Advances and challenges in isogeny-based protocols

Monika Trimoska

PQCSA workshop on Post-Quantum Cryptographic Protocols
Eurocrypt 2026 affiliated event

Rome, May 9, 2026

TU/e

PQCSA

Elliptic curves

What is an elliptic curve?

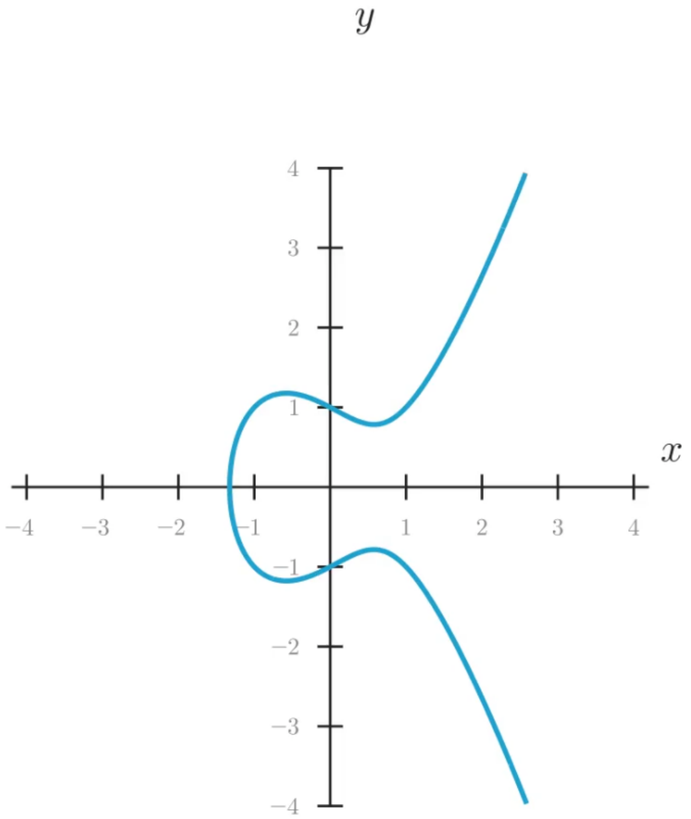
An elliptic curve is an algebraic curve that admits an affine equation of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

(general form of a Weierstrass curve)

with $a_i \in k$, where k is the field where the point is defined.

Example. $y^2 = x^3 - x + 1$



→ A point on E means that the point (x, y) satisfies the curve equation.

Elliptic curves over $\mathbb{F}_q$

In cryptography, we use elliptic curves over finite fields $\mathbb{F}_q$, $q = p^k$ (but we draw the figures over $\mathbb{R}$ because it's nicer).

→ We denote by $E(k)$ the set of k-rational points on E.

↳ defined over k

Hasse bound

$$\#E(\mathbb{F}_q) \in [q + 1 - 2\sqrt{(q)}, q + 1 + 2\sqrt{(q)}]$$

Elliptic curves in cryptography

- Short Weierstrass form

$$y^2 = x^3 + c_4 x + c_6$$

- The set of points on E with the addition law form a group.

- The group law is constructed geometrically.

The ECDLP problem

Input: Two points $P, Q \in E(\mathbb{F}_q)$.
Question: Find an integer x such that $xP = Q$.

Elliptic curves in cryptography

A curve is

- non-singular (or smooth) if it does not have a singular point.

  Jacobi criterion: a point on E is singular if (x, y) also satisfies the two partial derivatives $2y + a_1x + a_3 = 0$ and $a_1y = 3x^2 + 2a_2x + a_4$.

- supersingular (also non-singular) if and only if $\#E(\mathbb{F}_p) = p + 1$ (for $p > 3$).

  equivalently: iff $E[p] = \{\infty\}$

  $E[n] = \{P \in E(\overline{\mathbb{F}_p}) \mid nP = \infty\}$ (the n-torsion group)

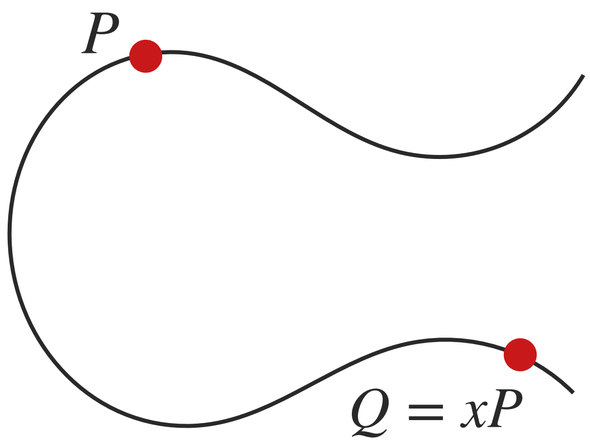
Supersingular curves and cyclic groups

- $E(\mathbb{F}_p) \cong \mathbb{Z}/(p+1)$
- $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1) \times \mathbb{Z}/(p+1)$

Isogenies

A familiar isogeny

The multiplication-by-d map

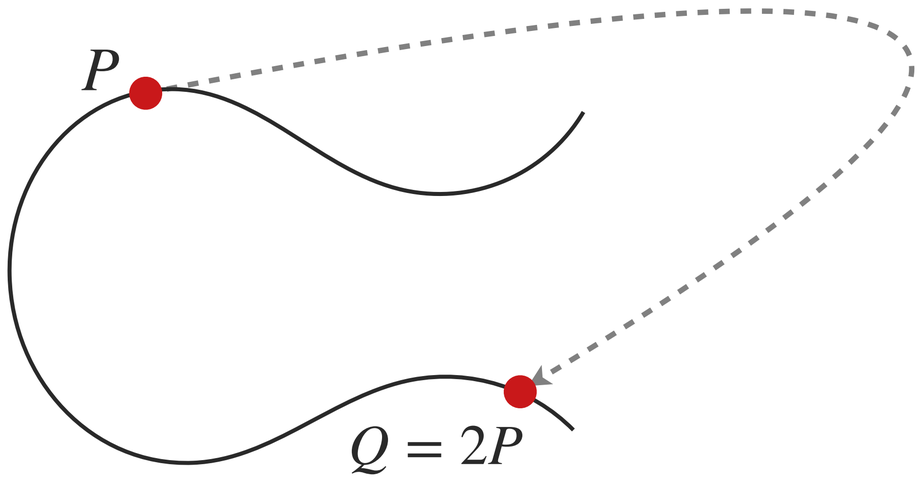


A familiar isogeny

The multiplication-by-d map

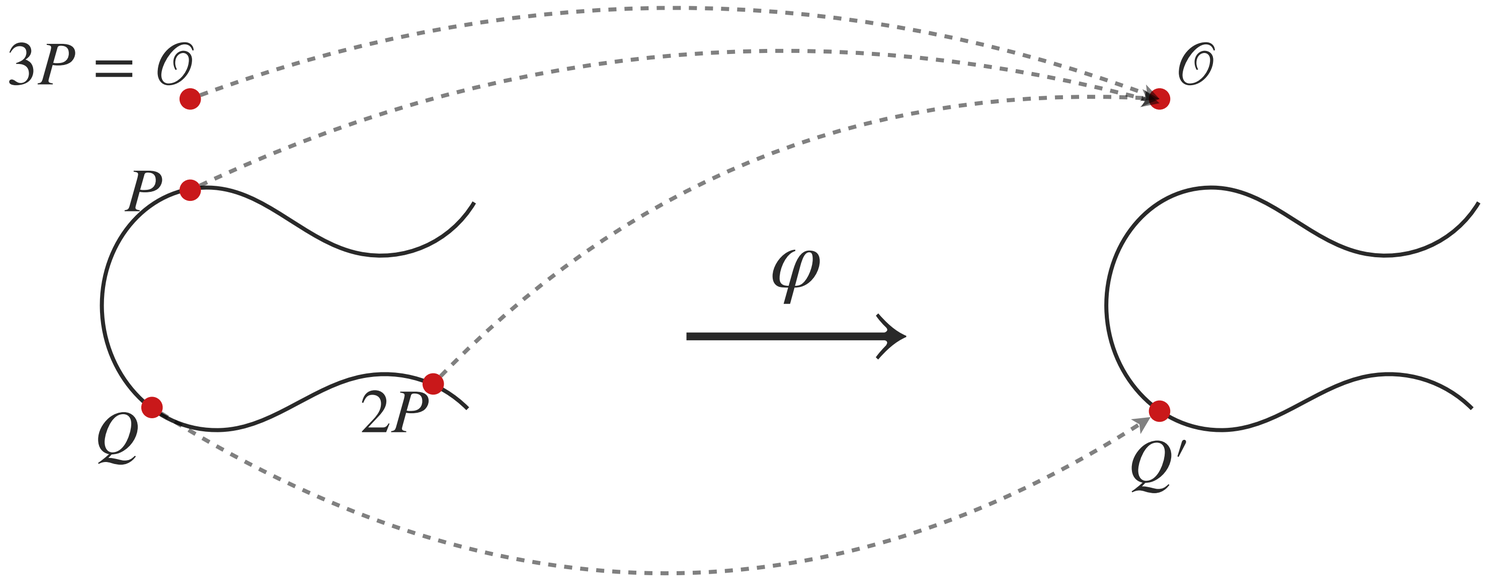
$$(x, y) \mapsto (\lambda^2 - 2x, \lambda x + y),$$

$$\lambda = \frac{3x^2 + a}{2y}$$



Isogenies

- Isogenies: maps between elliptic curves



$$(x, y) \mapsto \left(\frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{x^3 - 6x^2 - 14x + 35}{(x-2)^3} \cdot y\right)$$

Isogenies

An isogeny φ of elliptic curves is a non-zero map $E \to E'$ that is

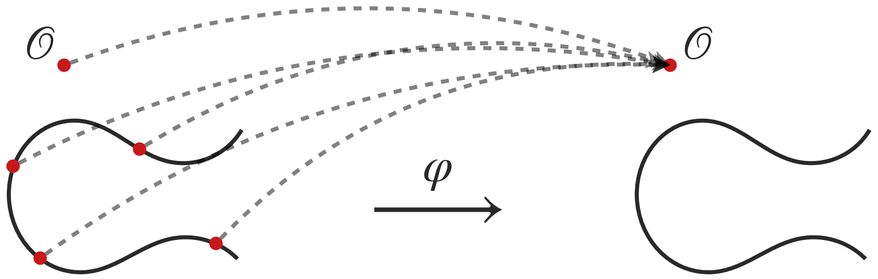
- given by rational functions
- that is a group homomorphism

$$\varphi(P+Q) = \varphi(P) + \varphi(Q)$$

$$\frac{f(x,y)}{g(x,y)}, \text{ where } f, g \text{ are polynomials}$$

→ An isogeny is uniquely defined by its kernel: $\{P \in E \mid \varphi(P) = \mathcal{O}_{E'}\}$.

→ The degree of a (separable) isogeny is the size of its kernel.



Isogenies - a toy example

Example.

$$(x, y) \mapsto \left(\frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{x^3 - 6x^2 - 14x + 35}{(x-2)^3} \cdot y\right)$$

defines a degree-3 isogeny of the elliptic curves

$$\{y^2 = x^3 + x\} \to \{y^2 = x^3 - 3x + 3\}$$

over $\mathbb{F}_{71}$. Its kernel is $\{(2,9), (2,-9), \mathcal{O}\}$.

ℓ-isogeny:

- $x \to \frac{f(x)}{g(x)}$, with $\deg(f) = \ell, \deg(g) = \ell - 1$
- $y \to \ldots$

Isogeny representations

Computing isogenies

*We consider only supersingular curves from now on.

→ **Goal**: Compute an ℓ-isogeny from E.

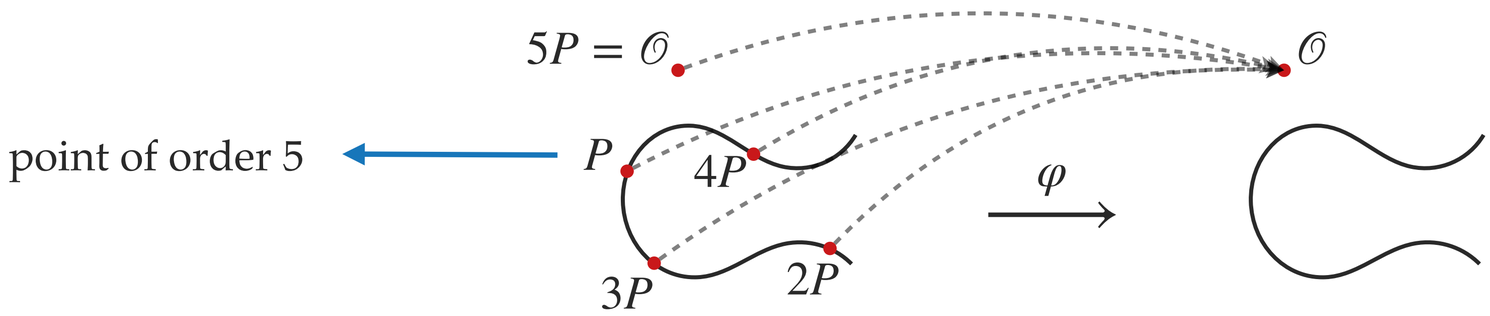
Find a point P on E of order ℓ

↳ Take the cyclic group generated by P

↳ Obtain a subgroup of order ℓ

↳ Obtain a kernel of an ℓ-isogeny

↳ Compute an ℓ-isogeny



Vélu's formulas

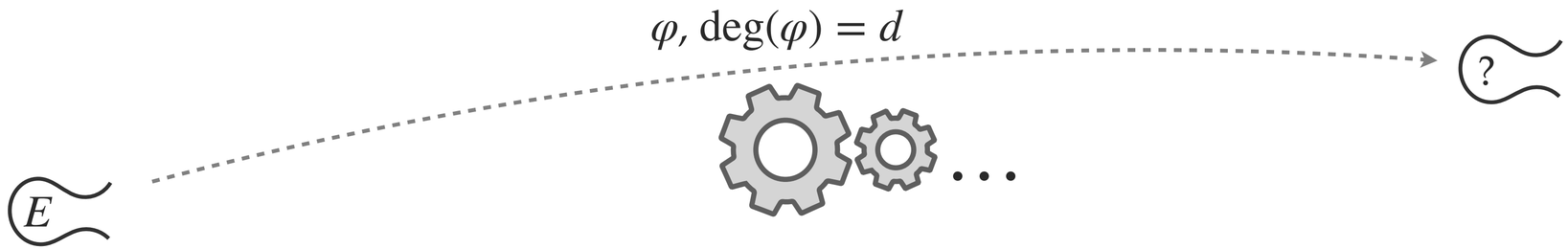
→ For any finite subgroup G of E, there exists a unique (up to isomorphism) separable isogeny $\varphi_G : E \to E'$ with kernel G.

Vélu '71

- Formulas for computing E' and evaluating φ_G at a point.
- Complexity: $\Theta(\#G)$ → only suitable for small degrees.

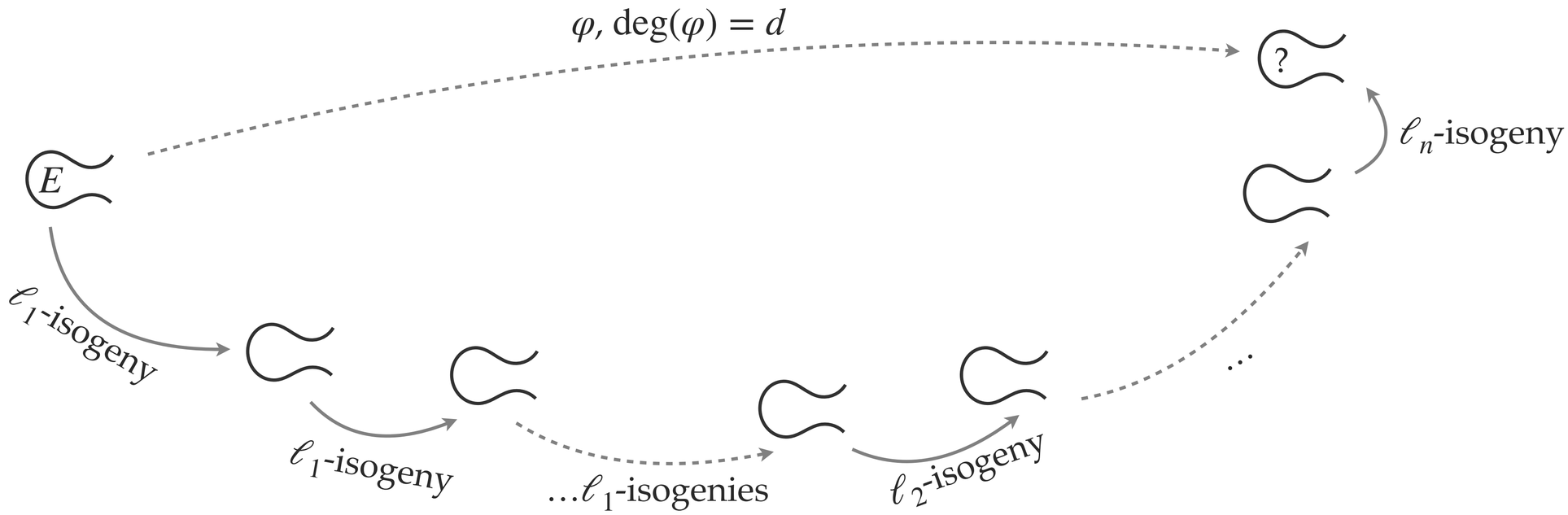
Composing isogenies

Goal: Compute a d-isogeny from E.



Composing isogenies

Goal: Compute a d-isogeny from E, with d a smooth integer ($d = \ell_1^{e_1} \cdot \ell_2^{e_2} \cdots \ell_n^{e_n}$).



Isogenies in SageMath

Computing isogenies

```
p=139
A=0
E=EllipticCurve(GF(p), [0, A, 0, 1, 0])
assert E.order()==p+1 #check that it is a supersingular curve
print("We can compute isogenies of the following degrees:", factor((p+1)/4))
P=E.random_point()
while P.order().is_prime() == False:
    P=E.random_point()
print("We will compute an isogeny of degree", P.order())
print(E.montgomery_model()) #needs Sage 10.3
phi=E.isogeny(P)
print(phi)
E2=phi.codomain()
print(E2.montgomery_model()) #needs Sage 10.3
```

✓ 0.0s

```
We can compute isogenies of the following degrees: 5 * 7
We will compute an isogeny of degree 5
Elliptic Curve defined by y^2 = x^3 + x over Finite Field of size 139
Isogeny of degree 5 from Elliptic Curve defined by y^2 = x^3 + x over Finite Field of size 139 to Elliptic Curve defined by y^2 = x^3 + 72*x + 30 over Finite Field of size 139
Elliptic Curve defined by y^2 = x^3 + 126*x^2 + x over Finite Field of size 139
```

Efficient isogeny representations

- The kernel representation (for smooth-degree isogenies)
- The HD representation
- The ideal representation (requires knowledge of the endomorphism ring)
- Etc.

Hard problems in isogeny-based crypto

Endomorphism rings

Dual isogeny

- For isogeny $\varphi : E \to E'$ there exists a unique dual isogeny $\hat{\varphi} : E' \to E$.
- The composition $\hat{\varphi} \circ \varphi$ is the multiplication-by-d map on E and $\varphi \circ \hat{\varphi}$ the multiplication-by-d map on E', where $d = \deg(\varphi) = \deg(\hat{\varphi})$.

The multiplication-by-d map

- The multiplication-by-d map $[d] : E \to E$ is a degree-d^2 isogeny from E to E.

  → It is an endomorphism.

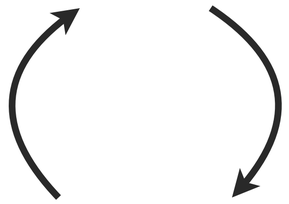
$\mathrm{End}(E)$

- An endomorphism is an isogeny from a curve E to itself.
- The set of endomorphisms forms a ring $\mathrm{End}(E)$ under $+$ and $\circ$.

Some hard problems and reductions

The isogeny path problem

Input: Two supersingular curves E and E'.
Question: Find an isogeny φ from E to E'.



The EndRing problem

Input: A supersingular curve E.
Question: Find a basis of $\mathrm{End}(E)$.

Random Prime-degree Isogenies problem

Input: A supersingular curve E and a positive integer n.
Question: generate an isogeny φ from E to E' of degree n, where E' is some other curve.

Isogeny graphs

- Vertices are $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves.
- Edges are prime-degree isogenies between them.

How hard is isogeny path finding ?

Generic attacks are all in $\tilde{\mathcal{O}}(N^{\frac{1}{2}})$, where N is the size of the search space.

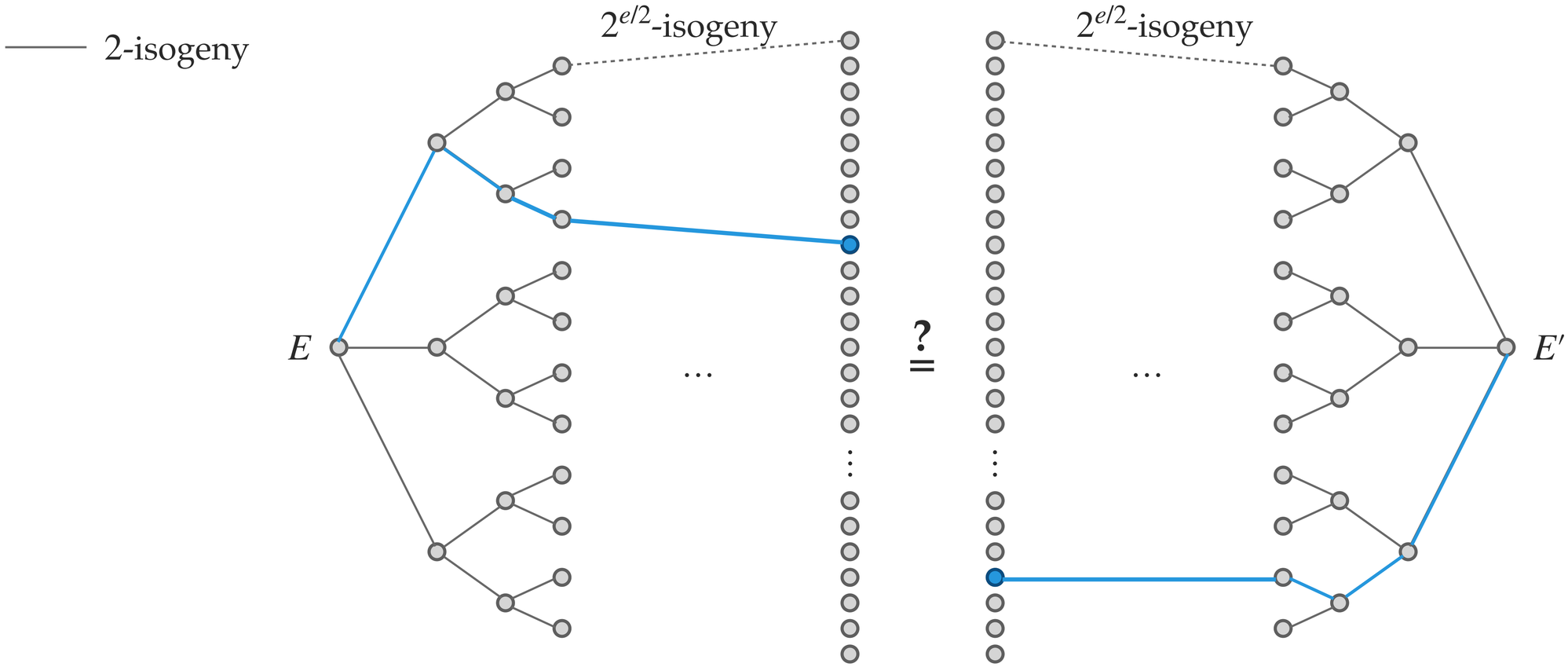
- $\#E(\mathbb{F}_q)$ (for ECDLP)
- Nb. of isogenies from E of the fixed degree (for fixed-degree isogeny path finding)
- Nb. of isogenies from E to the (expected) diameter of the isogeny graph

Relevant algorithms:

- Meet-in-the-middle
- Parallel Collision Search (vOW)
- Delfs–Galbraith

Meet-in-the-middle

Example. **Goal**: Find a 2^e-isogeny from E to E'.



Isogeny-based schemes

Overview of protocols (non-exhaustive)

Building blocks

(group actions)

CSIDH

generalization

(qt-)PEGASIS

PKE

(Q)FESTA

LIT-SiGamal

POKE

Signatures

SQIsign

PRISM

Advanced primitives

DeuringVRF

Tanuki/Wombat

Blind signatures

PQarrots

Threshold: PKE, signature, DKG

SQIsign

The EndRing problem

Input: A supersingular curve E.
Question: Find a basis of $\mathrm{End}(E)$.

TABLE 5. SQISIGN performance in 10^6 CPU cycles on an Intel Core i7-13700K CPU. Results are the median of 1,000 benchmark runs.

Parameter set	`KeyGen`	`Sign`	`Verify`
Reference implementation (with default GMP installation)			
NIST-I	71.8	163.1	11.3
NIST-III	188.2	427.0	30.4
NIST-V	325.4	751.8	61.9
Reference implementation (with GMP `--disable-assembly`)			
NIST-I	84.4	203.1	11.3
NIST-III	227.9	548.9	30.5
NIST-V	402.6	1021.0	62.2
Assembly-optimized implementation for Intel Broadwell or later			
NIST-I	43.3	101.6	5.1
NIST-III	134.0	309.2	18.6
NIST-V	212.0	507.5	35.7

TABLE 4. SQISIGN key and signature sizes in bytes for each security level.

Parameter set	Public key	Secret key	Signature
NIST-I	65	353	148
NIST-III	97	529	224
NIST-V	129	701	292

PRISM

Random Prime-degree Isogenies

Input: A supersingular curve E and a positive integer n.
Question: generate an isogeny φ from E to E' of degree n, where E' is some other curve.

Table 3. Signature sizes for the signature scheme

Protocol	PRISM-sig	salt-PRISM
Sig. size (bits)	12λ	$6\lambda + 4a$

Table 5. Run time comparison in millions of clock cycles

		Level I	Level III	Level V
PRISM	KeyGen	31.2	123.4	166.9
	Sign	50.3	172.1	260.0
	Verify	9.4	23.0	42.2

Overview of protocols (non-exhaustive)

Building blocks

(group actions)

CSIDH

generalization

(qt-)PEGASIS

PKE

(Q)FESTA

LIT-SiGamal

POKE

Signatures

SQIsign

PRISM

Advanced primitives

DeuringVRF

Tanuki/Wombat

Blind signatures

PQarrots

Threshold: PKE, signature, DKG

Challenges

Challenges

- Improving efficiency (of isogeny representations)
  - → Even (no adjectives) implementation can be a challenge for higher dimensional isogenies
- Provable security (sometimes including adapting the security models)
- Protection against physical attacks

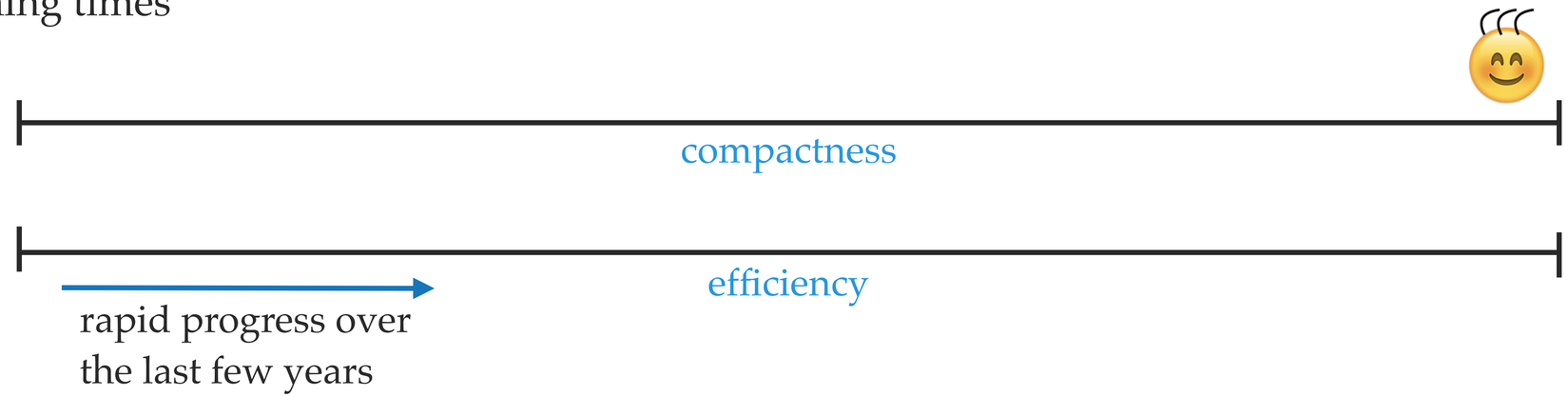
See also: Hot Topics and Open Problems in Post-Quantum Cryptography by the PQCSA project

	Hot topics	Open problems	More attention
Families of cryptosystems			
Isogeny-based cryptography	8	3	
MPC in the head	8		
Lattice-based cryptography	5		
Diversity of families & problems	3	4	3

→ Survey: 54 participants (65% academic researchers, 35% industry experts)

Recap

- Diversifying the post-quantum landscape
  - → the only post-quantum commutative group action
  - → perfect for applications where small sizes is a strong requirement, while it is possible to handle longer running times



- Join us!
  - → Design - provable security
  - → Implementation
  - → Physical security
  - → Quantum analysis

- Seminar series: The isogeny club https://isogeny.club/