SQIsign: New Trends and a Complete Security Proof

Andrea Basso

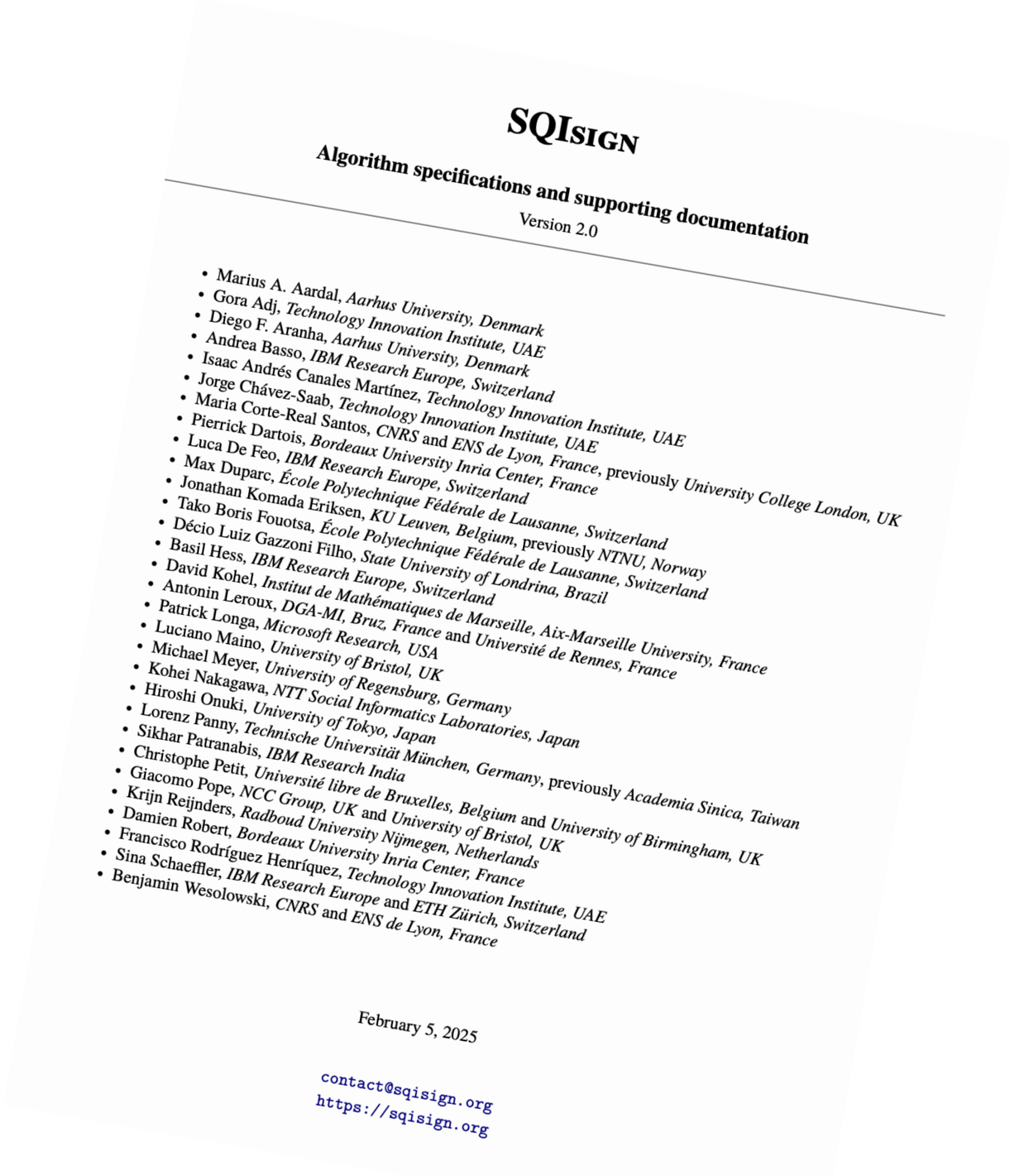
Neuchatel – St.Gallen – Zurich Seminar in Coding Theory and Cryptography

2nd April 2025

1 An introduction to SQIsign

2 The many variants of SQIsign

3 The security of SQIsign



SQIsign

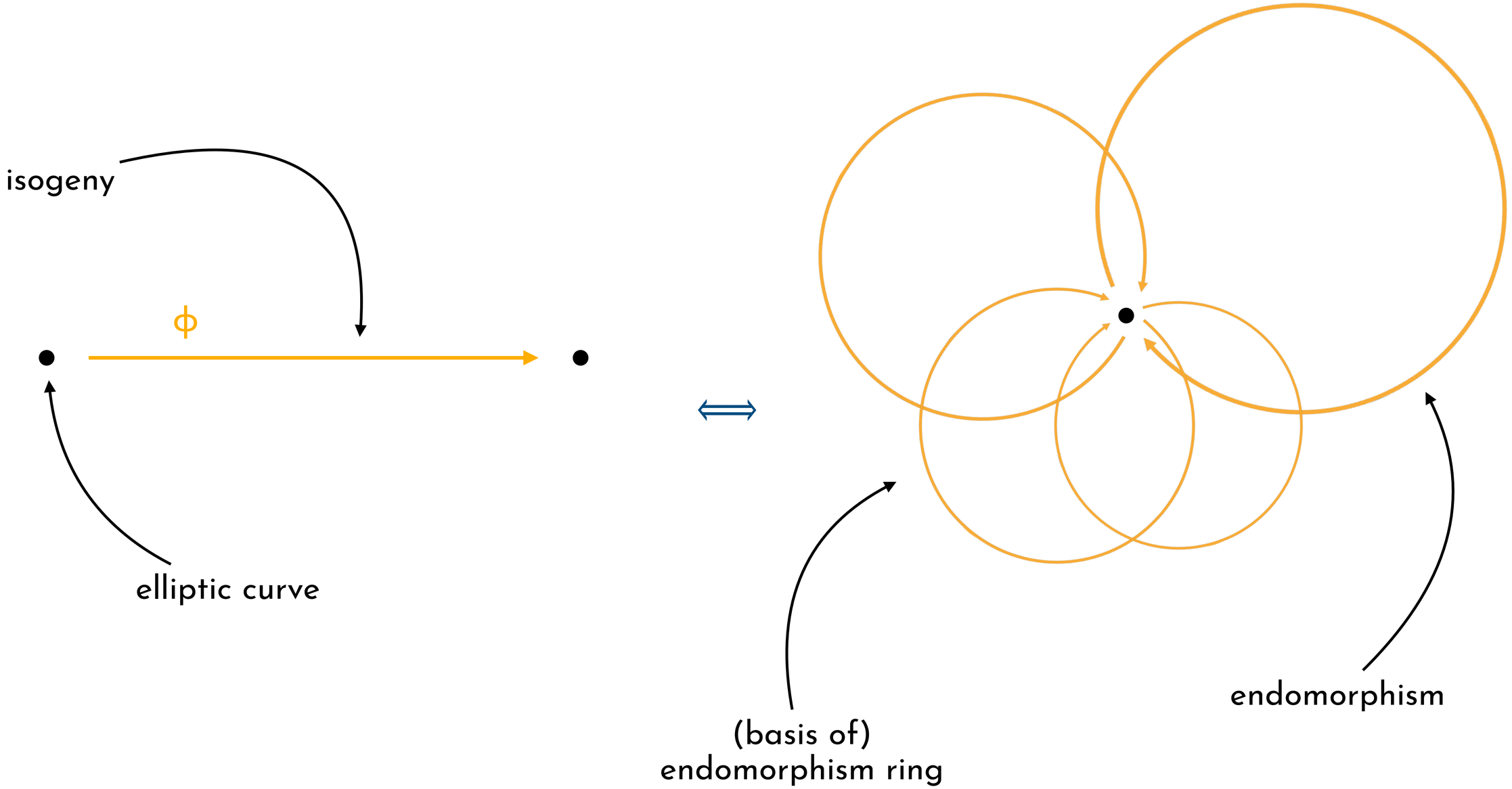
Algorithm specifications and supporting documentation

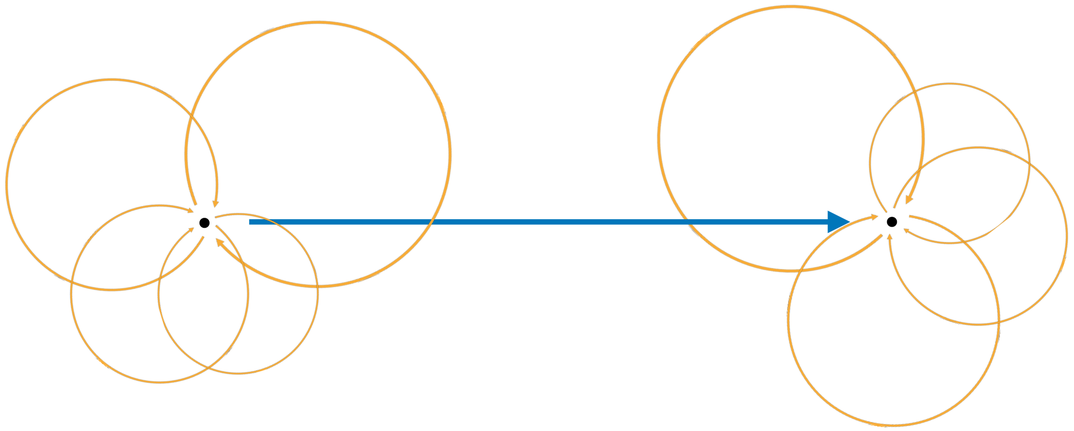
Version 2.0

- Marius A. Aardal, *Aarhus University, Denmark*
- Gora Adj, *Technology Innovation Institute, UAE*
- Diego F. Aranha, *Aarhus University, Denmark*
- Andrea Basso, *IBM Research Europe, Switzerland*
- Isaac Andrés Canales Martínez, *Technology Innovation Institute, UAE*
- Jorge Chávez-Saab, *Technology Innovation Institute, UAE*
- Maria Corte-Real Santos, *CNRS* and *ENS de Lyon, France*, previously *University College London, UK*
- Pierrick Dartois, *Bordeaux University Inria Center, France*
- Luca De Feo, *IBM Research Europe, Switzerland*
- Max Duparc, *École Polytechnique Fédérale de Lausanne, Switzerland*
- Jonathan Komada Eriksen, *KU Leuven, Belgium*, previously *NTNU, Norway*
- Tako Boris Fouotsa, *École Polytechnique Fédérale de Lausanne, Switzerland*
- Décio Luiz Gazzoni Filho, *State University of Londrina, Brazil*
- Basil Hess, *IBM Research Europe, Switzerland*
- David Kohel, *Institut de Mathématiques de Marseille, Aix-Marseille University, France*
- Antonin Leroux, *DGA-MI, Bruz, France* and *Université de Rennes, France*
- Patrick Longa, *Microsoft Research, USA*
- Luciano Maino, *University of Bristol, UK*
- Michael Meyer, *University of Regensburg, Germany*
- Kohei Nakagawa, *NTT Social Informatics Laboratories, Japan*
- Hiroshi Onuki, *University of Tokyo, Japan*
- Lorenz Panny, *Technische Universität München, Germany*, previously *Academia Sinica, Taiwan*
- Sikhar Patranabis, *IBM Research India*
- Christophe Petit, *Université libre de Bruxelles, Belgium* and *University of Birmingham, UK*
- Giacomo Pope, *NCC Group, UK* and *University of Bristol, UK*
- Krijn Reijnders, *Radboud University Nijmegen, Netherlands*
- Damien Robert, *Bordeaux University Inria Center, France*
- Francisco Rodríguez Henríquez, *Technology Innovation Institute, UAE*
- Sina Schaeffler, *IBM Research Europe* and *ETH Zürich, Switzerland*
- Benjamin Wesolowski, *CNRS* and *ENS de Lyon, France*

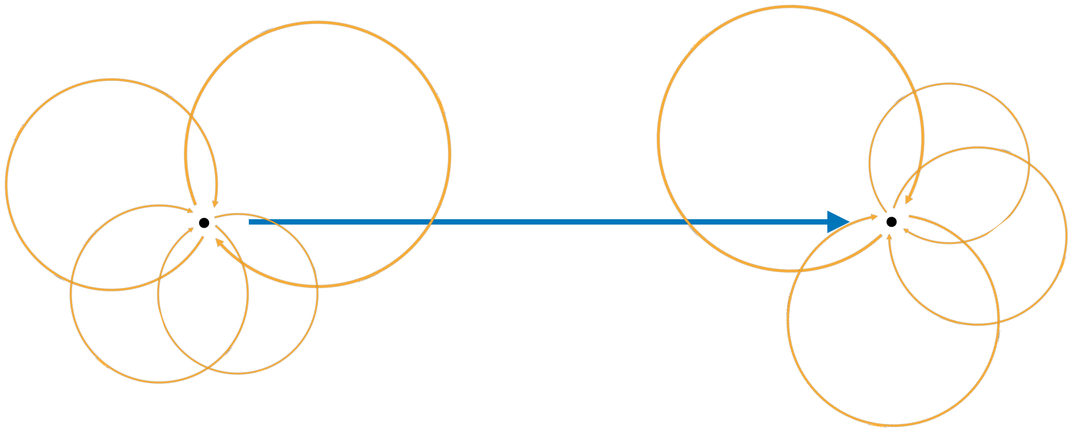
February 5, 2025

contact@sqisign.org
https://sqisign.org


isogeny
ϕ
elliptic curve
⟺
(basis of)
endomorphism ring
endomorphism

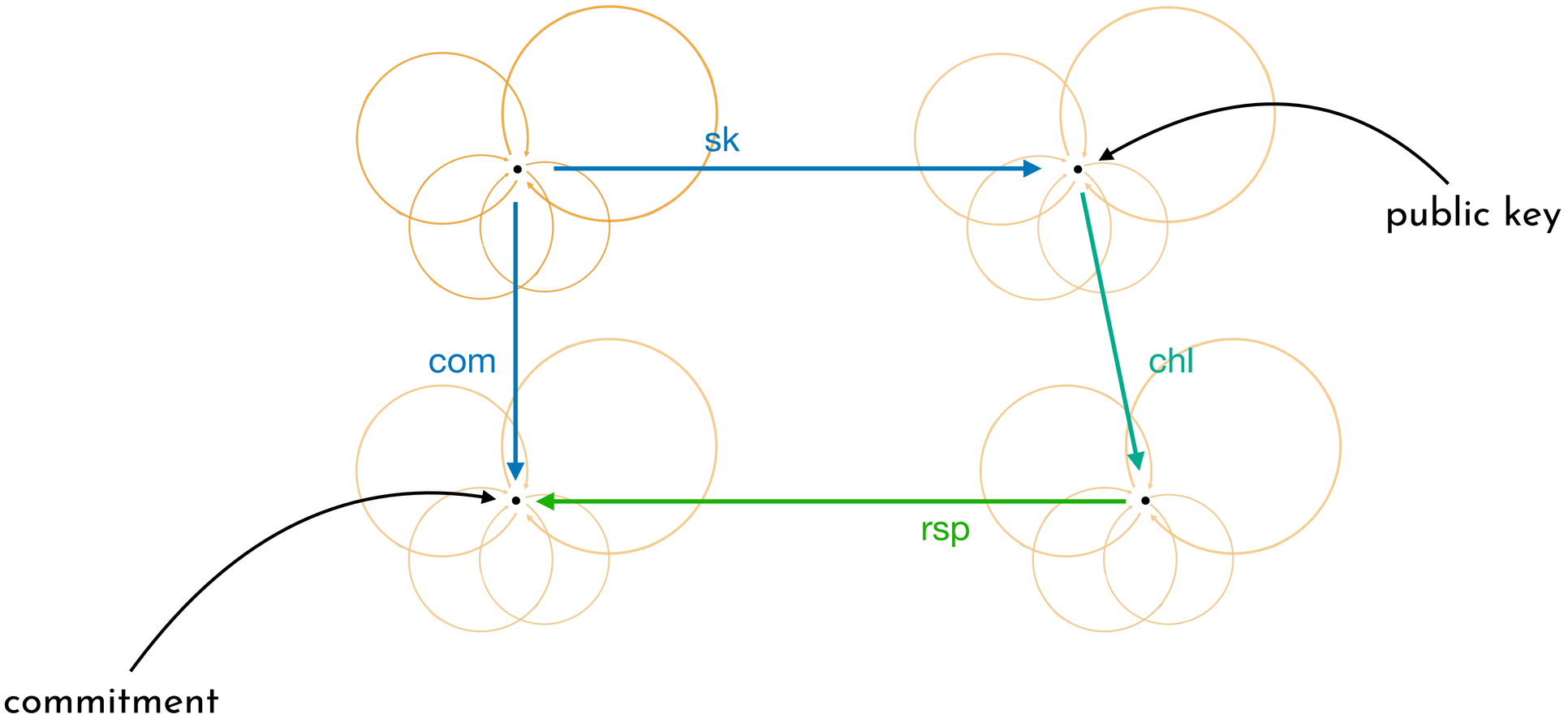


isogenies “carry”
knowledge of the
endomorphism ring

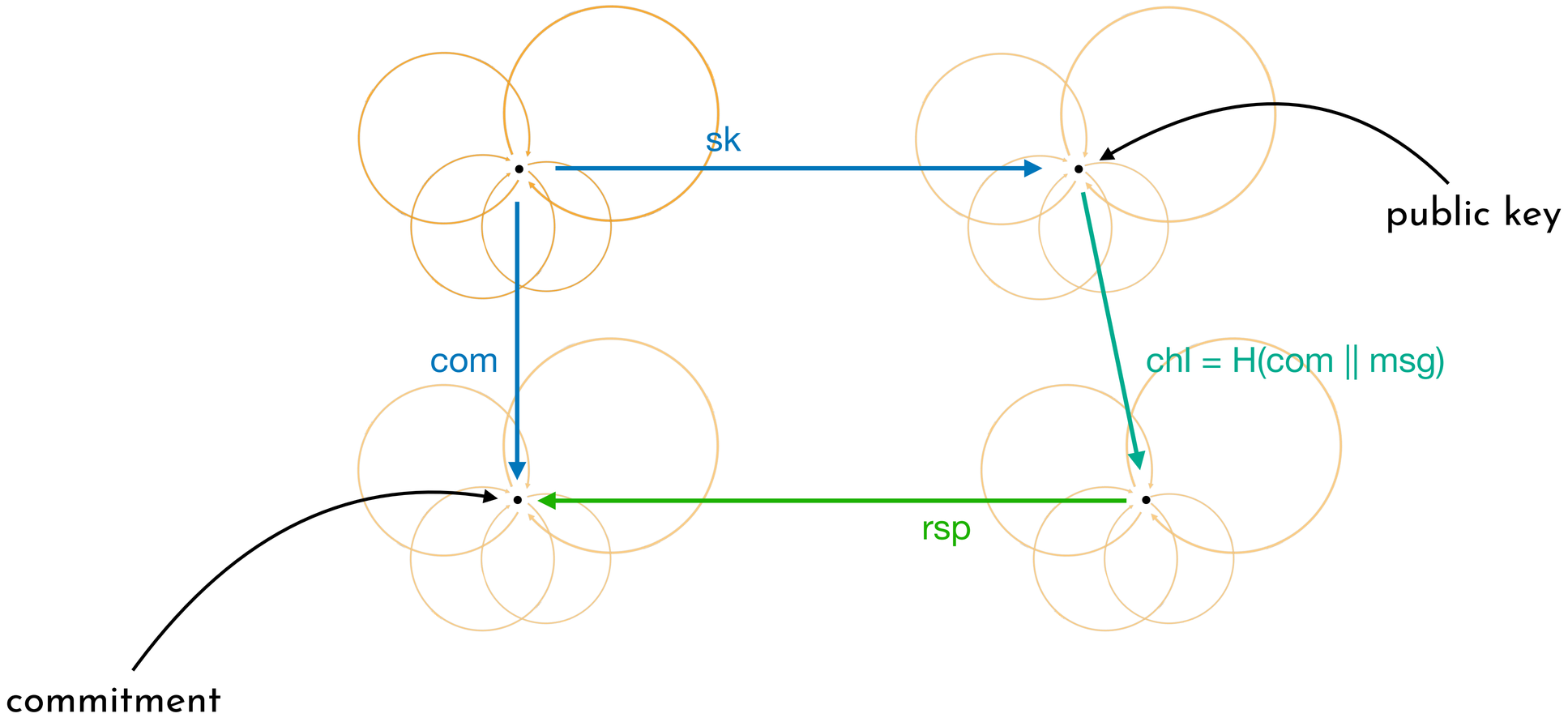


knowldege of
endomorphism rings
enable isogeny finding

SQIsign – ID protocol



SQIsign – signature



How do we represent isogenies?

deg ϕ
≈ length of ϕ

$$\bullet \xrightarrow{\phi} \bullet$$

cost ≈ deg ϕ
#isogenies ≈ deg ϕ

if $\deg\phi = 2^a$ $\longrightarrow$

$$\overbrace{\bullet \to \bullet \to \bullet \to \bullet \to \bullet \to \bullet \to \bullet \to \bullet}^{a \text{ isogenies of deg} = 2}$$

cost ≈ $2a$
#isogenies ≈ 2^a

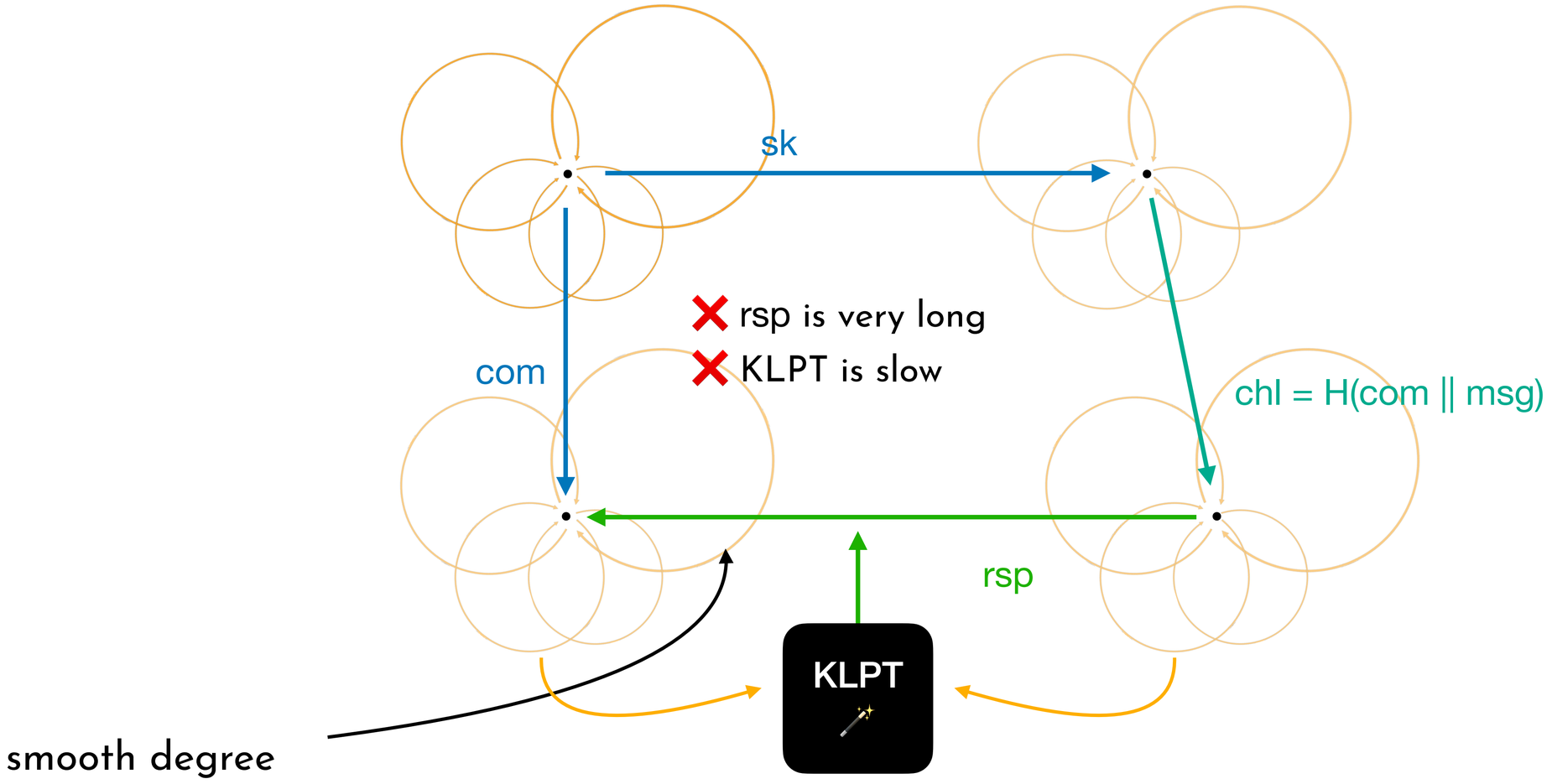
if $\deg\phi$ = prime

higher-dimensional representation

- E_0, E_1
- P, Q and $\phi(P)$, $\phi(Q)$
- deg ϕ

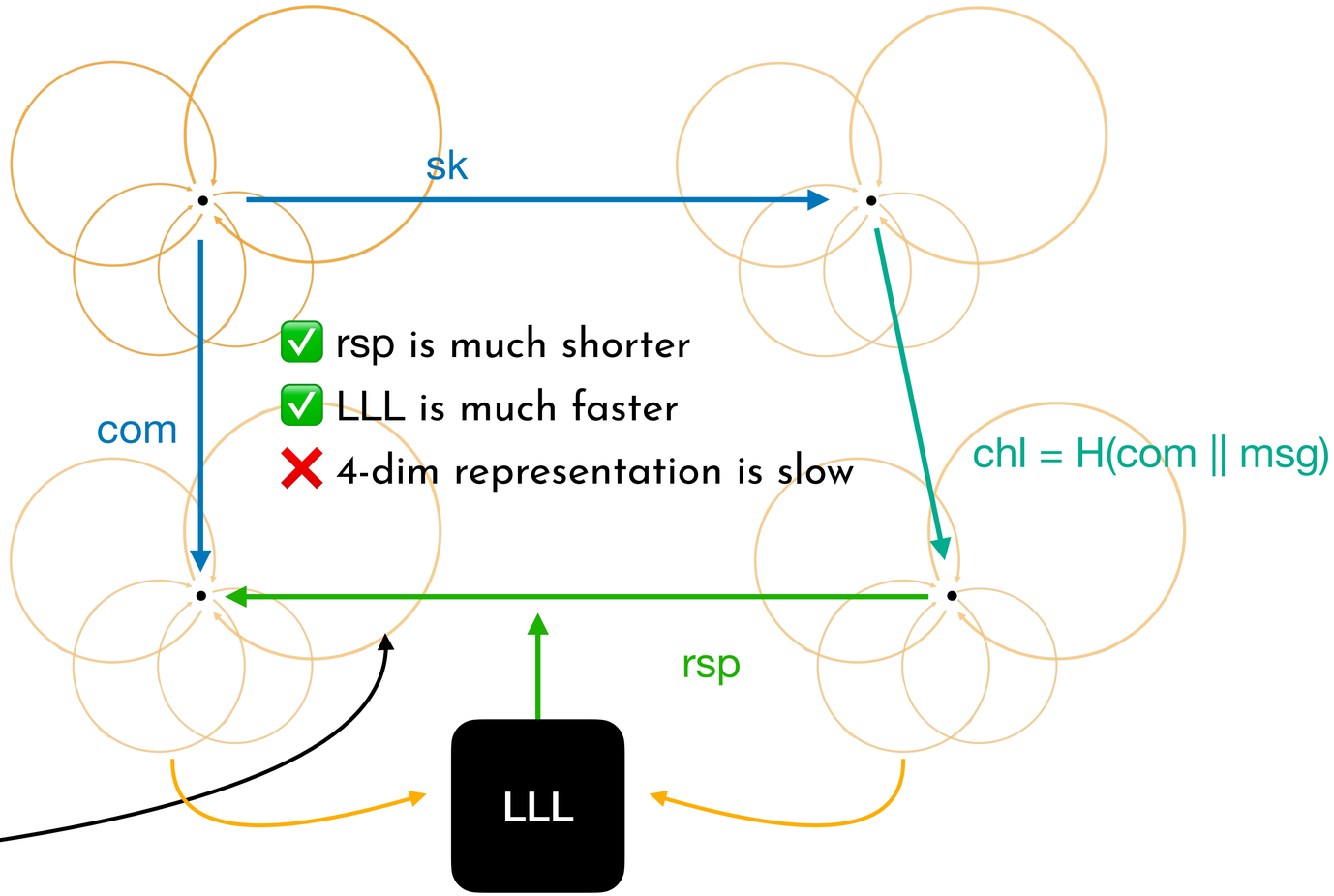
cost =
- 😁 if $\deg\phi = q(2^a - q)$
- 😐 otherwise

SQIsign1D – smooth responses



De Feo, Kohel, Leroux, Petit, Wesolowski (2020) + De Feo, Leroux, Longa, Wesolowski (2022)

SQIsignHD



✅ rsp is much shorter

✅ LLL is much faster

❌ 4-dim representation is slow

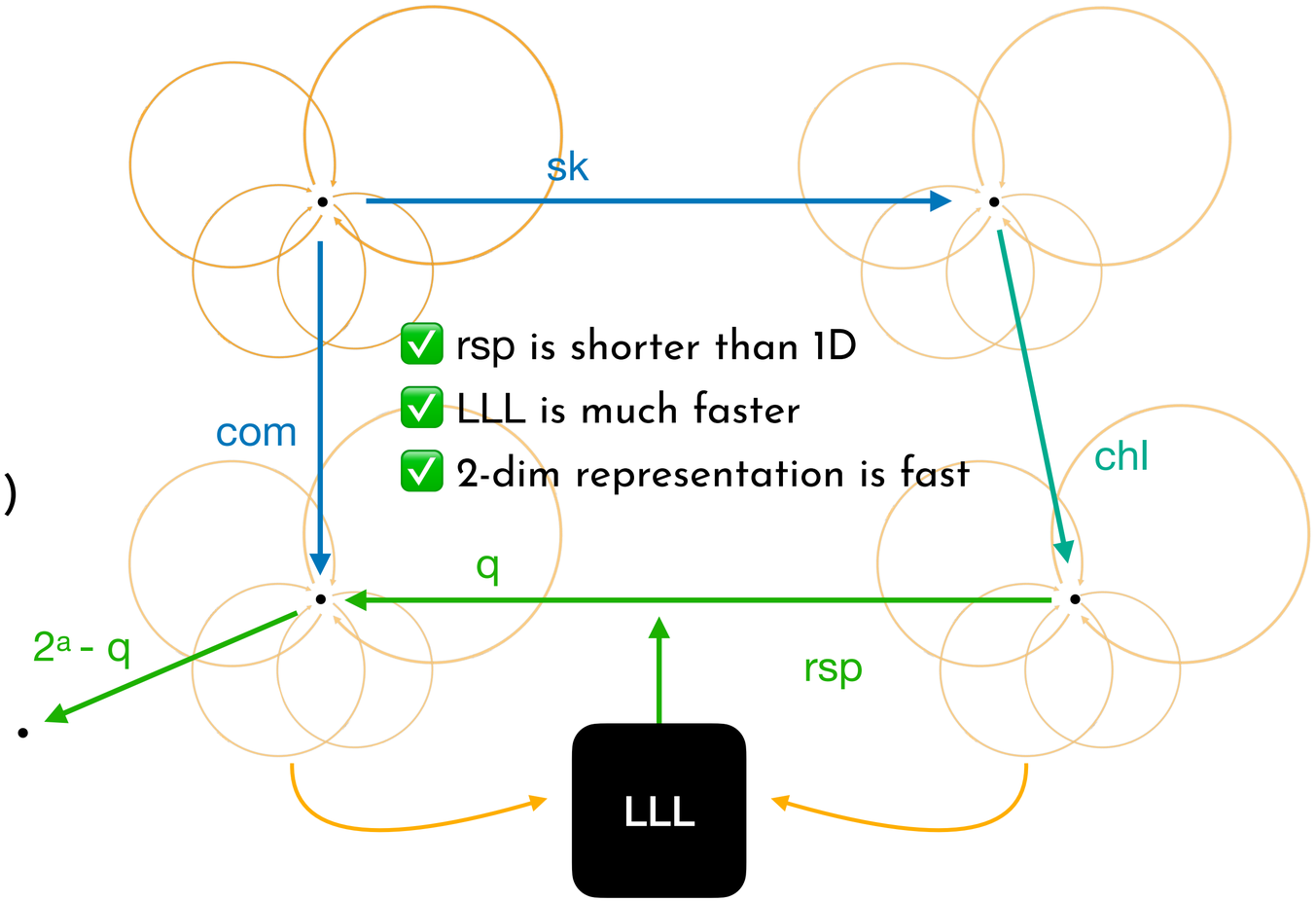
UNsmooth degree,
4-dimensional
representation

Dartois, Leroux, Robert, and Wesolowski (2023)

SQIsign2D

2-dimensional representation requires

deg rsp = $q(2^a - q)$



✅ rsp is shorter than 1D

✅ LLL is much faster

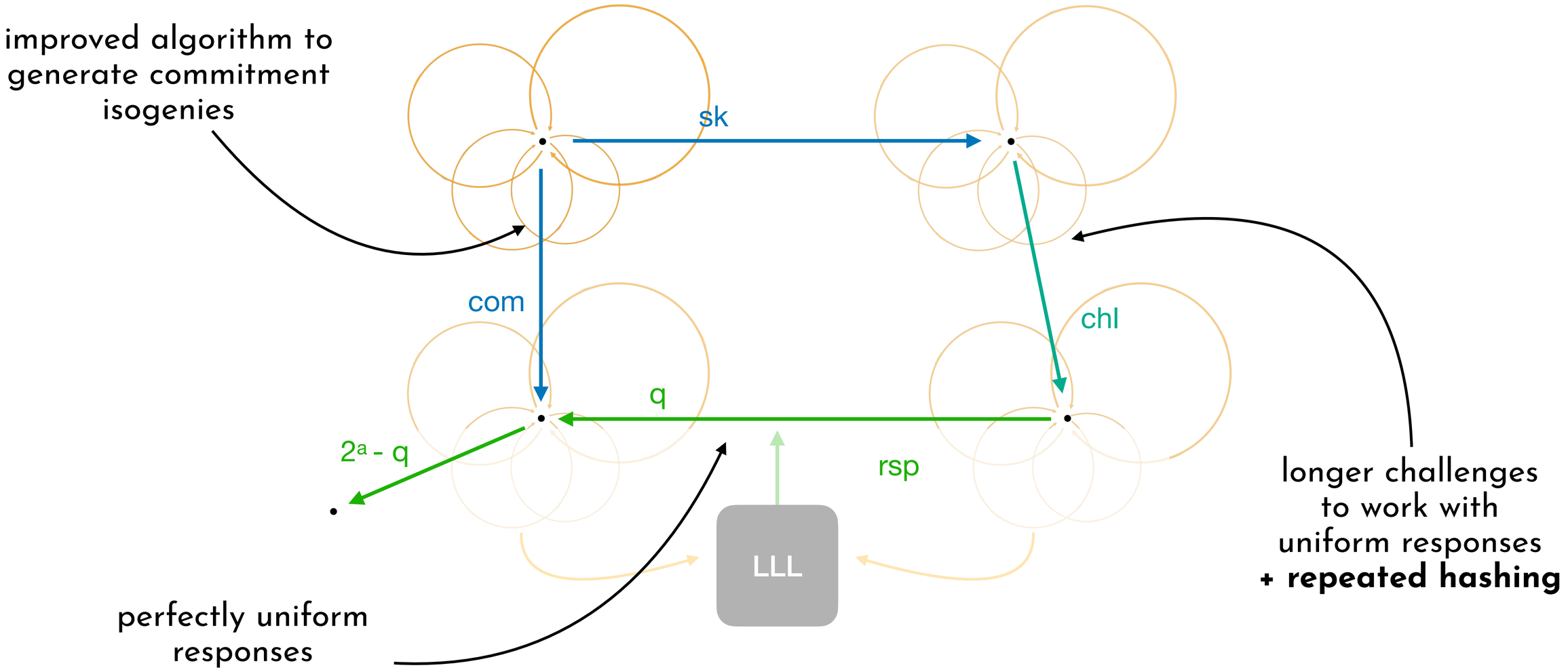
✅ 2-dim representation is fast

- new algorithm to sample secret keys and commitment isogenies (but it may fail!)
- ≈uniform public keys and commitment curves
- conservative approach in parameters and design choices

Basso, Dartois, De Feo, Leroux, Maino, Pope, Robert, Wesolowski (2024)

	SQIsign	SQIsignHD	SQIsign2D
Signature size	🎉	🎉🎉🎉	🎉🎉
Signing efficiency	😔	👍👍	👍
Verification efficiency	👍	😶	👍👍
Security	😶	👍	👍
Scalability	👎	🎉	🎉

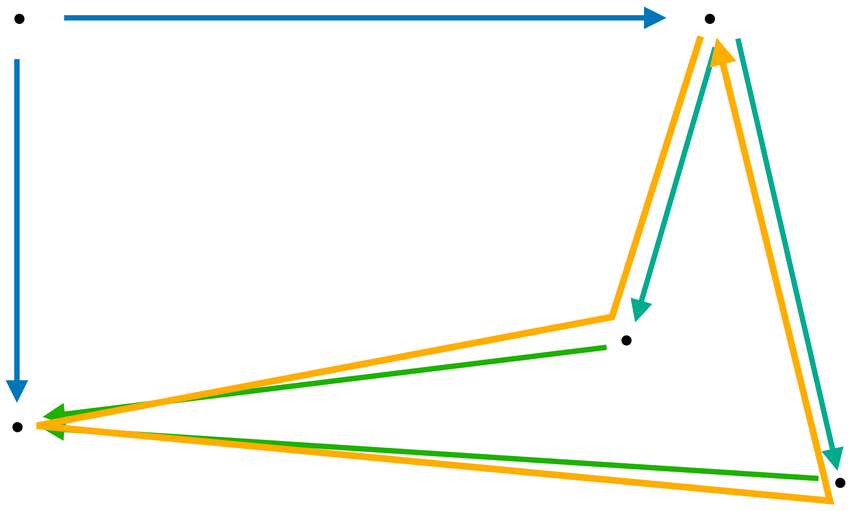
SQIsign 2.0


improved algorithm to generate commitment isogenies
sk
com
chl
q
$2^a - q$
rsp
LLL
longer challenges to work with uniform responses
+ repeated hashing
perfectly uniform responses

	sizes (byte)		**timings** (ms)		
	public key	**signature**	**key gen**	**signing**	**Verification**
NIST level 1	**65**	**148**	**12.7**	**29.9**	**1.5**
NIST level 3	97	224	39.4	90.9	5.5
NIST level 5	129	292	62.4	149.3	10.5

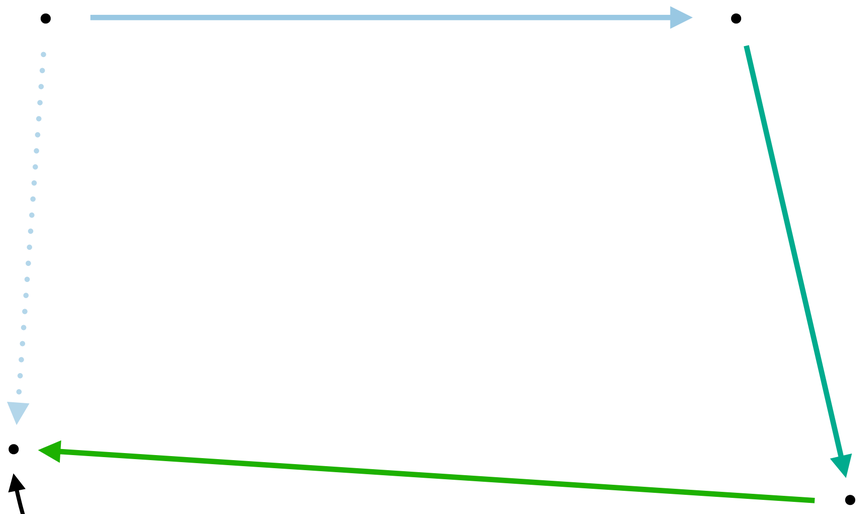
Security

2-soundness



two transcripts, one commitment $\Longrightarrow$ one endomorphism of pk $\Longrightarrow$ endomorphism ring of pk

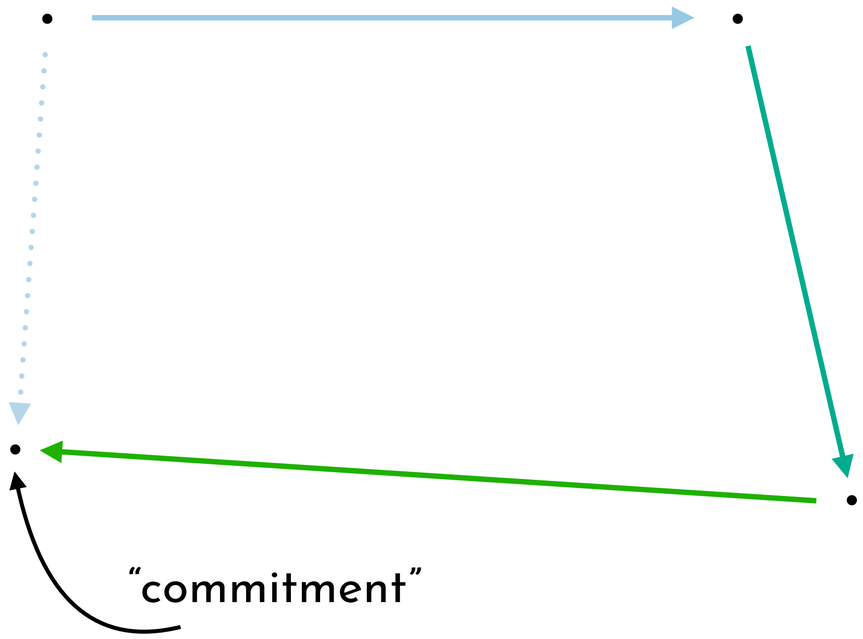
zero-knowledge



"commitment"

how to sample?

Zero knowledge



1. Sample a random challenge ✅
2. Sample a random response ❌
3. Is the commitment uniform? ❌

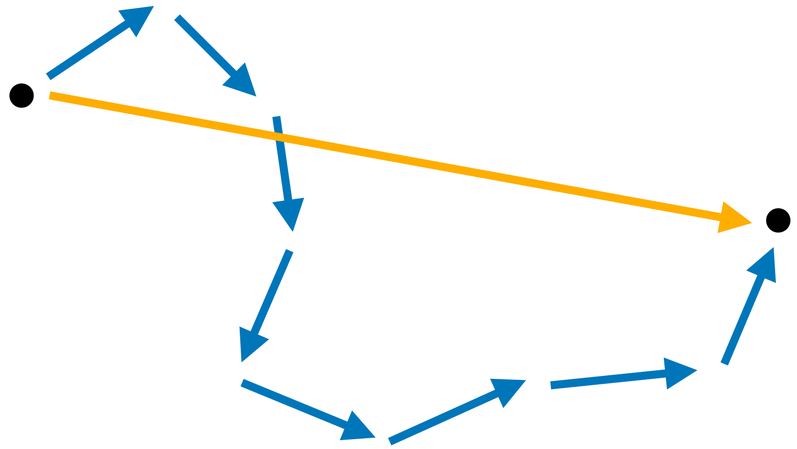
Previous solution: assume we have an oracle that

1. samples a random curve
2. samples a connecting isogeny

Partial security proofs

Previous solution: assume we have an oracle that

1. samples a random curve
2. samples a connecting isogeny



Intuition: unsmooth-degree isogenies do not provide more info than smooth-degree ones

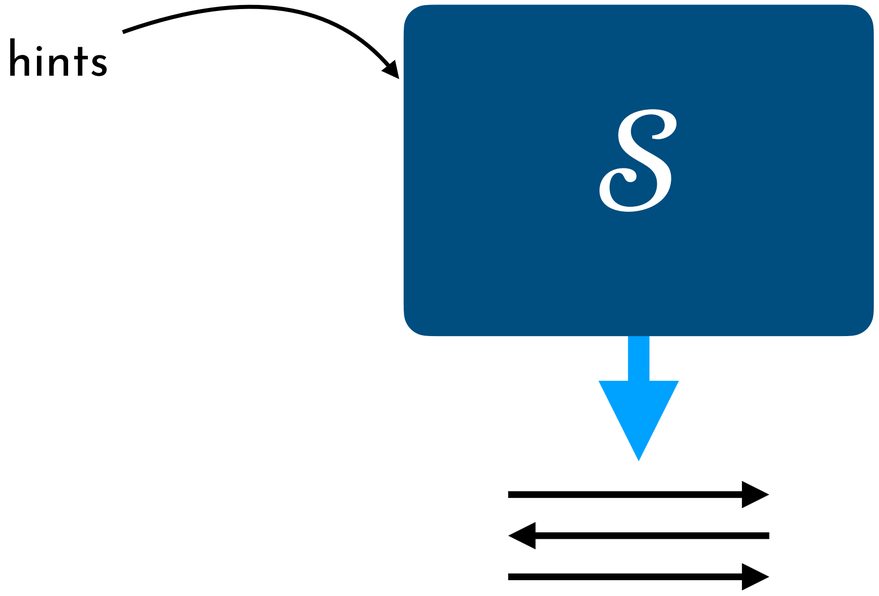
1 Uniform distribution on the target curve strongly requires knowledge of the secret

2 **All** previous security proofs only hold in *ad-hoc* idealized models

A new security proof

1. A proof that holds in the ROM (without additional oracles)
2. No interactive hardness assumptions
3. A complete proof that leads to a precise quantification of losses

Fiat–Shamir *with hints*

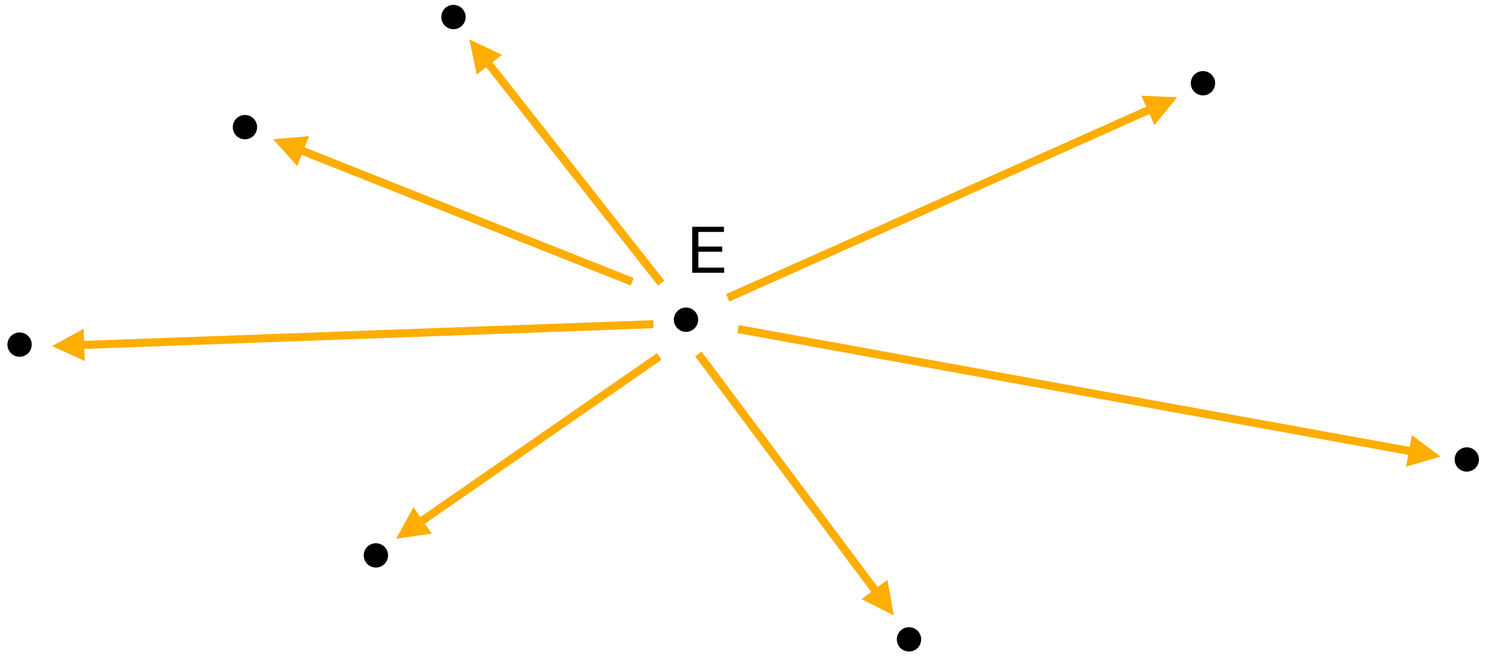


EUF–CMA of FS signature, assuming soundness assumption *given hints*

Aardal, Basso, De Feo, Patranabis, Wesolowski (2025)

SQIsign is EUF–CMA secure

assuming that, given



it's hard to find the endomorphism ring of E

(plus one technical assumption)

1

SQIsign has evolved a lot over the years, benefitting from the introduction of HD representations

2

But **SQIsign** is also reaching maturity, in terms of design and security assumptions

3

Much more work ahead:

- Better algorithms
- QROM security
- Constant-time implementation

SQIsign2D–West

https://ia.cr/2024/760

Security proof

https://ia.cr/2025/379

NIST spec

https://sqisign.org/spec/