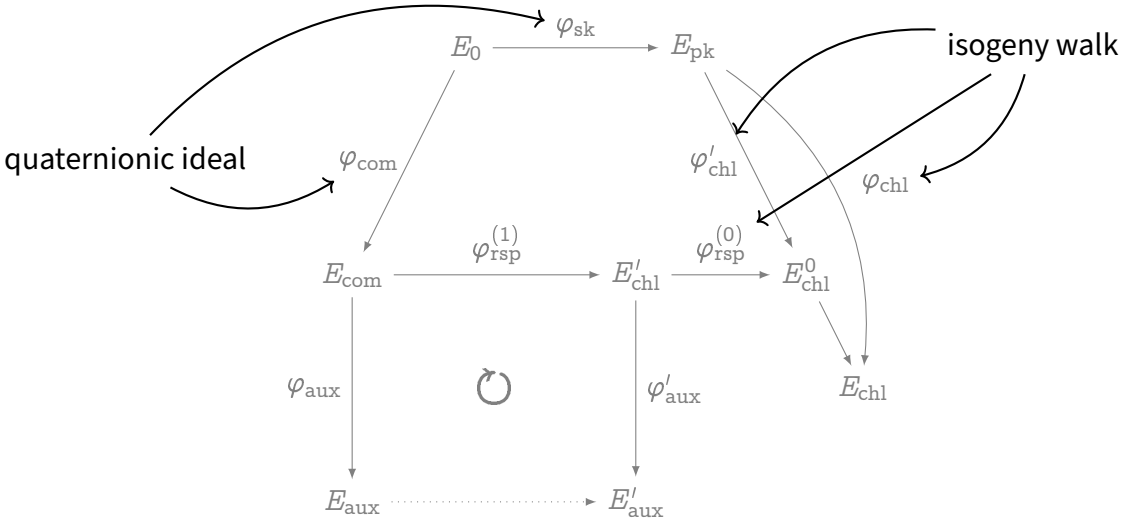

AND THEN THEY SAID...
OUR KEY EXCHANGE IS QUANTUM-SAFE!

SQisign '20



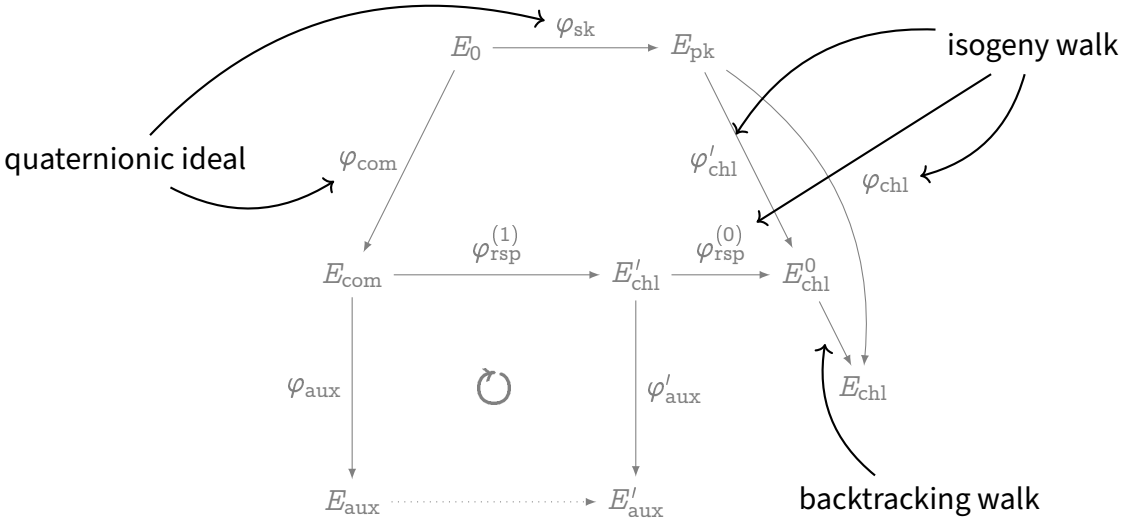
[1] From *"SQIsign2D–West: The Fast, the Small, and the Safer"*, Asiacrypt 2024.

SQisign '20



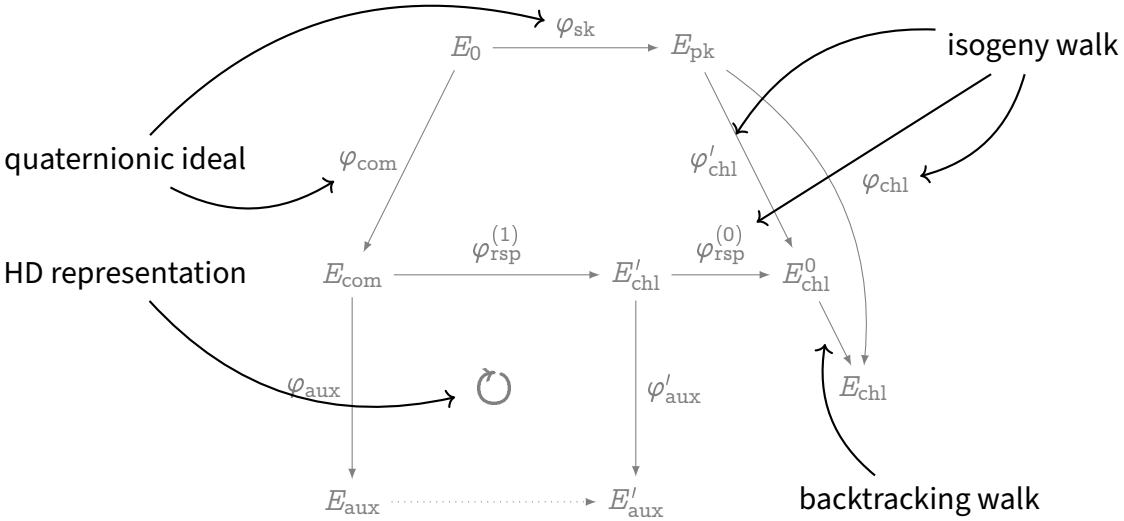
[1] From *"SQIsign2D–West: The Fast, the Small, and the Safer"*, Asiacrypt 2024.

SQisign '20



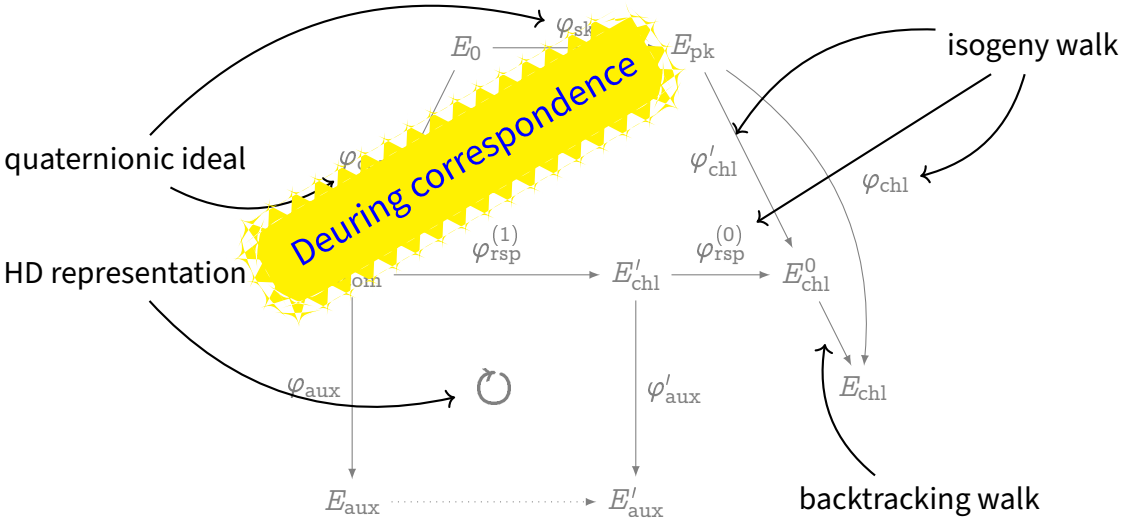
[1] From *"SQIsign2D–West: The Fast, the Small, and the Safer"*, Asiacrypt 2024.

SQisign ’20



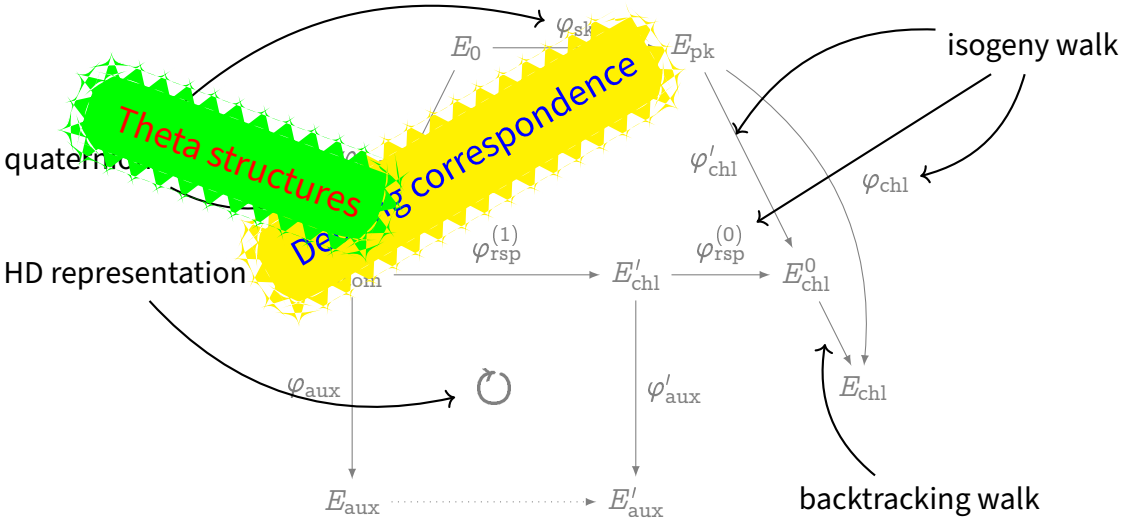
[1] From *“SQIsign2D–West: The Fast, the Small, and the Safer”*, Asiacrypt 2024.

SQisign '20



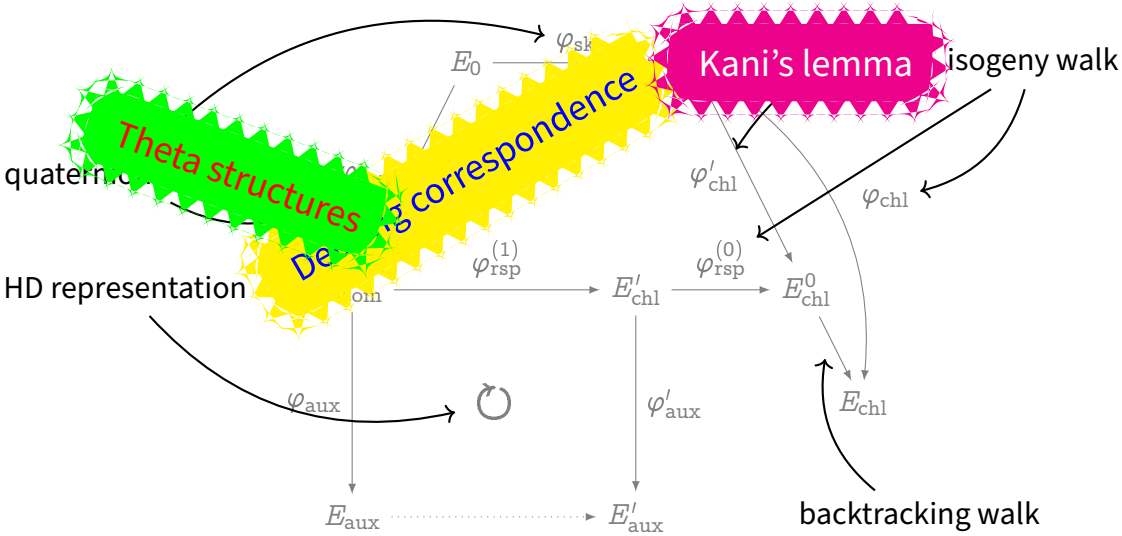
[1] From *"SQIsign2D–West: The Fast, the Small, and the Safer"*, Asiacrypt 2024.

SQisign ’20



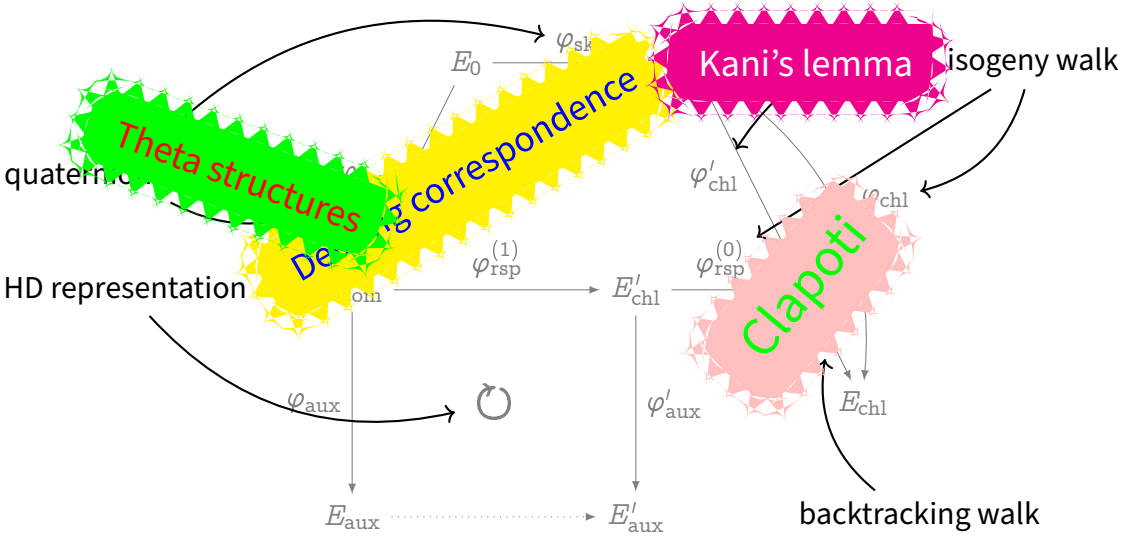
[1]From *“SQIsign2D–West: The Fast, the Small, and the Safer”*, Asiacrypt 2024.

SQisign ’20



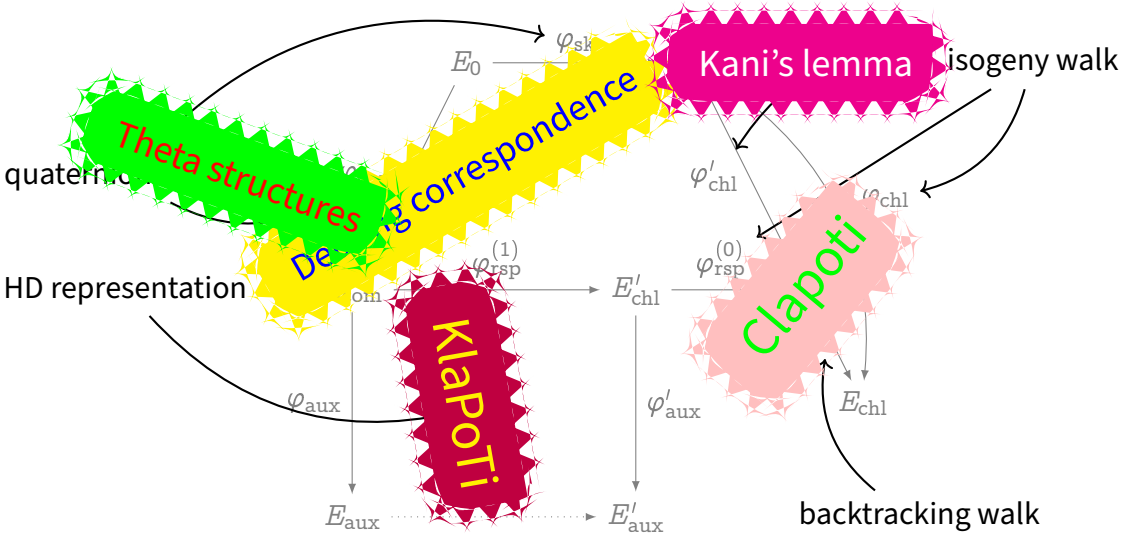
[1] From *“SQIsign2D–West: The Fast, the Small, and the Safer”*, Asiacrypt 2024.

SQisign ’20



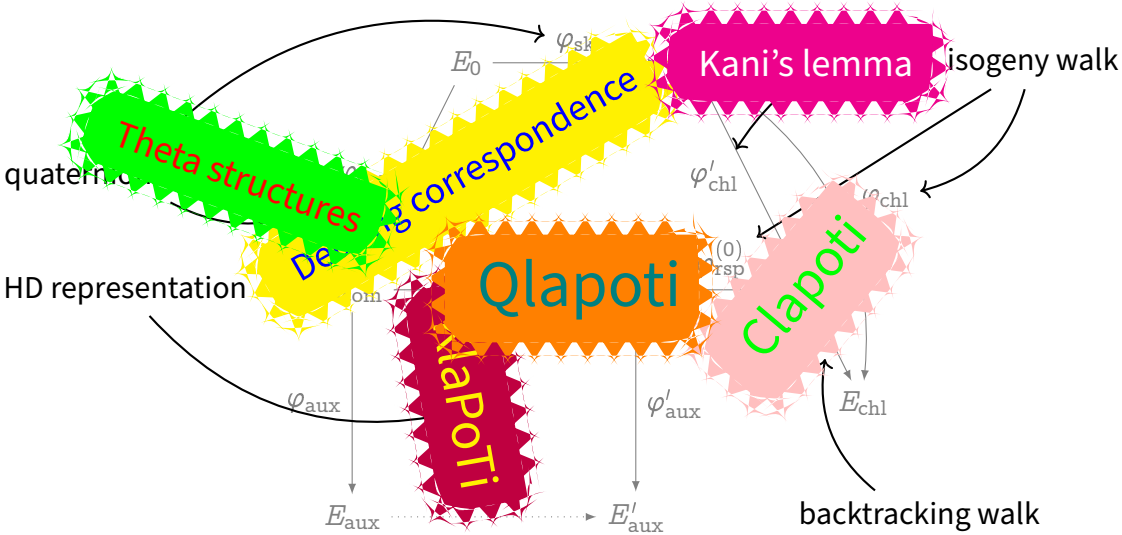
[1] From *“SQIsign2D–West: The Fast, the Small, and the Safer”*, Asiacrypt 2024.

SQisign ’20

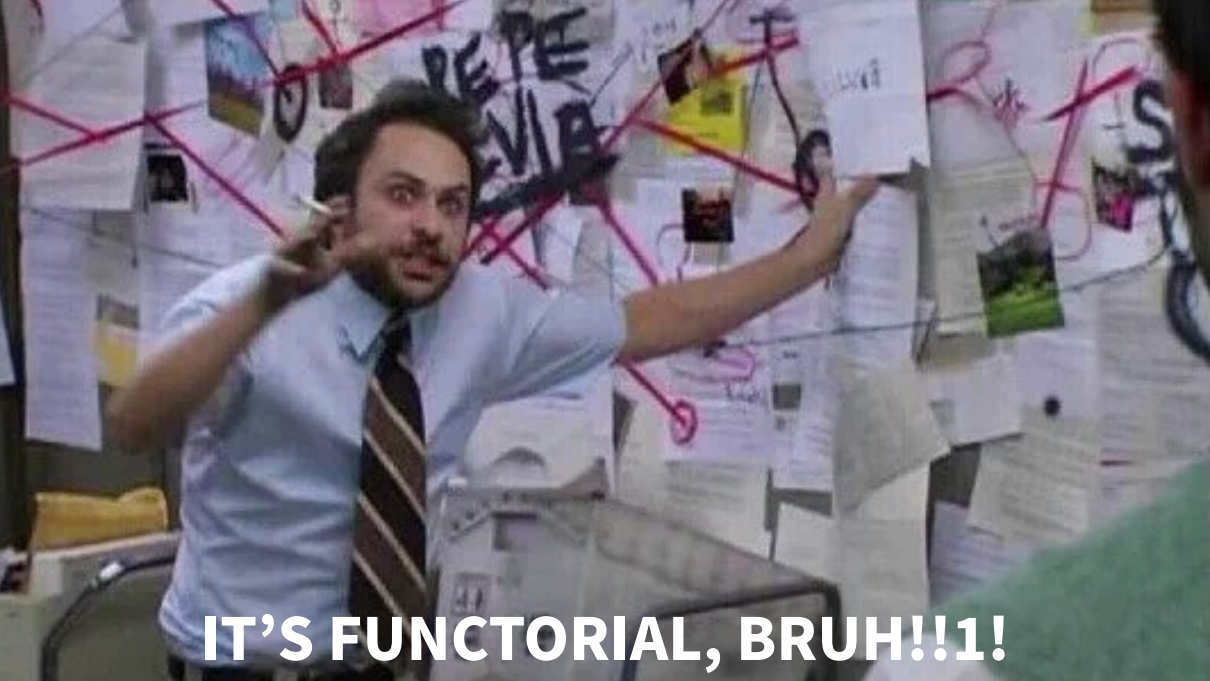


[1] From *“SQIsign2D–West: The Fast, the Small, and the Safer”*, Asiacrypt 2024.

SQisign ’20



[1] From *“SQIsign2D–West: The Fast, the Small, and the Safer”*, Asiacrypt 2024.


IT’S FUNCTORIAL, BRUH!!1!

Too small to fail

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

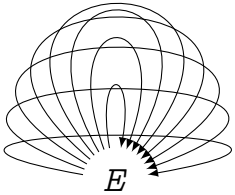
Technical slides ahead

Algebraic geometry: the classical PoV (…–1930's)

$$
\begin{array}{cccccc}
x^2 & +3y^2 & +xy & +10x & -7y & +4 = 0 \\
x^2 & -y^2 & +xy & +9x & -y & -3 = 0 \\
 & -2y^2 & & -3x & -8y & +9 = 0 \\
x^2 & +y^2 & +13xy & +10x & -7y & = 0 \\
x^2 & -5y^2 & +xy & +10x & +11y & +3 = 0 \\
x^2 & +y^2 & +11xy & -8x & +6y & = 0 \\
x^2 & & & & -9y & +4 = 0
\end{array}
$$

- Syzygies
  - Gröbner bases
  - Distinguishers for codes
- Invariants
  - Tensors
  - Exterior algebra
  - Moduli spaces
- …

Algebraic geometry: the modern PoV (1930's–…)



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

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

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

Endomorphism rings

$$\mathbb{Q}(\sqrt{-p})$$

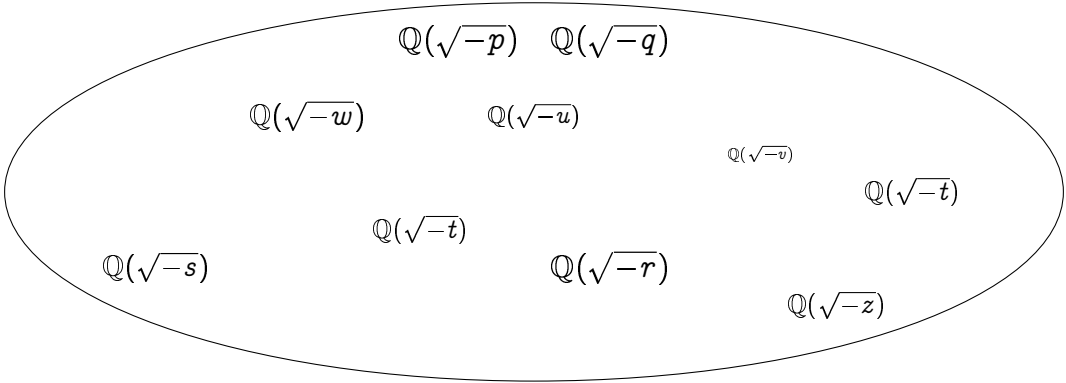
Quadratic imaginary field

Endomorphism rings

$$\mathbb{Q}(\sqrt{-p}) \quad \mathbb{Q}(\sqrt{-q})$$

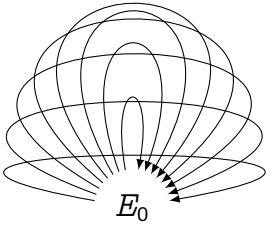
$$i^2 = -p \qquad j^2 = -q \qquad ij = -ji$$

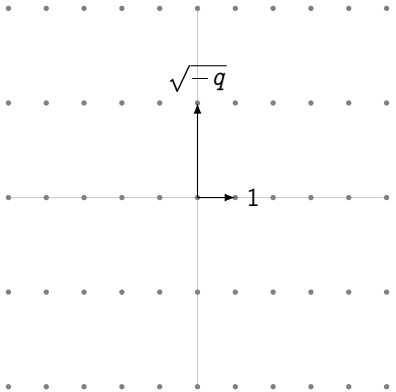
Endomorphism rings



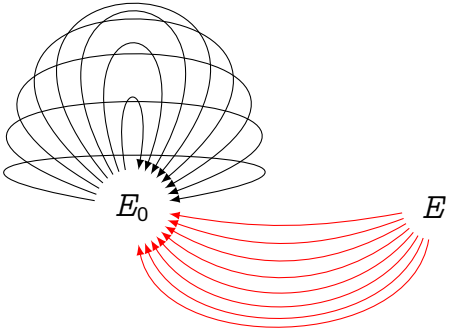
Quaternion algebra

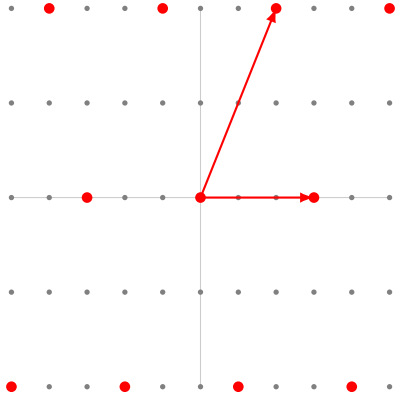
$$i^2 = -p \qquad j^2 = -q \qquad ij = -ji$$



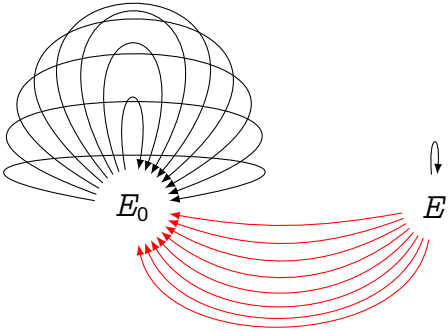


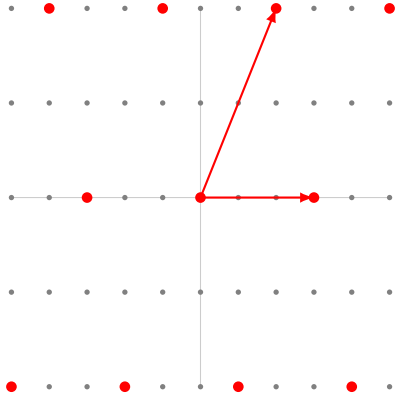
$\mathbb{Z}[\sqrt{-q}]$



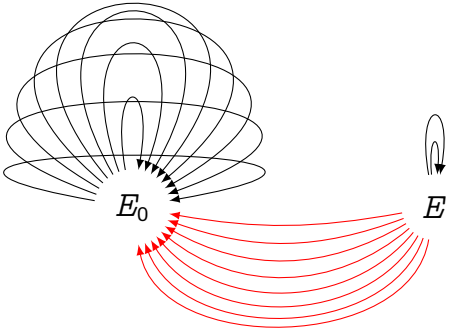


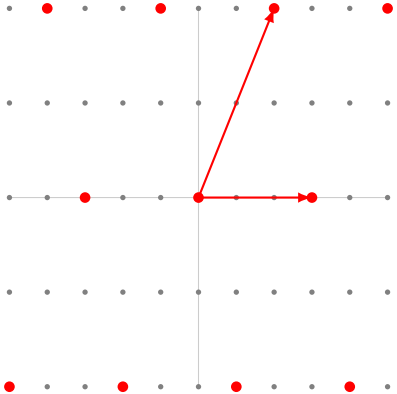
$\mathbb{Z}[\sqrt{-q}]$



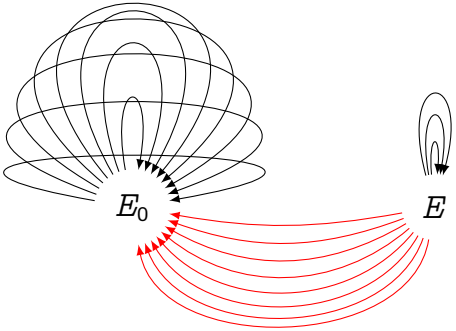


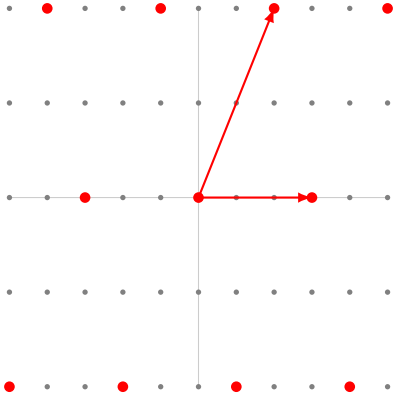
$\mathbb{Z}[\sqrt{-q}]$



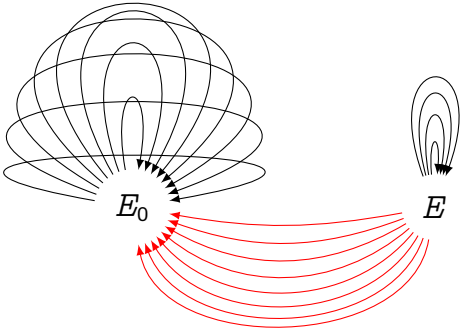


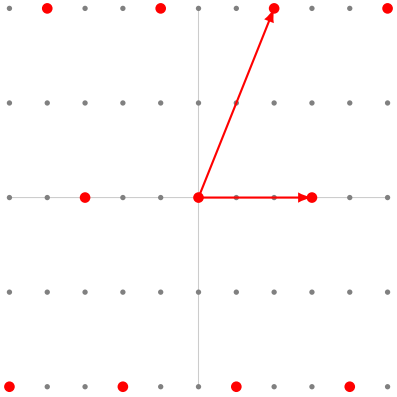
$\mathbb{Z}[\sqrt{-q}]$



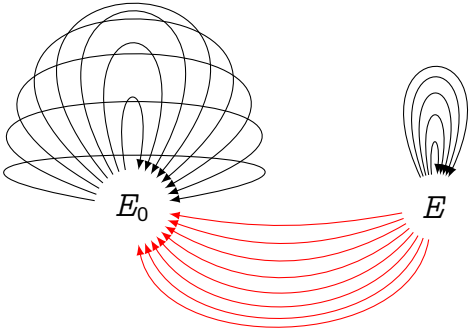


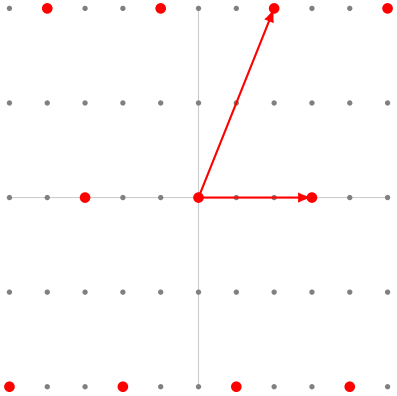
$\mathbb{Z}[\sqrt{-q}]$



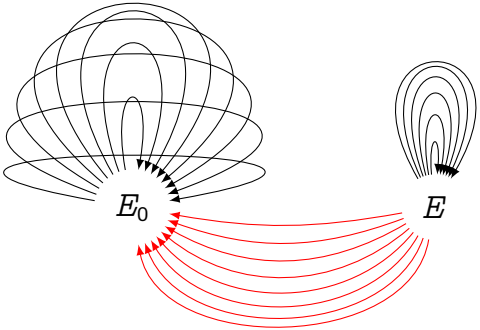


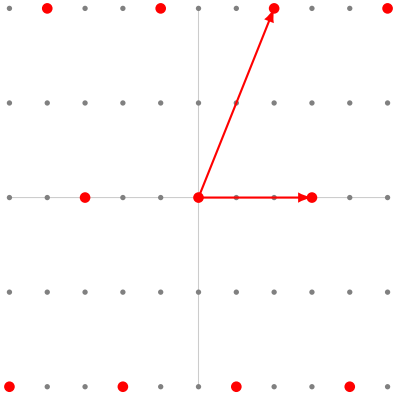
$\mathbb{Z}[\sqrt{-q}]$



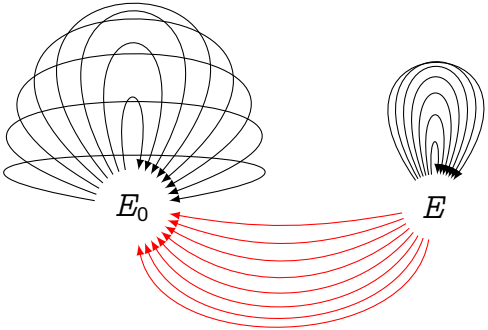


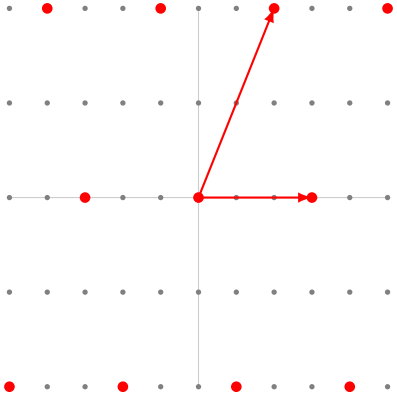
$\mathbb{Z}[\sqrt{-q}]$



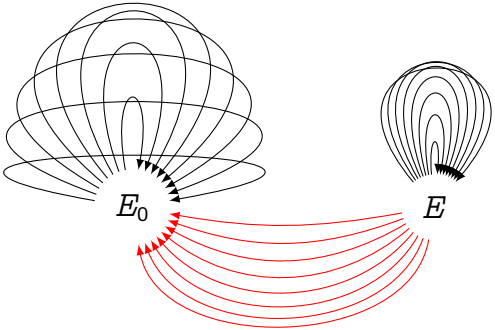


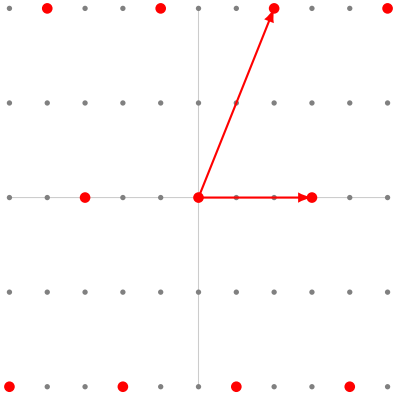
$\mathbb{Z}[\sqrt{-q}]$



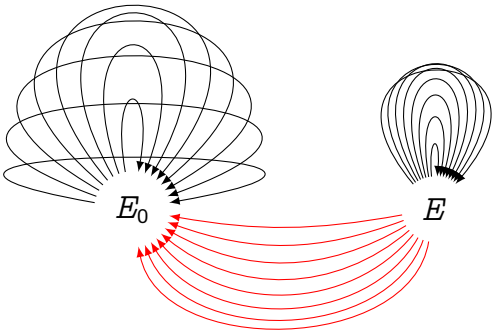


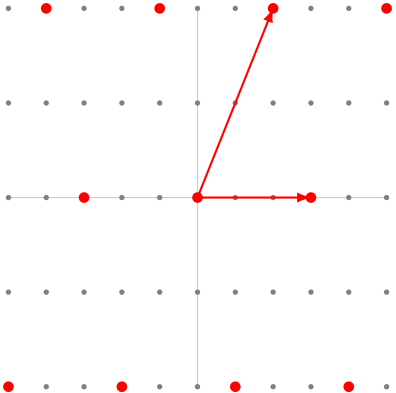
$\mathbb{Z}[\sqrt{-q}]$





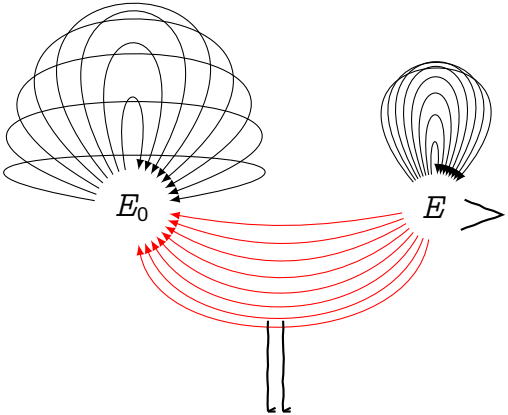
$\mathbb{Z}[\sqrt{-q}]$

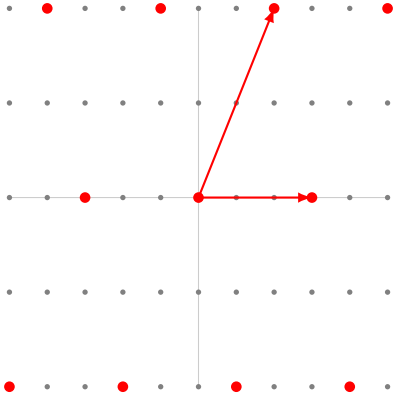




$\mathbb{Z}[\sqrt{-q}]$

Deuring: $\mathrm{End}(E_0)$-lattices are in 1-to-1 correspondence with curves isogenous to E_0.

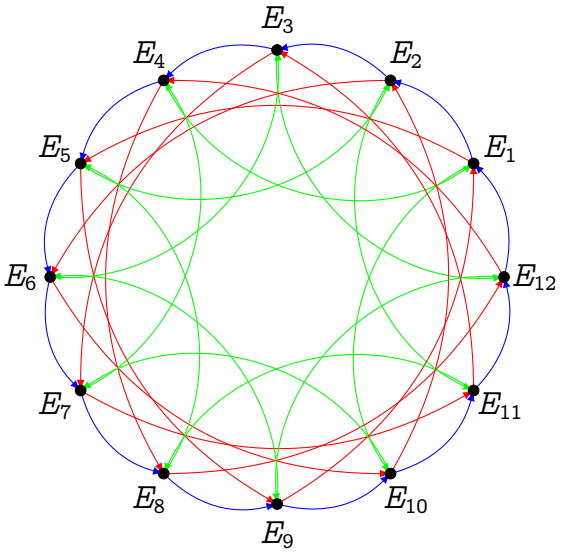




$\mathbb{Z}[\sqrt{-q}]$

Deuring: $\mathrm{End}(E_0)$-lattices are in 1-to-1 correspondence with curves isogenous to E_0.

Class group action (Complex multiplication)



Lattices ↻ Isogenies

↓

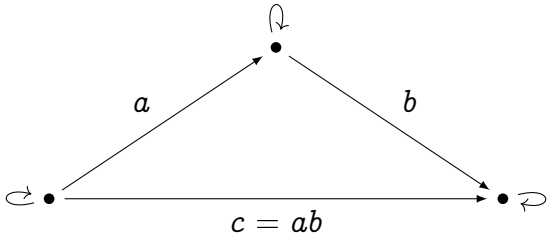
Ideals

↓

Ideal classes ↻ Curves

Grupoid action (Quaternionic multiplication)

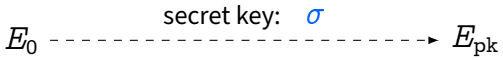
Grupoid = group with “partial” multiplication



(Ideal) Lattices  Curves

Algebra  Geometry

Identification Schemes from Group(oid) Actions



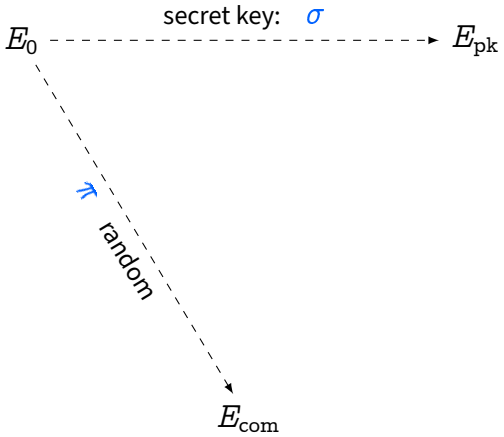
Graph isomorphism: Goldreich, Micali, Widgerson 1992;

Class group action: Couveignes 1997 / Stolbunov 2008;

Quaternionic multiplication: Galbraith, Petit, Silva 2016;

Code equivalence: Biasse, Micheli, Persichetti, Santini 2020;

Identification Schemes from Group(oid) Actions



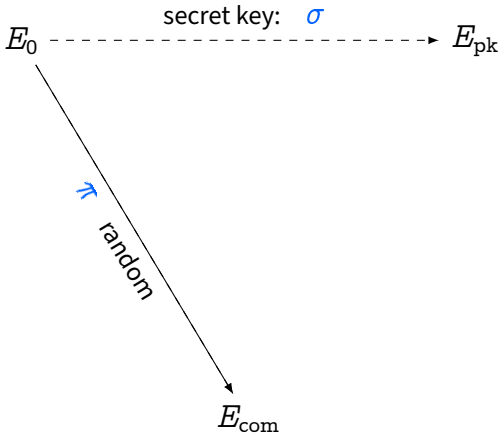
Graph isomorphism: Goldreich, Micali, Widgerson 1992;

Class group action: Couveignes 1997 / Stolbunov 2008;

Quaternionic multiplication: Galbraith, Petit, Silva 2016;

Code equivalence: Biasse, Micheli, Persichetti, Santini 2020;

Identification Schemes from Group(oid) Actions



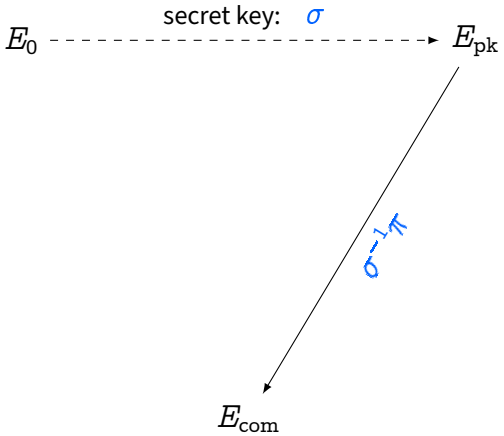
Graph isomorphism: Goldreich, Micali, Widgerson 1992;

Class group action: Couveignes 1997 / Stolbunov 2008;

Quaternionic multiplication: Galbraith, Petit, Silva 2016;

Code equivalence: Biasse, Micheli, Persichetti, Santini 2020;

Identification Schemes from Group(oid) Actions



Graph isomorphism: Goldreich, Micali, Widgerson 1992;

Class group action: Couveignes 1997 / Stolbunov 2008;

Quaternionic multiplication: Galbraith, Petit, Silva 2016;

Code equivalence: Biasse, Micheli, Persichetti, Santini 2020;

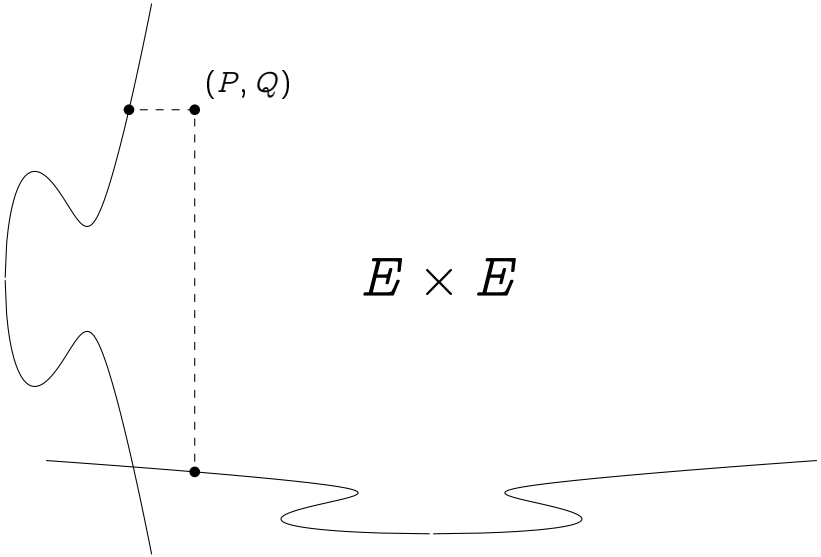
Coming soon

How general (or not) is SQIsign?

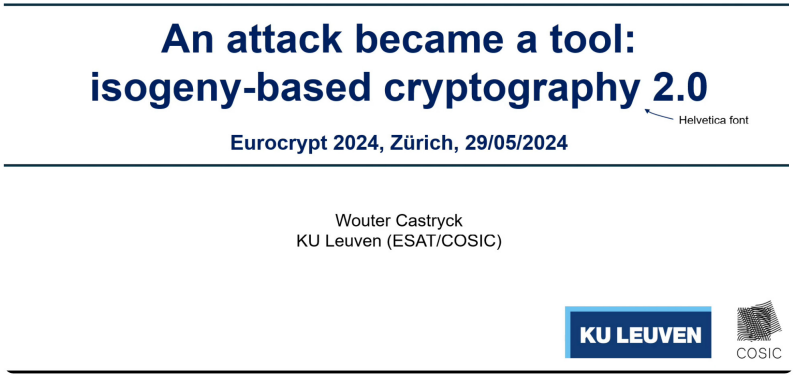
Beyond groupoids: axiomatizing SQIsign

joint work with Basso, Patranabis, Radulescu, Wesolowski

Higher dimensional abelian varieties



HD-mania



youtu.be/CpqjkfuXeoQ

Hermitian Lattices (rank g)

Abelian varieties (dimension g)

FAQ

Aren’t isogenies broken anyway?

As much as:

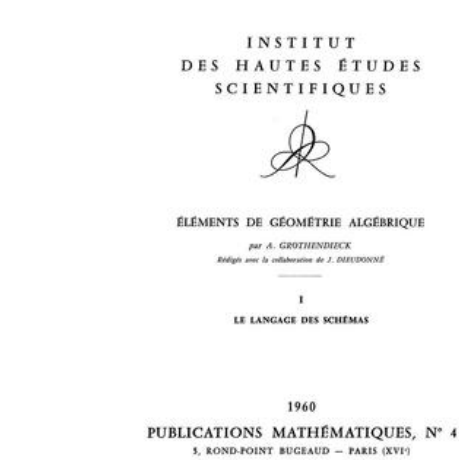
ECC: MOV pairing attack

Lattices: Basically any signature before Fiat–Shamir w aborts

Codes: Signatures, Syzygy distinguishers

Multivariate: HFE, Rainbow

Do I need to study the EGA to understand isogenies?



INSTITUT
DES HAUTES ÉTUDES
SCIENTIFIQUES

ÉLÉMENTS DE GÉOMÉTRIE ALGÉBRIQUE

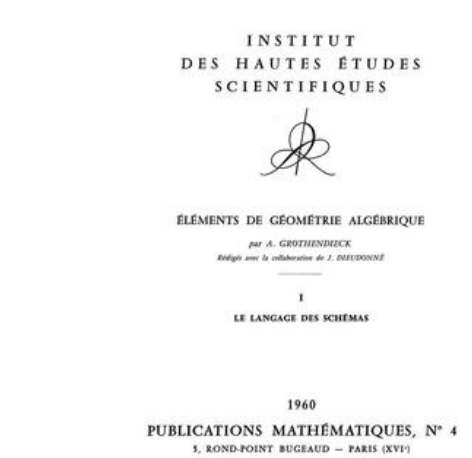
par A. GROTHENDIECK
Rédigés avec la collaboration de J. DIEUDONNÉ

I
LE LANGAGE DES SCHÉMAS

1960
PUBLICATIONS MATHÉMATIQUES, N° 4
5, ROND-POINT BUGEAUD — PARIS (XVI^e)

No.

Do I need to study the EGA to understand isogenies?



INSTITUT
DES HAUTES ÉTUDES
SCIENTIFIQUES

ÉLÉMENTS DE GÉOMÉTRIE ALGÉBRIQUE

par A. GROTHENDIECK
Rédigés avec la collaboration de J. DIEUDONNÉ

I
LE LANGAGE DES SCHÉMAS

1960
PUBLICATIONS MATHÉMATIQUES, N° 4
5, ROND-POINT BUGEAUD — PARIS (XVI^e)

No. But it won't hurt you.

When are you going to write a book?

When are you going to write a book?

Next question!

Community

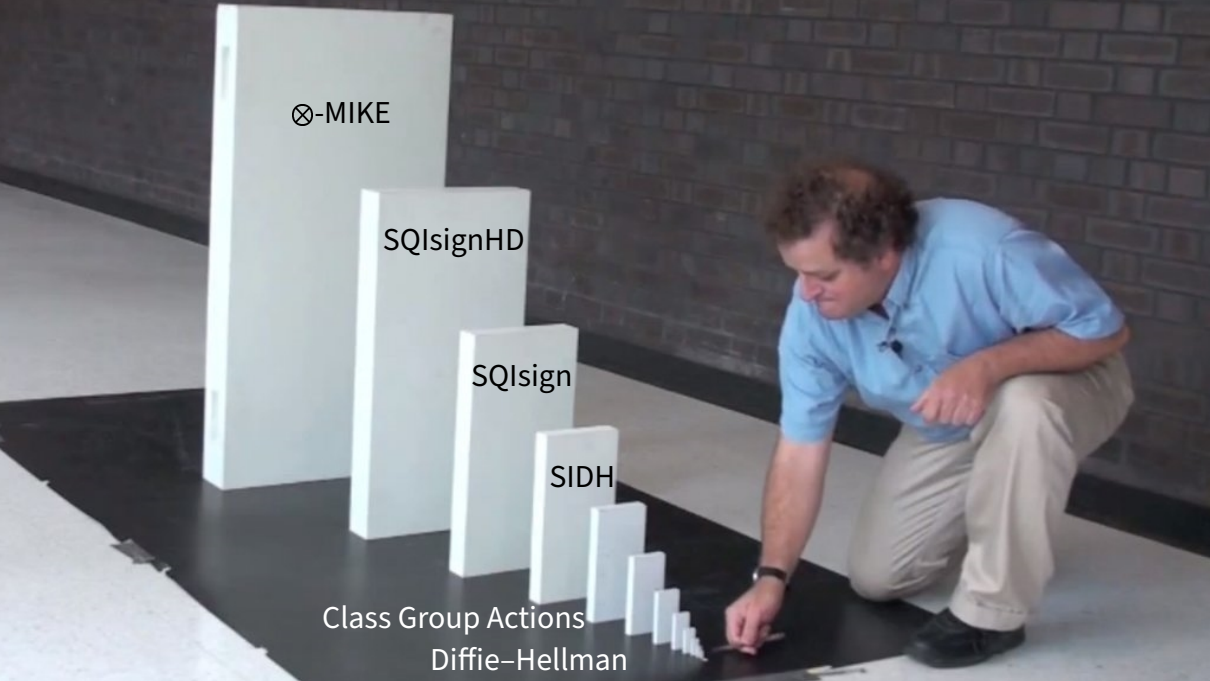
THE

isogeny club

https://isogeny.club

Famous last words

Algebra  Geometry


⊗-MIKE
SQIsignHD
SQIsign
SIDH
Class Group Actions
Diffie–Hellman

Thank you

https://defeo.lu/

@luca_defeo@ioc.exchange

@bsky.defeo.lu