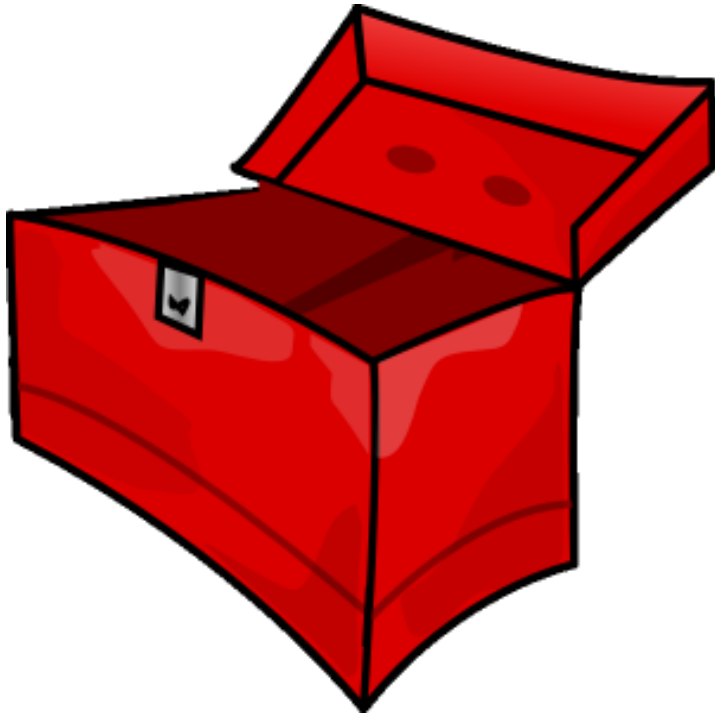


ECC is the best of both worlds



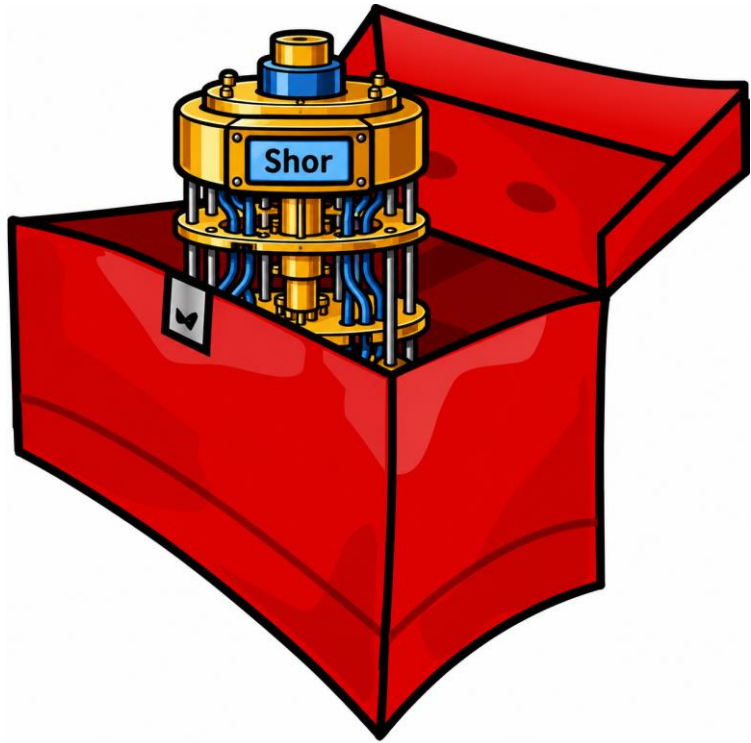
attacker's toolbox

vs.



our toolbox

Quantum computers change the problem



attacker's toolbox



our toolbox

From objects to maps

Yesterday: elliptic curves and their groups of points.

Today's talk: maps between elliptic curves.

$$\varphi: E \longrightarrow E'$$

$$\varphi(P + Q) = \varphi(P) + \varphi(Q), \quad \varphi(O) = O'$$

The promise of isogeny-based cryptography

Craig Costello

Workshop on Elliptic Curves

University of Sydney, 2 October 2026

Shor's algorithm breaks RSA and ECC

Factoring and elliptic-curve discrete logarithms admit quantum polynomial-time algorithms

$$Q = [x]P \dots \text{find } x$$

Superposition

$$|a, b\rangle |0\rangle \mapsto |a, b\rangle |[a]P + [b]Q\rangle$$

Evaluate many input pairs

2026 projections for 256-bit ECDLP

Google

$\leq 1,450$ logical qubits

≤ 70 million Toffoli gates

IonQ

1,457 logical qubits

39 million Toffoli gates

PQC standards: ML-KEM and ML-DSA use lattice problems

ML-KEM: key establishment. ML-DSA: digital signatures. NIST standards since 2024.

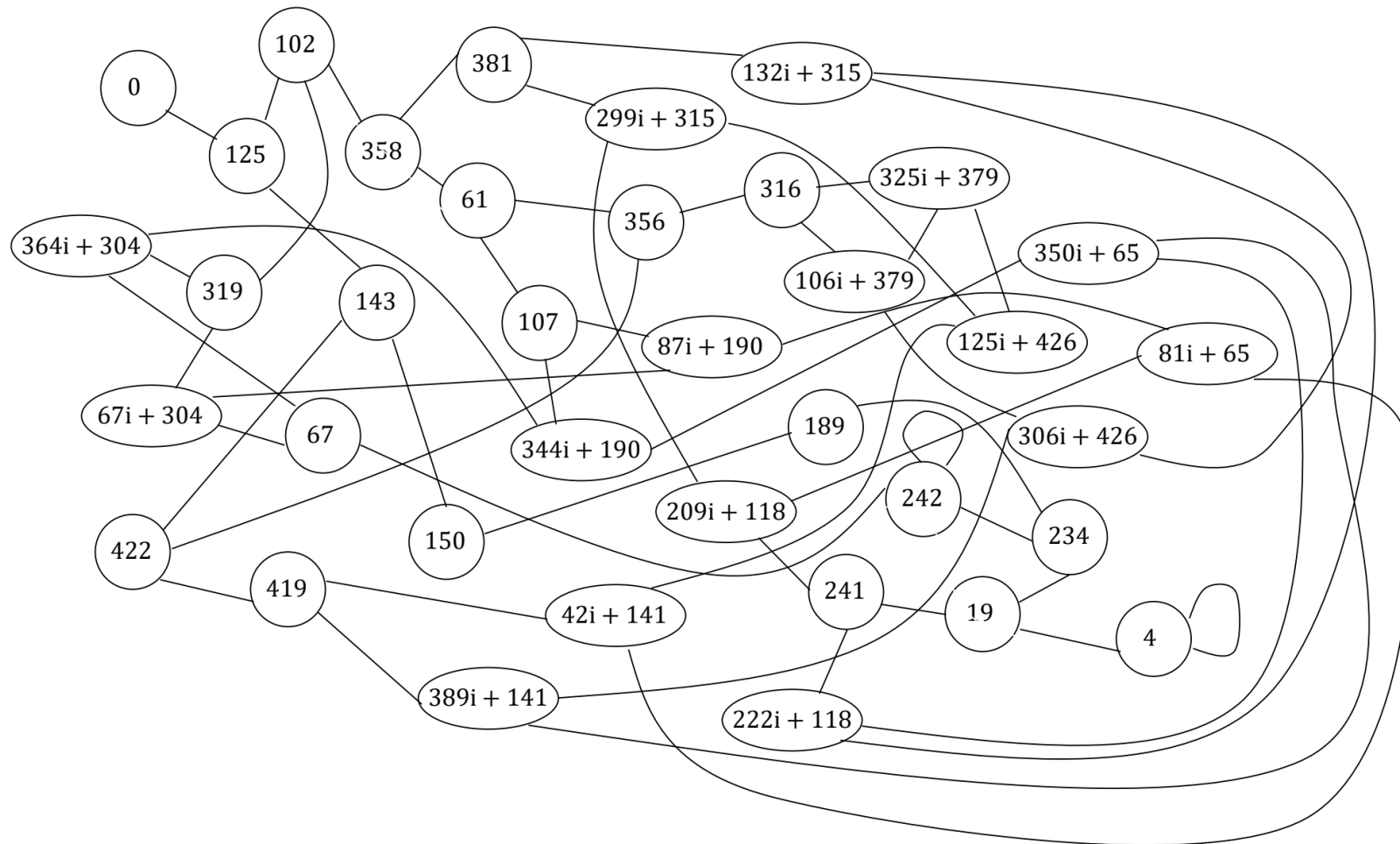
Learning with errors

$$b = As + e$$

$$\begin{array}{c} \text{A public} \\ \begin{bmatrix} 2 & 5 & 1 & 3 \\ 1 & 3 & 4 & 2 \\ 4 & 1 & 2 & 5 \\ 3 & 2 & 5 & 1 \end{bmatrix} \end{array} \times \begin{array}{c} \text{s secret} \\ \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} \end{array} + \begin{array}{c} \text{e small} \\ \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} \end{array} \equiv \begin{array}{c} \text{b public} \\ \begin{bmatrix} 2 \\ 0 \\ 7 \\ 12 \end{bmatrix} \end{array} \pmod{13}$$

Given A and b, recover s from noisy modular equations.

The supersingular 2-isogeny graph



37

curves, up to
isomorphism

$p = 431$

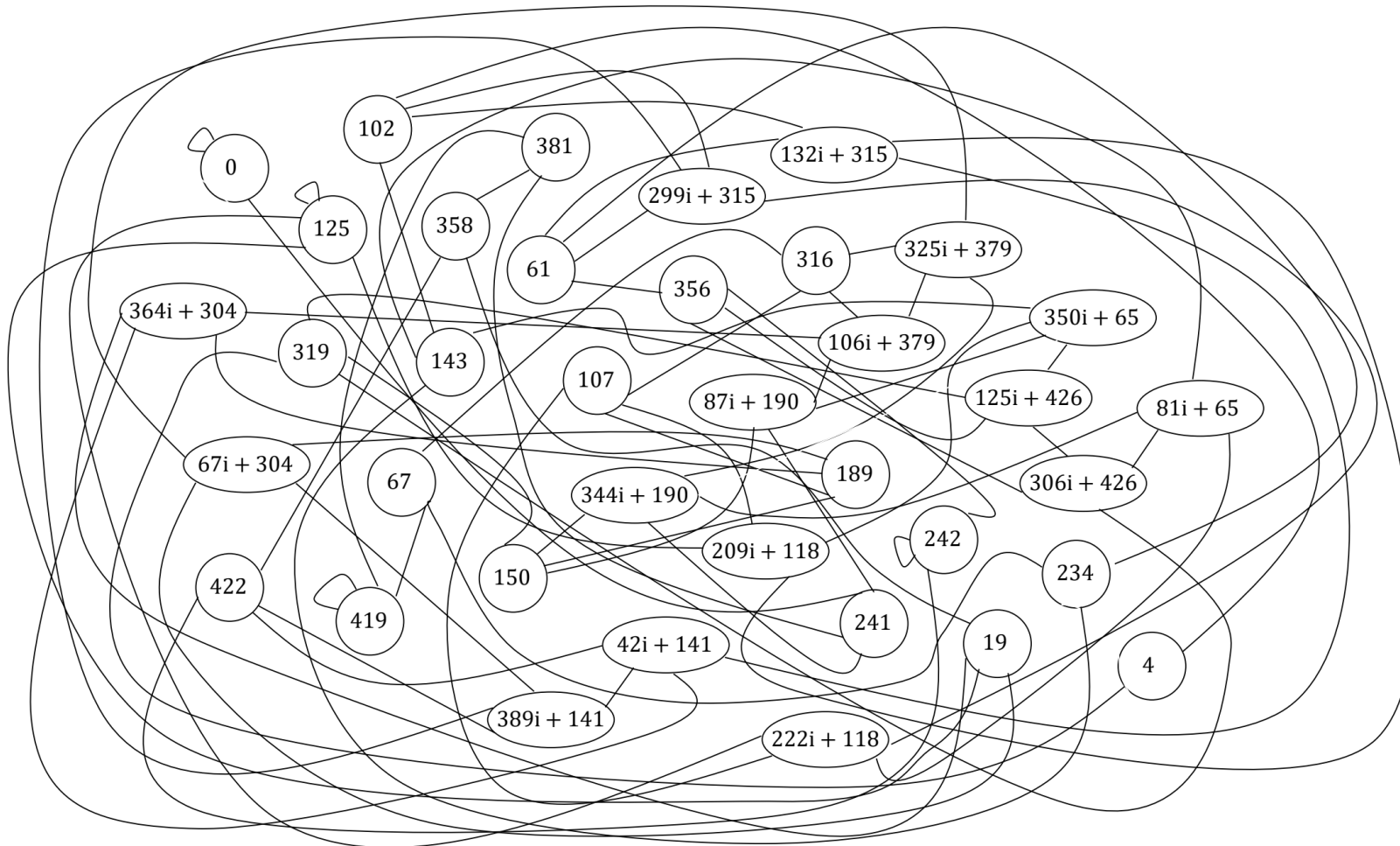
$j \in \mathbb{F}_{p^2}$

**3 outgoing choices
at each vertex**

Loops and multiplicities count.
Drawing suppresses weights.

The supersingular 3-isogeny graph

The same curves, with four outgoing kernel choices at each vertex



Ramanujan

$$|\lambda| \leq 2\sqrt{\ell}$$

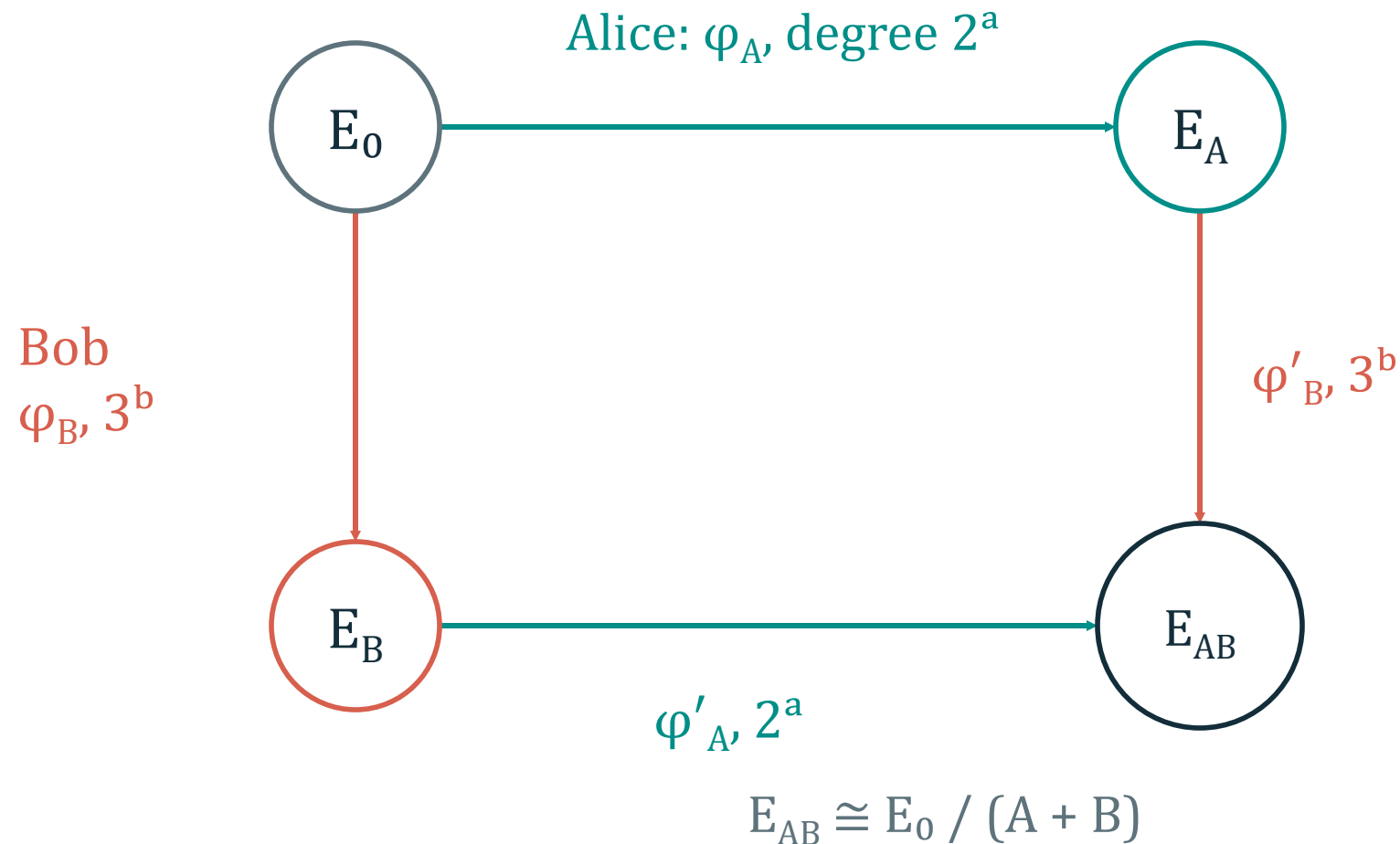
An expander

$O(\log p)$ steps
to mix

Easy to walk.
Hard to find a path.

SIDH: the square behind SIKE

Historical key exchange, broken in 2022



Public keys also carry transported torsion bases

Alice sends

$E_A, \varphi_A(P_B), \varphi_A(Q_B)$

Shared secret

$j(E_{AB})$

Why SIKE attracted attention

NIST category 1 parameters, before the 2022 break

330

byte public key

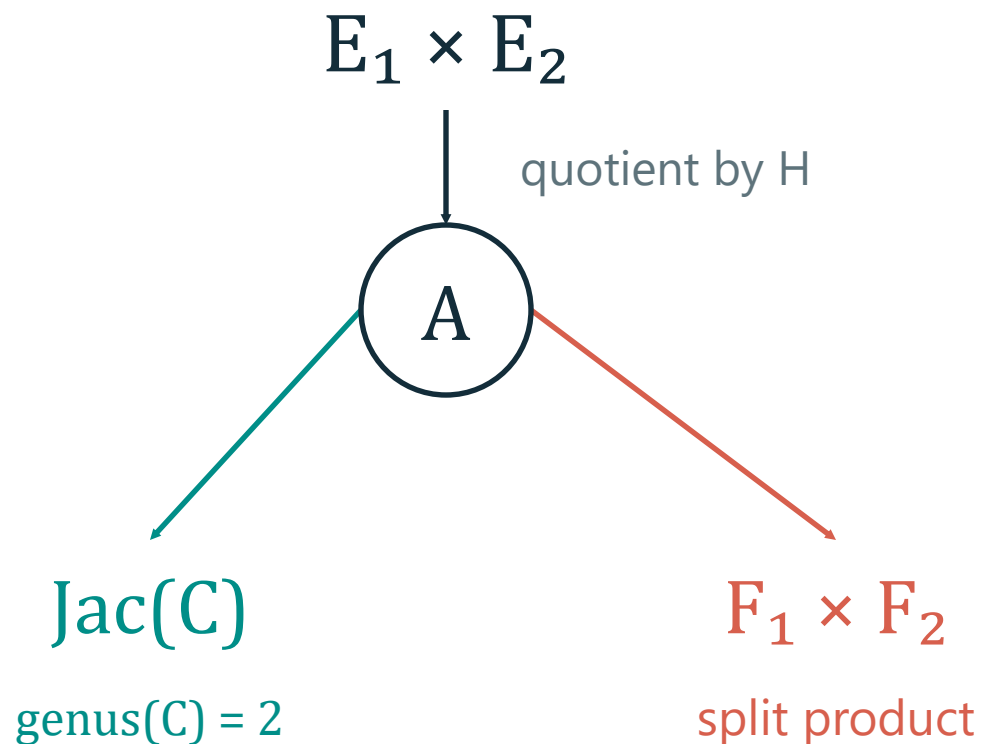
SIKEp434

SCHEME	PUBLIC KEY	CIPHERTEXT
SIKEp434	330	346
Kyber512	800	768
McEliece348864	261,120	128

**Compact keys were the promise.
The auxiliary torsion data was the weakness.**

Kani's lemma and the Castryck–Decru attack

Kani turns product splitting into a test for SIDH secret isogenies



Geometrically, as principally polarized surfaces.

- Use the public torsion images.
- Construct an auxiliary isogeny.
- Glue the two elliptic curves.
- Apply Kani's splitting criterion.
- Recover the secret path progressively.

Identification and Fiat–Shamir

Schnorr’s protocol as a model: $G = \langle g \rangle$ has prime order q

Prover

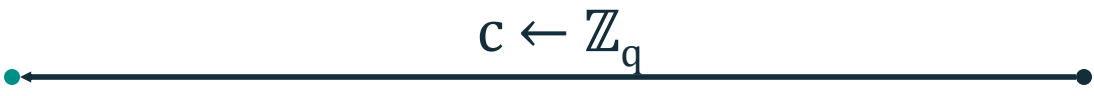
secret x

$$r \leftarrow \mathbb{Z}_q$$

Verifier

public $Y = g^x$


$$R = g^r$$


$$c \leftarrow \mathbb{Z}_q$$

random challenge


$$z = r + cx \pmod{q}$$

check $g^z = RY^c$

Fiat–Shamir

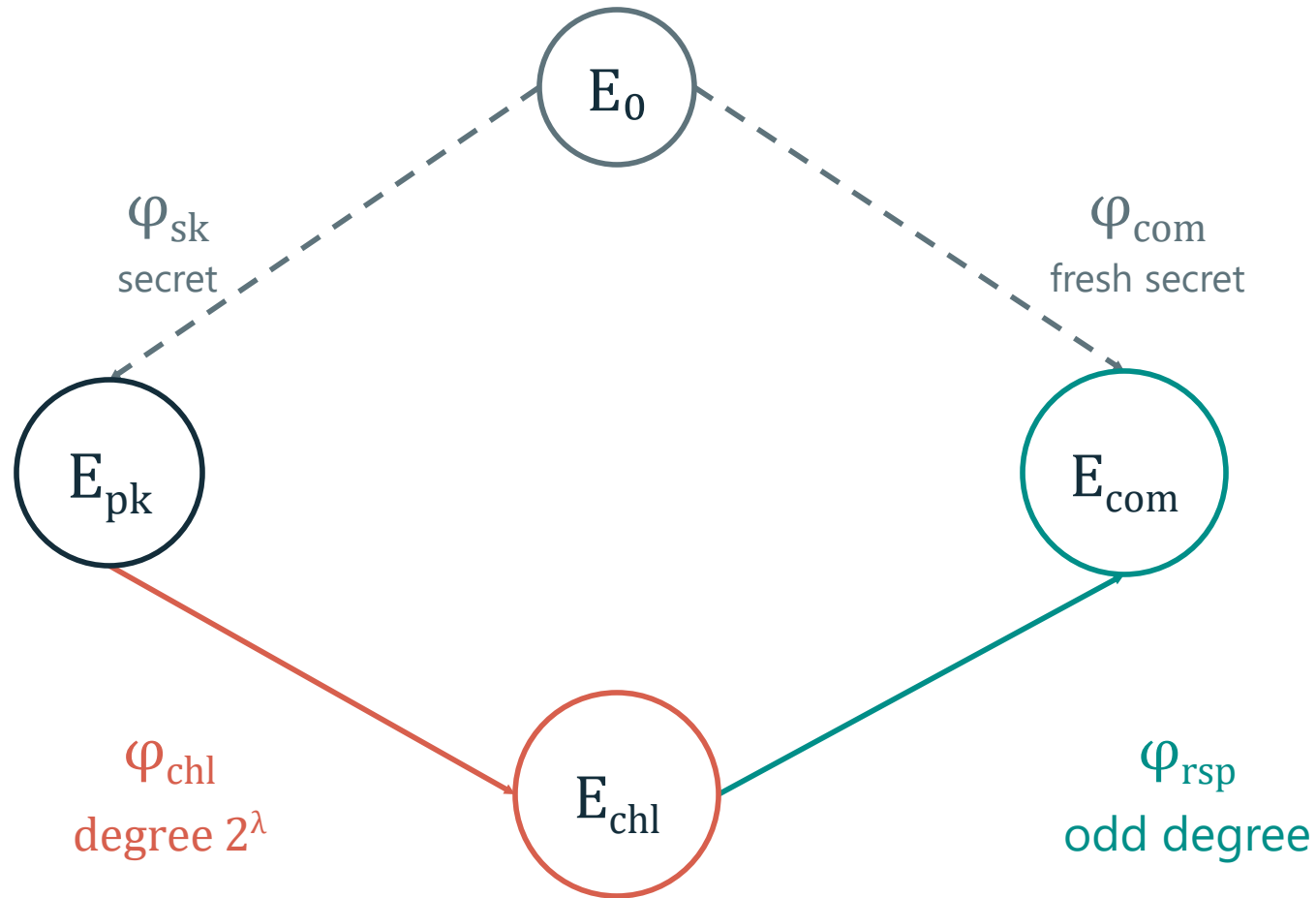
$$c = H(Y, R, m)$$

signature: (R, z)

The message fixes the challenge. The verification equation stays the same.

SQIsign: the identification diamond

Public key E_{pk} , secret isogeny φ_{sk} and its quaternion description



Commit

$$R = E_{com}$$

Challenge

$$c = H(E_{pk}, E_{com}, m)$$

$$E_{chl} = E_{pk} / \langle P + [c]Q \rangle$$

Respond

$$\sigma = (c, \text{enc}(\varphi_{rsp}))$$

Verify: recover E_{com} ,
then check the hash.

SQLsign and post-quantum signatures

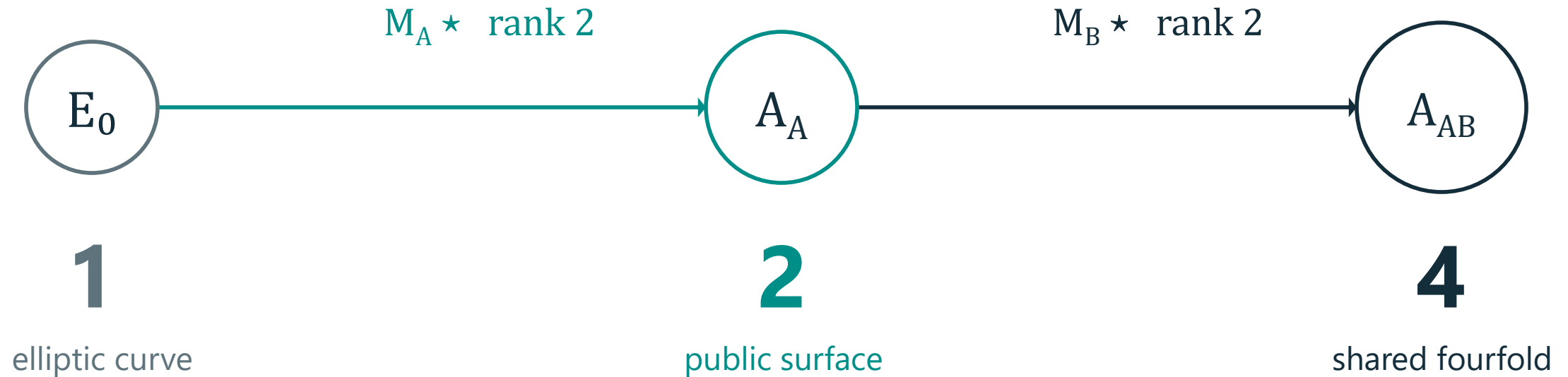
Smallest parameter sets. Public-key and signature sizes in bytes.

SCHEME	CATEGORY	PUBLIC KEY	SIGNATURE
SQLsign-I	1	83	200
ML-DSA-44	2	1,312	2,420
SLH-DSA-128s	1	32	7,856
Falcon-512	1	897	666

Tensor-MIKE: rank multiplies dimension

Rank-two modules turn one elliptic-curve dimension into two

$$\dim(M \star A) = \text{rank}_R(M) \cdot \dim(A)$$



Special surfaces use elliptic j-data: **64-byte public keys demonstrated**; security calibration ongoing.

Delfs–Galbraith: reach the subfield

The classical baseline for finding an unrestricted isogeny



$$\approx p / 12$$

vertices in the full graph

$$\tilde{O}(\sqrt{p})$$

subfield vertices

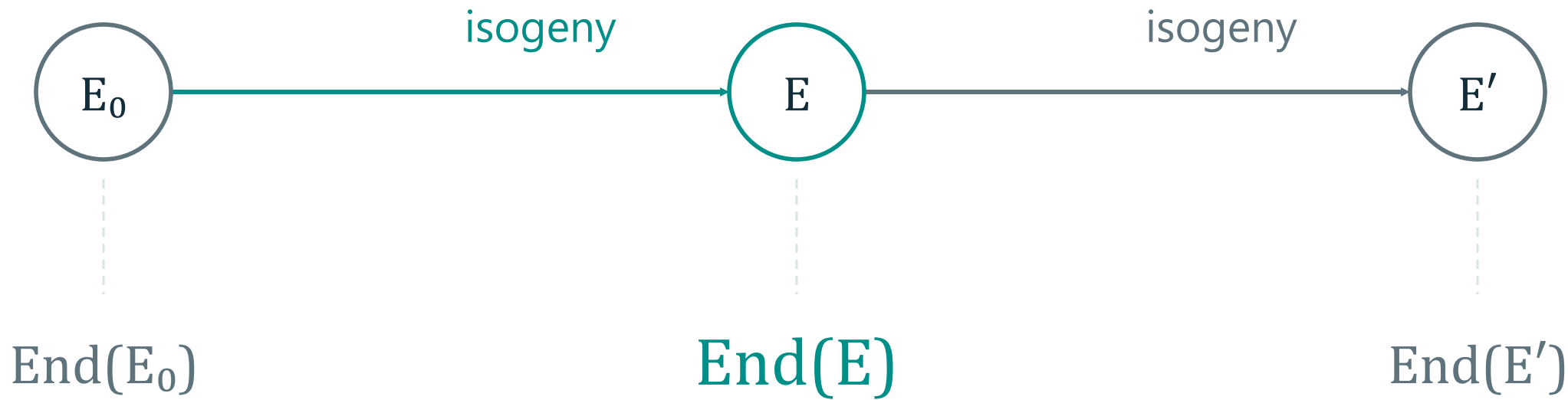
$$\tilde{O}(p^{1/2}) + \tilde{O}(p^{1/4})$$

reach subfield

connect

Every vertex hides a quaternion order

The endomorphism ring records all algebraic self-maps of the curve



Maximal orders in $B_{p,\infty}$

Find an isogeny $\Leftrightarrow$ Compute $\text{End}(E)$ $\Leftrightarrow$ Find a non-scalar endomorphism

An explicit endomorphism ring

$$y^2 = x^3 - x$$

$$\iota(x, y) = (-x, \sqrt{-1} y) \qquad \pi(x, y) = (x^p, y^p)$$

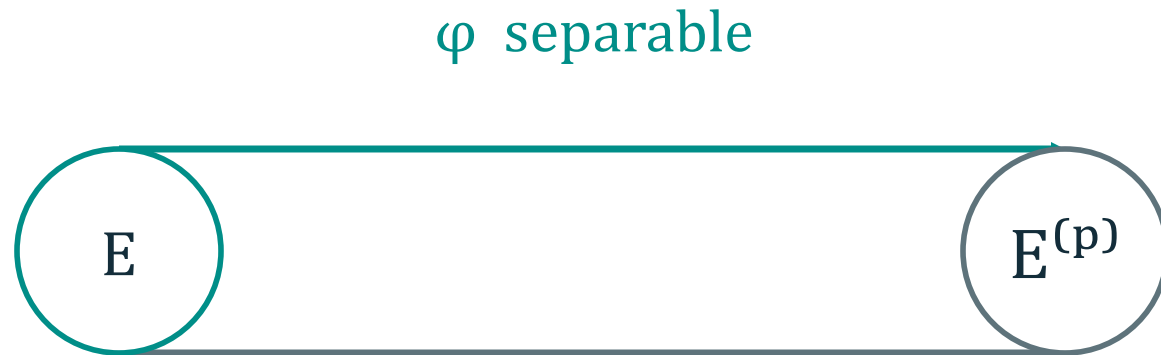
$$\iota^2 = -1 \qquad \pi^2 = -p \qquad \pi\iota = -\iota\pi$$

$$\text{End}(E_0) = \mathbb{Z} \left\langle 1, \iota, \frac{1 + \pi}{2}, \frac{\iota + \iota\pi}{2} \right\rangle$$

A maximal order in $B_{p,\infty} = (-1, -p)_{\mathbb{Q}}$

Wesolowski's 2026 breakthrough

Use Frobenius to turn a short isogeny into an endomorphism



$$\pi \circ \varphi \in \text{End}(E) \setminus \mathbb{Z}$$

$$p^{1/3}$$

+ $o(1)$ in the exponent

time and memory

Under a smoothness heuristic

Asymptotic progress is dramatic. Practical costs are still being assessed.

Open problems

isogeni.es/problems

01 The Supersingular Isogeny Problem

2026 breakthrough

02 Vectorization for Oriented Elliptic Curves

03 Hashing into Supersingular Curves

04 Optimal KLPT

05 Large-degree Isogenies from Elliptic Curves

06 Transferring Endomorphism Rings along Isogenies

07 Strong Encryption Protocols

Which mathematical obstacle should we tackle next?