SQIsign in round 3

andrea basso
and the SQIsign team

swiss crypto day – ETH zurich

sep 4, 2026

2017

Post-Quantum Cryptography PQC

Call for Proposals

Authority: This work is being initiated pursuant to NIST's responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107–347.

The submission deadline of November 30, 2017 has passed. Please see the Round 1 Submission page for a list of complete and proper submsisions.

The Call for Proposals is available for historical reference.

2024

FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

FIPS 204

Federal Information Processing Standards Publication

Module-Lattice-Based Digital Signature Standard

FIPS 205

Federal Information Processing Standards Publication

Stateless Hash-Based Digital Signature Standard

+2

2023

Post-Quantum Cryptography: Additional Digital Signature Schemes

Call for Proposals

Authority: This work is being initiated pursuant to NIST's responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107–347.

Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process (PDF)
Closed June 1, 2023

round 1 (2023):
40 signatures

round 2 (2024):
14 signatures

SQIsign

round 3 (2026):
8~~9~~ signatures

Short Quaternion and Isogeny signature

based on isogeny assumptions

✅ very compact

smallest pk + signature
of any PQ scheme

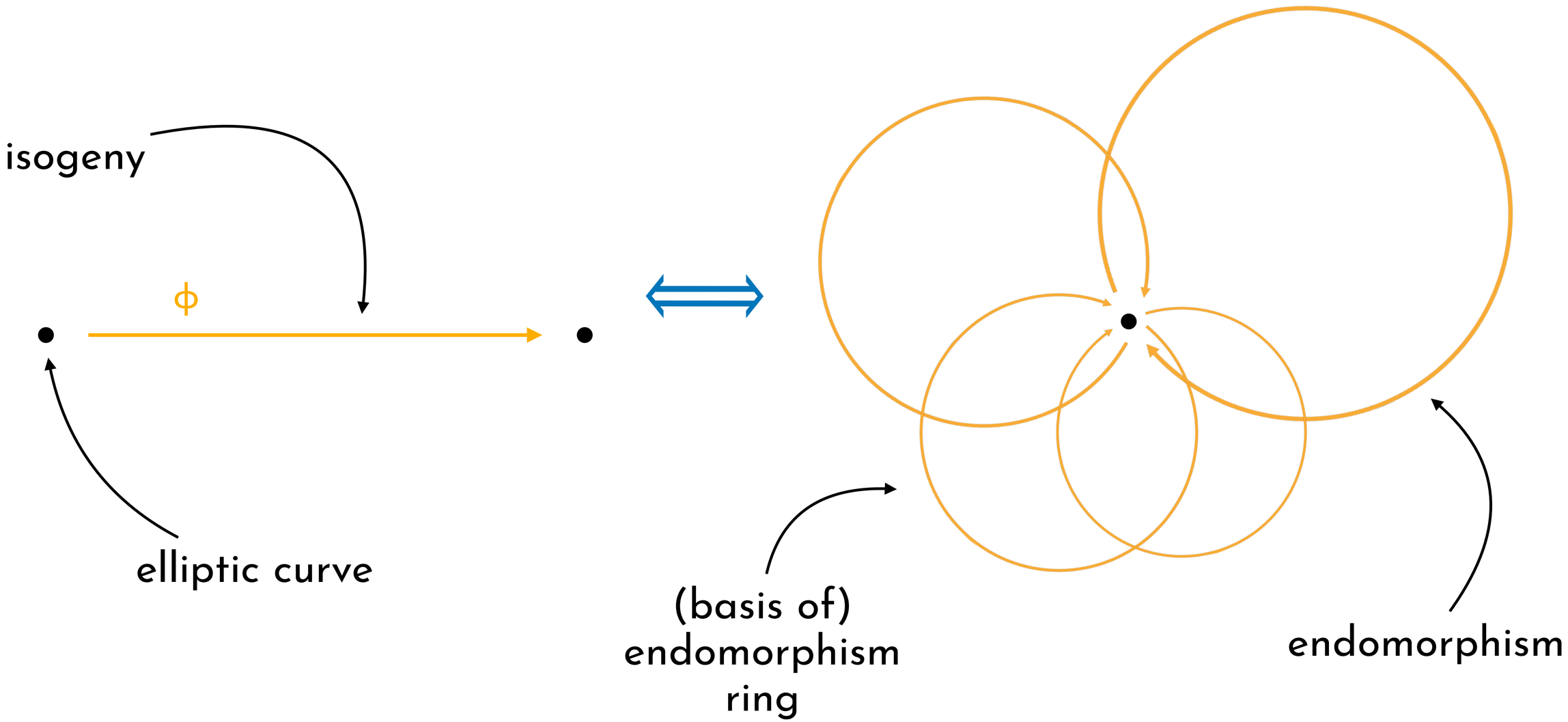
❌ fairly complex

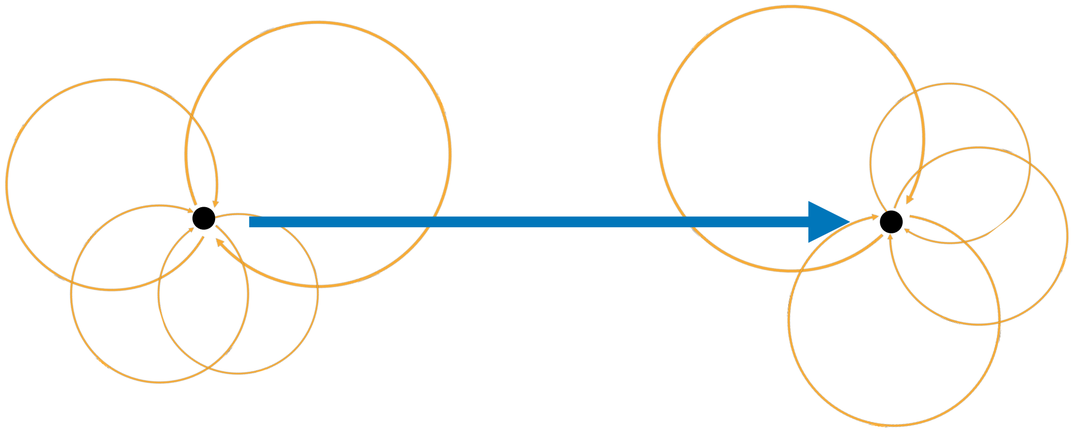
slow(ish)

no constant-time
implementation

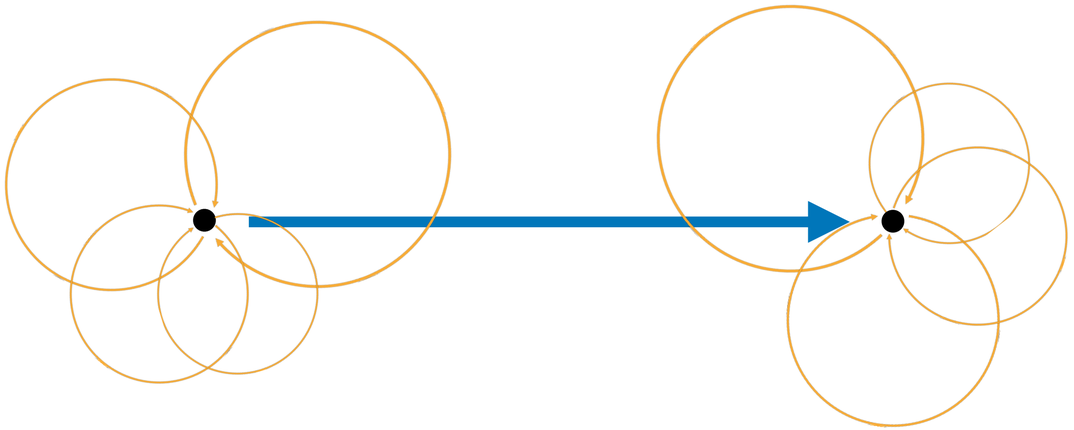
the isogeny problem

the EndRing problem



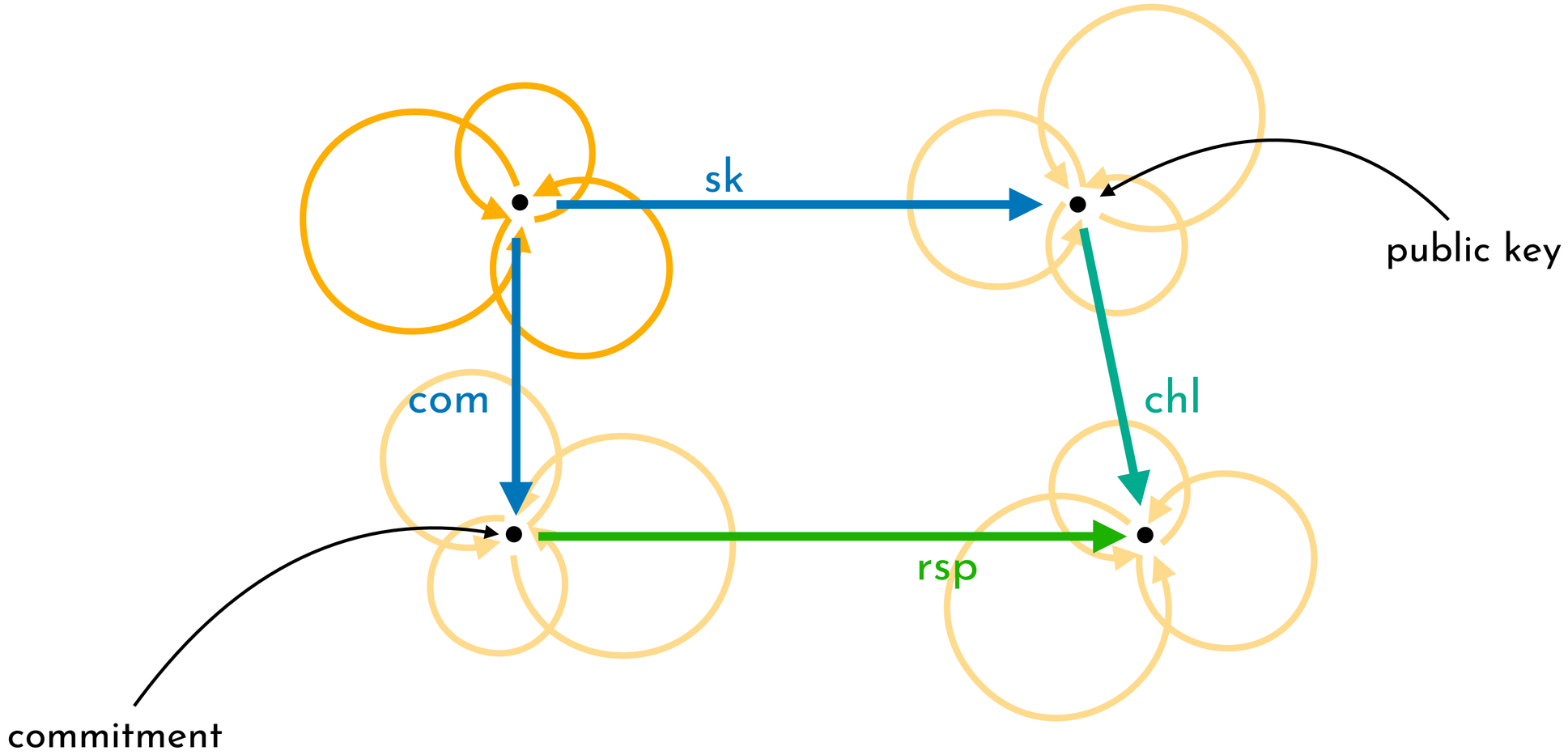


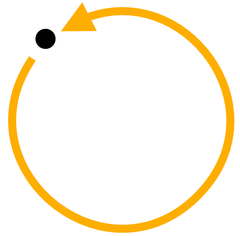
isogenies “carry”
knowledge of the
endomorphism ring

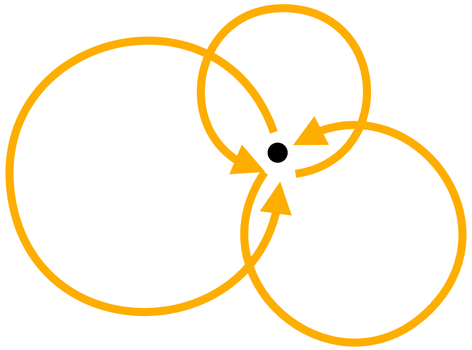


endomorphism rings
act as a trapdoor
for isogeny finding

SQIsign







quaternion

$$a + bi + cj + dij$$

rational numbers

$$i^2 = -1$$

$$j^2 = -p$$

$$ij = -ji$$

order = rank-4 **Z**-lattice
and a ring

end ring acts
as a trapdoor

ideal

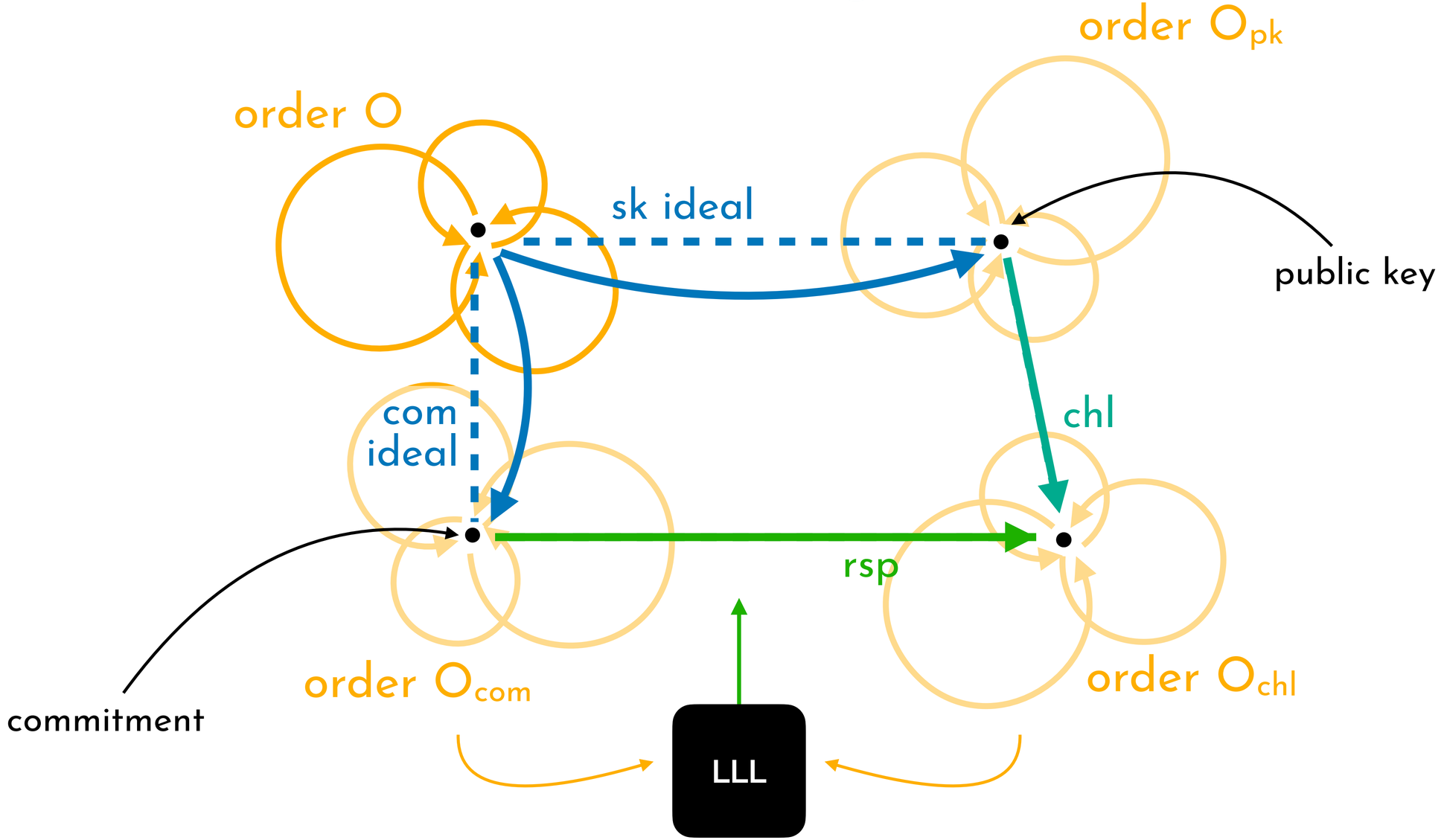
hard problems

finding a connecting isogeny

easy problems

finding a connecting ideal

SQIsign


order O_{pk}
order O
sk ideal
public key
com
ideal
chl
rsp
commitment
order O_{com}
order O_{chl}
LLL

what changed in round 3?

the first attack in 20 years

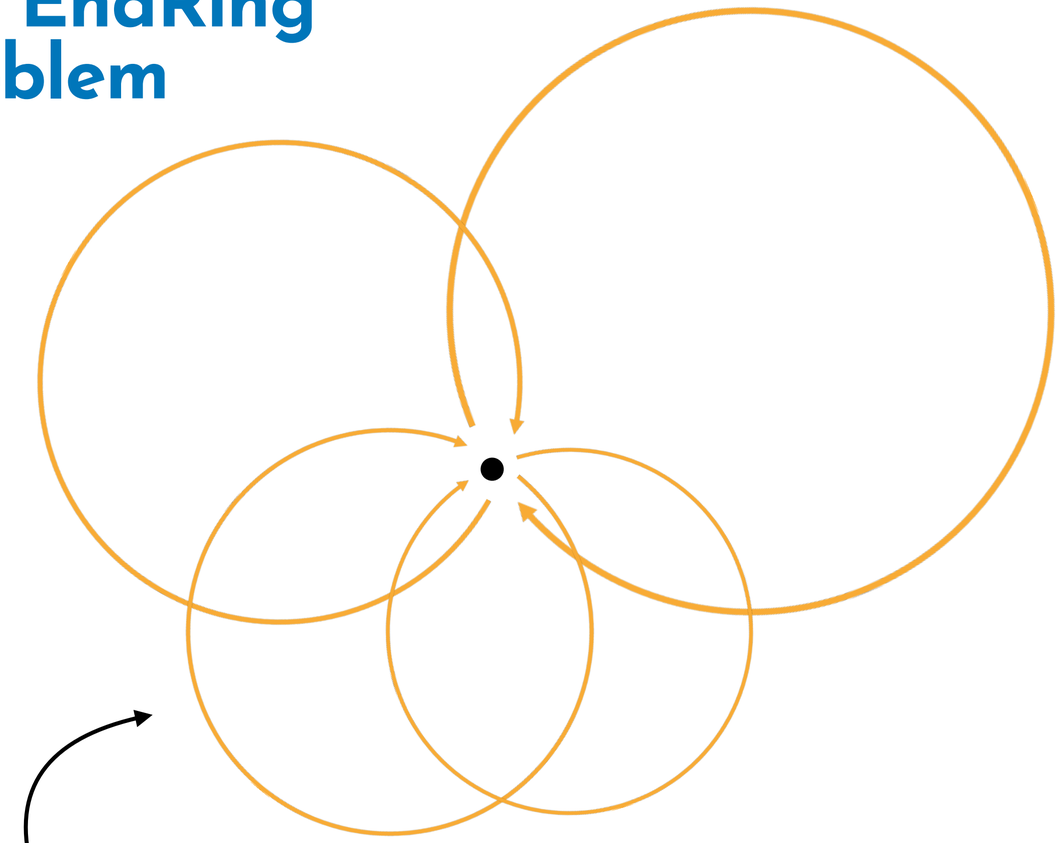
THE SUPERSINGULAR ISOGENY PROBLEM IN TIME AND MEMORY $p^{1/3+o(1)}$

BENJAMIN WESOLOWSKI

ABSTRACT. We prove that under a plausible heuristic assumption (on the smoothness of certain random integers), the supersingular isogeny problem can be solved in time and memory $p^{1/3+o(1)}$. This improves upon the previous best complexity of $p^{1/2} \cdot (\log p)^{O(1)}$.

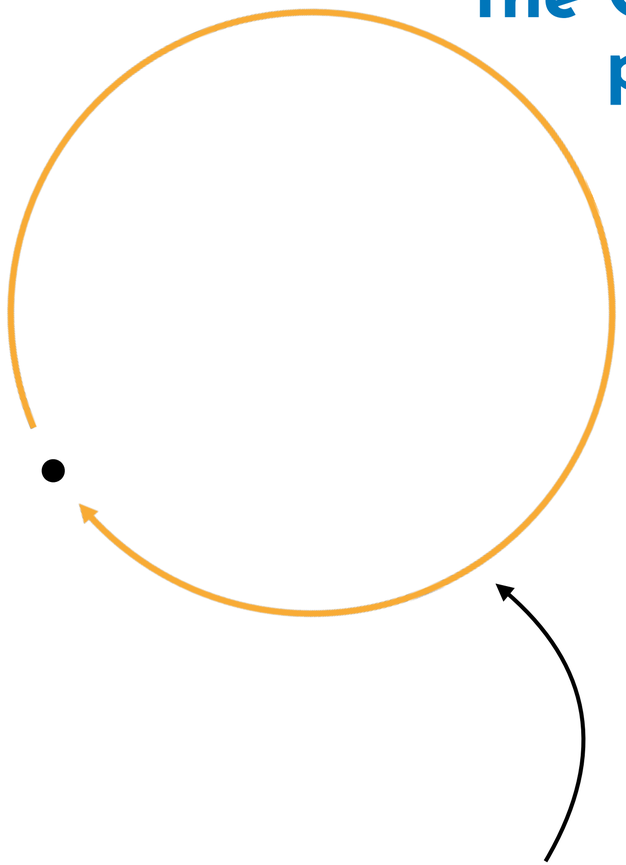
This problem is arguably *the* central hard problem underlying isogeny-based cryptography, and the cost of its resolution is a major (and often the only) factor in the choice of secure parameters. The impact on concrete parameter sets remains to be clarified, as the asymptotic advantage of the new algorithm is mitigated by a superpolynomial overhead hiding in the $o(1)$ exponent, and by its high memory requirement.

the EndRing problem



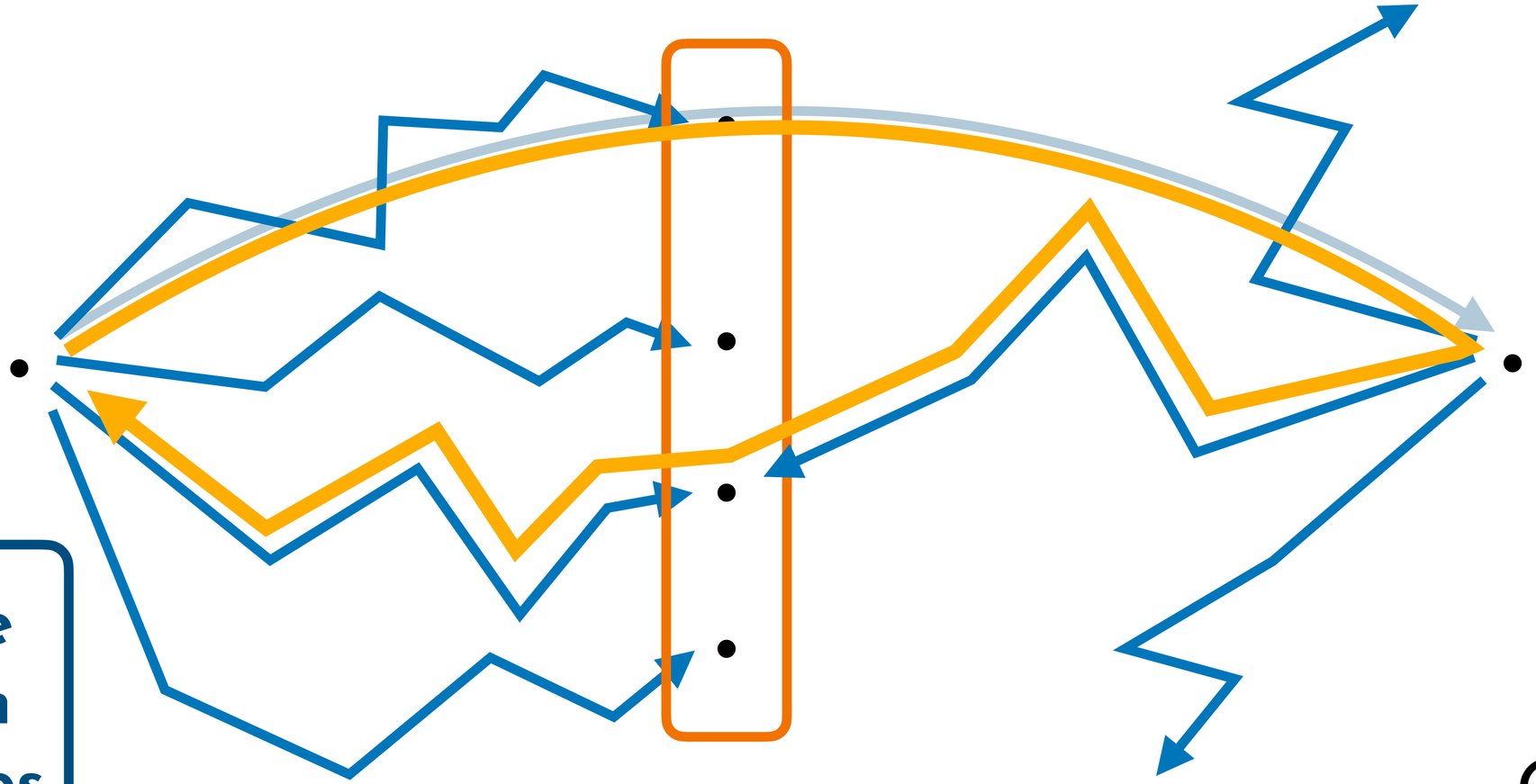
endomorphism ring

the OneEnd problem



a (non-trivial) endomorphism

a simple attack: meet in the middle



distance between two curves

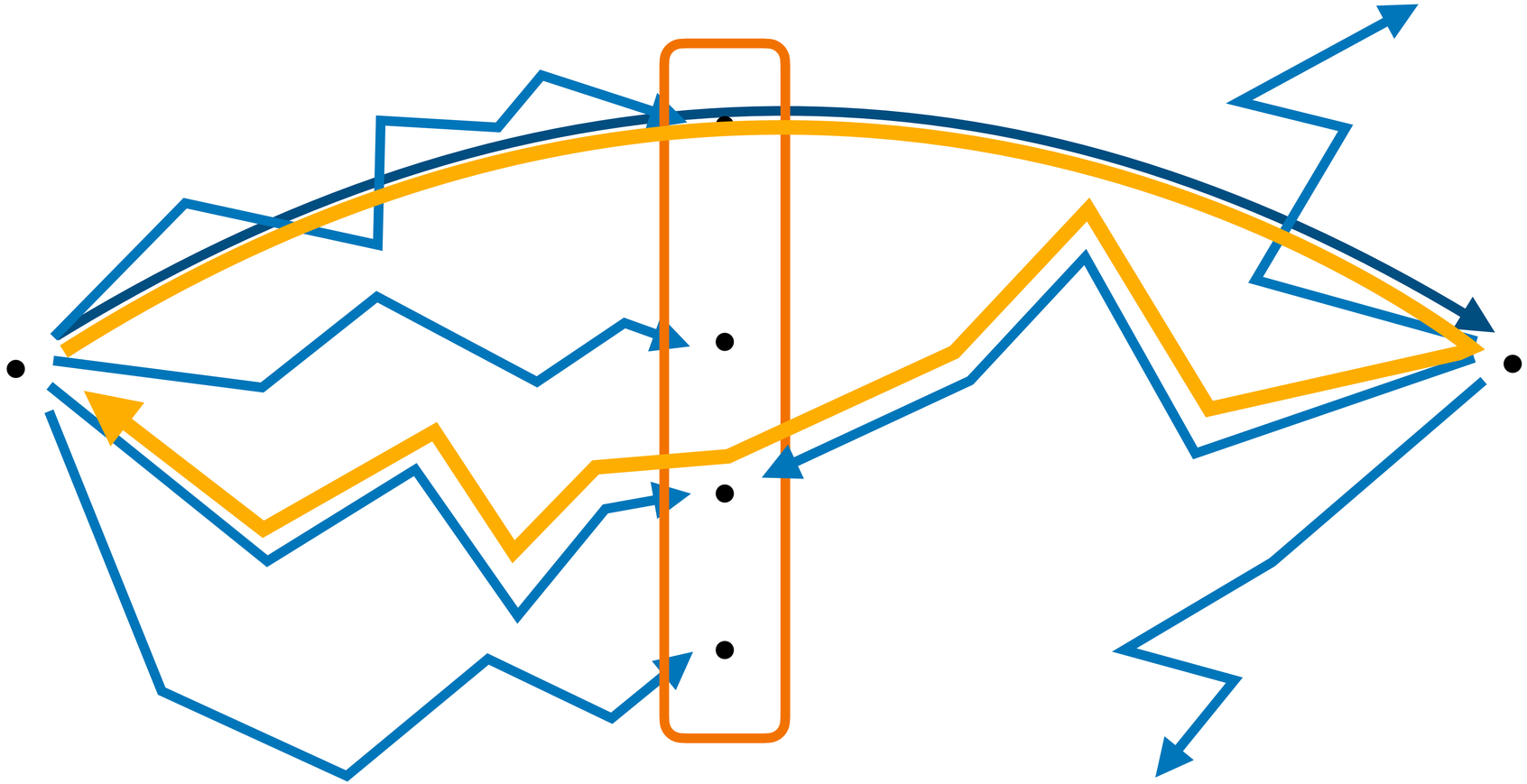
$p^{1/2}$

time = $O(p^{1/2})$

memory = $O(p^{1/2})$ ~~$O(p^{1/2})$~~ $O(1)$

the new attack

if  is special, it turns out the two curves are closer than expected ($p^{1/3}$ vs $p^{1/2}$)



time = $O(p^{1/3})$

memory = $O(p^{1/3})$

what parameters to pick?

before

$p = O(2^{2\lambda})$

after the attack

fix memory limit

ignore poly factors

2^{80}
2^{100}
2^{120}

SQIsign v3

$p = 3 \cdot 2^{324} - 1$
$p = 27 \cdot 2^{500} - 1$
$p = 17 \cdot 2^{664} - 1$

unlimited memory

account for poly factors

what *else* changed in round 3?

same overall design

better algorithms

simpler protocol

odd-degree responses

redesigned quaternion algs

2x faster ideal-to-isogeny translation

constant-time LLL
(no more floating point)

fixed-sized integers
(no more external libraries)

algorithm independent KATs

good progress on constant time

λ	|pk|	|sign|	Sign	Verify
128	83 B	200 B	27.6 ms	3.6 ms
192	129 B	306 B	94.2 ms	9.3 ms
256	169 B	406 B	198.4 ms	22.8 ms

1

SQIsign has matured a lot in round 3

same crypto, but simpler, cleaner, and with better algs

2

a new attack made security more expensive

larger parameters mean worse performance

3

still the smallest PQ signature!

83 B public keys, 200 B signatures at level I