SQIsign
past, present and future

Luca De Feo
IBM Research Zürich

April 28, 2025
The SQIparty, Lleida, Spain

What crypto from isogenies?

	Key exchange / Encryption	Identification / Signature	Other
Quadratic	Couveignes–Rostovtsev–Stolbunov CSIDH SCALLOP	SeaSign CSI-FiSh PEGASIS[1]	Threshold[2] PAKE …
Quaternionic	—	SQIsign SIDH-like signatures	Ring signatures Adaptor signatures …[3]
Ad hoc	SIDH † SIDH fixes FESTA	SIDH-like signatures	Time-release crypto …

[1] See P. Dartois' talk on Wednesday.
[2] See G. Borin's talk on Tuesday.
[3] See I. Radulescu's talk on Tuesday.

Zero-Knowledge Proofs of Knowledge

Prover

NP statement, witness

Verifier

NP statement

“OK, I believe you!”

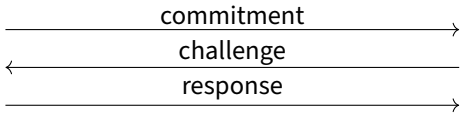
Zero-Knowledge Proofs of Knowledge

Prover

NP statement, witness

Verifier

NP statement



Σ-protocols

"OK, I believe you!"

Soundness: *"I really know the secret"*

Minimal definition: A prover with no knowledge of the secret only convinces the verifier with negligible probability.

Soundness: *"I really know the secret"*

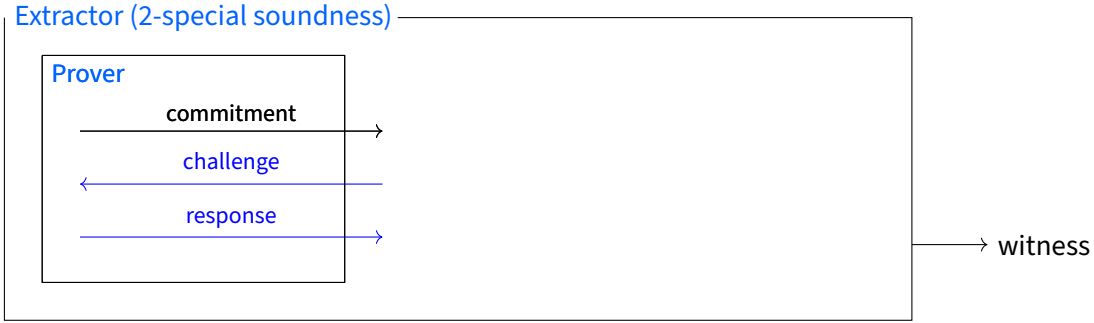
Minimal definition: A prover with no knowledge of the secret only convinces the verifier with negligible probability.

Extractor: An algorithm that extracts the witness by interacting repeatedly with the prover.

Soundness: *"I really know the secret"*

Minimal definition: A prover with no knowledge of the secret only convinces the verifier with negligible probability.

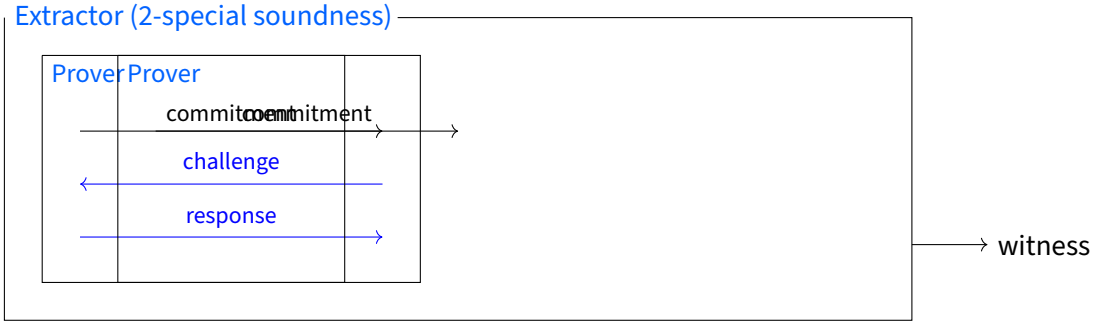
Extractor: An algorithm that extracts the witness by interacting repeatedly with the prover.



Soundness: *"I really know the secret"*

Minimal definition: A prover with no knowledge of the secret only convinces the verifier with negligible probability.

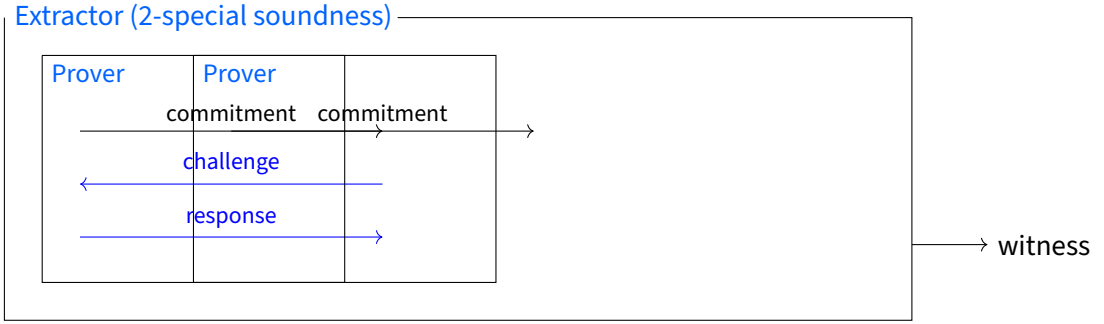
Extractor: An algorithm that extracts the witness by interacting repeatedly with the prover.



Soundness: *"I really know the secret"*

Minimal definition: A prover with no knowledge of the secret only convinces the verifier with negligible probability.

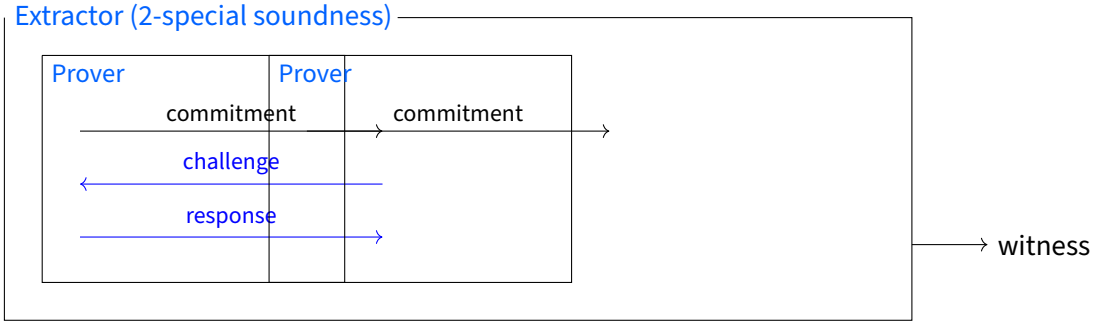
Extractor: An algorithm that extracts the witness by interacting repeatedly with the prover.



Soundness: *"I really know the secret"*

Minimal definition: A prover with no knowledge of the secret only convinces the verifier with negligible probability.

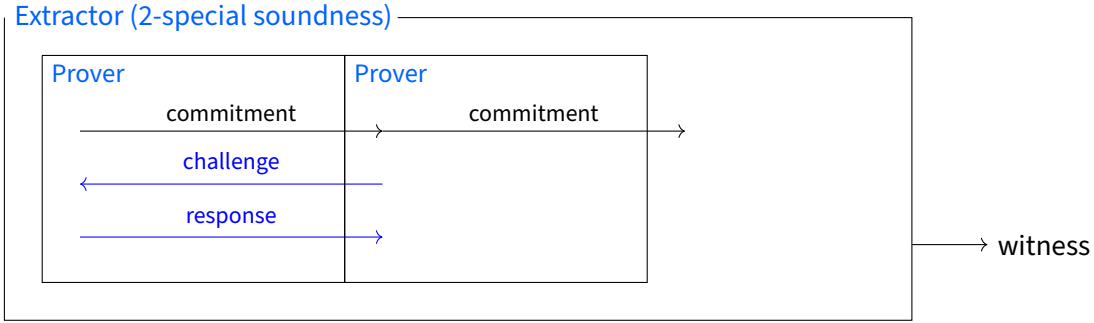
Extractor: An algorithm that extracts the witness by interacting repeatedly with the prover.



Soundness: *"I really know the secret"*

Minimal definition: A prover with no knowledge of the secret only convinces the verifier with negligible probability.

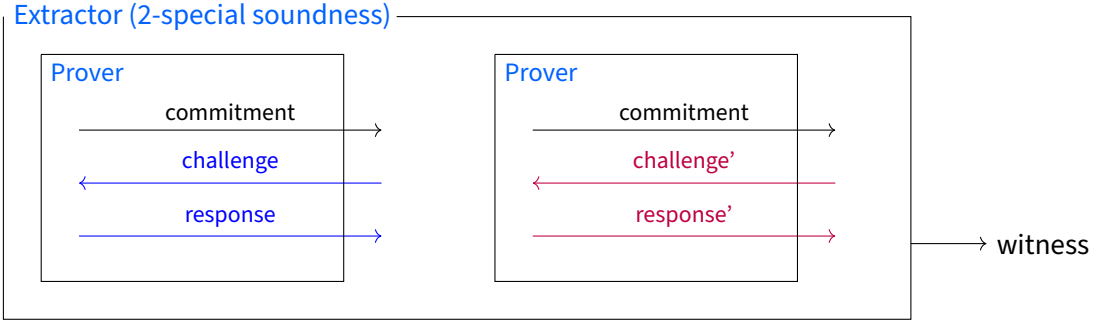
Extractor: An algorithm that extracts the witness by interacting repeatedly with the prover.



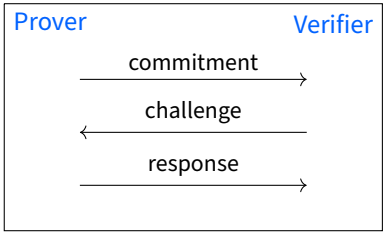
Soundness: *"I really know the secret"*

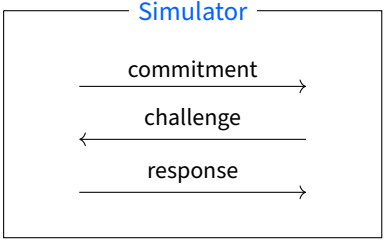
Minimal definition: A prover with no knowledge of the secret only convinces the verifier with negligible probability.

Extractor: An algorithm that extracts the witness by interacting repeatedly with the prover.



Zero-Knowledge: *“You learned nothing about the secret”*





How to Explain Zero-Knowledge Protocols to Your Children

QUISQUATER Jean-Jacques[1], *Myriam*, *Muriel*, *Michaël*
GUILLOU Louis[2], *Marie Annick*, *Gaïd*, *Anna*, *Gwenolé*, *Soazig*
in collaboration with *Tom BERSON*[3] for the English version

[1] Philips Research Laboratory, Avenue Van Becelaere, 2, B–1170 Brussels, Belgium.
[2] CCETT/EPT, BP 59, F–35512 Cesson Sévigné, France.
[3] Anagram Laboratories, P.O. Box 791, Palo Alto CA 94301, USA.

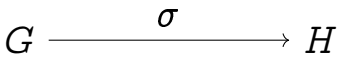
The Strange Cave of Ali Baba

◇ Know, oh my children, that very long ago, in the Eastern city of Baghdad, there lived an old man named Ali Baba. Every day Ali Baba would go to the bazaar to buy or sell things. This is a story which is partly about Ali Baba, and partly also about a cave, a strange cave whose secret and wonder exist to this day. But I get ahead of myself ...

One day in the Baghdad bazaar a thief grabbed a purse from Ali Baba who right away started to run after him. The thief fled into a cave whose entryway forked into two dark winding passages: one to the left and the other to the right (The Entry of the Cave).

Ali Baba did not see which passage the thief ran into. Ali Baba had to choose which way to go, and he decided to go to the left. The left-hand passage ended in a dead end. Ali Baba searched all the way from the fork to the dead end, but he did not find the thief. Ali Baba said to himself that the thief was perhaps in the other passage. So he searched the right-hand passage, which also came to a dead end. But again he did not find the thief. "This cave is pretty strange," said Ali Baba to himself, "Where has my thief gone?"

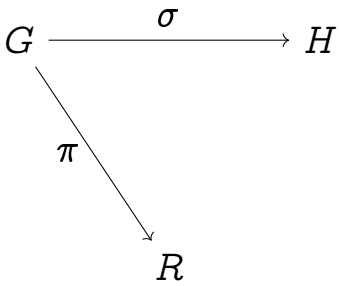
A ZK-PoK for Graph Isomorphism (after Goldwasser–Micali–Rackoff)



Prover

Verifier

A ZK-PoK for Graph Isomorphism (after Goldwasser–Micali–Rackoff)



Prover

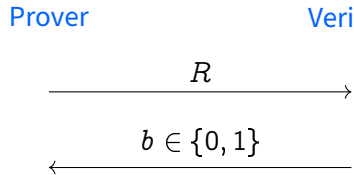
Verifier

R

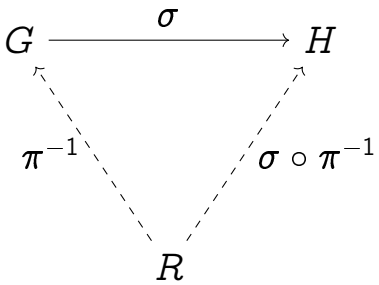
A ZK-PoK for Graph Isomorphism (after Goldwasser–Micali–Rackoff)

$$G \xrightarrow{\sigma} H$$

$$R$$



A ZK-PoK for Graph Isomorphism (after Goldwasser–Micali–Rackoff)



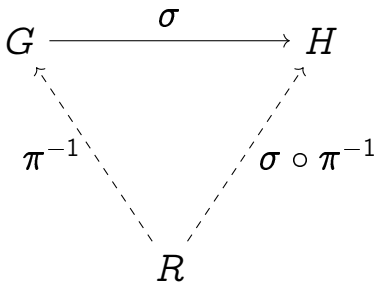
Prover Verifier

R

$b \in \{0, 1\}$

$\sigma^b \circ \pi^{-1}$

The “Group Action” point of view



- “Public” set: $G, H, R \in \mathcal{S}$
- “Private” group: $\pi, \sigma \in \mathcal{G}$
- Group action: $\mathcal{G} \circlearrowright \mathcal{S}$

More on group actions

Protocols:

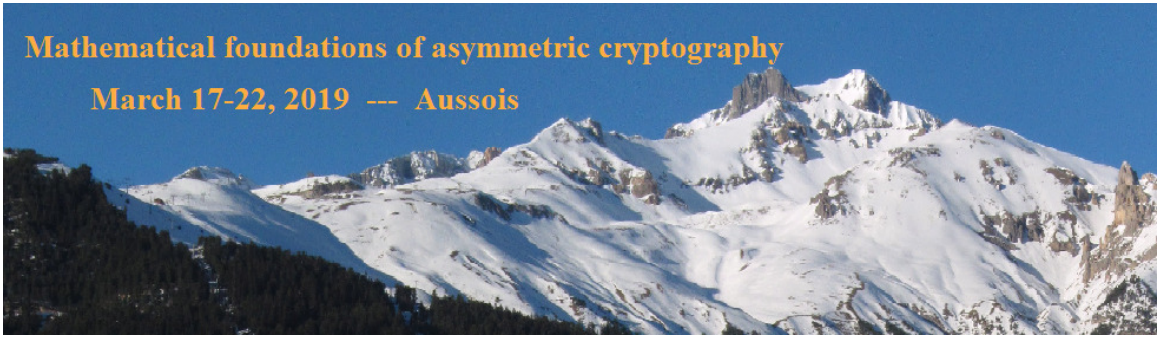
- Giacomo Borin
  — *Threshold signatures from different group actions*

Instantiations:

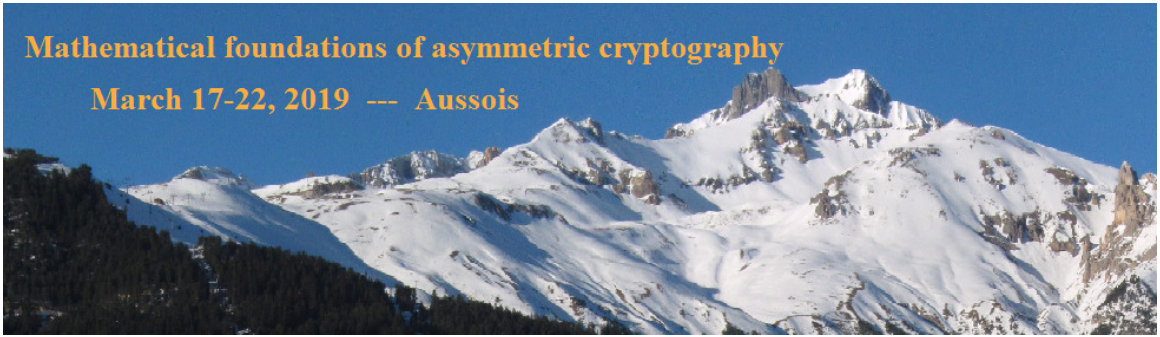
- Marc Houben
  — *A Montgomery-ladder for isogenies*
- Pierrick Dartois
  — *PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies*
- Eli Orvis
  — *Generalized class group actions via class field theory*

The birth of SQIsign

The birth of SQIsign



The birth of SQIsign



the Short Quaternion and Isogeny signature

De Feo, Kohel, Leroux, Petit, Wesolowski — Asiacrypt 2020

Endomorphism ring	Maximal order
Isogeny	Ideal
$\mathrm{Hom}(E, E')$	Ideal class
Degree	Norm

More on correspondences

Algorithms for the Deuring correspondence:

- Jordi Pujolàs
  — *On prime degree twisting endomorphisms of supersingular elliptic curves*

Higher dimensions:

- Enric Florit
  — *Quaternionic multiplication and abelian fourfolds*
- Péter Kutas
  — *Biquaternion cryptography*

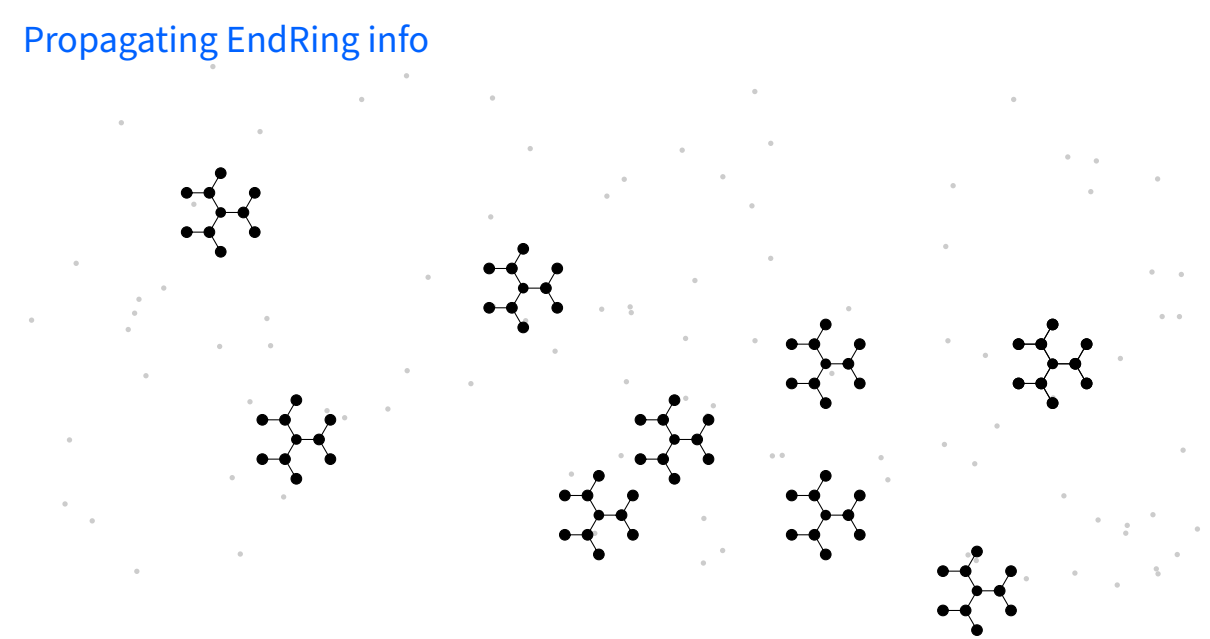
Other kinds:

- Harun Kir
  — *Exploring Kani's Research*
- Chloe Martindale
  — *Hidden geometry in supersingular isogeny graphs*

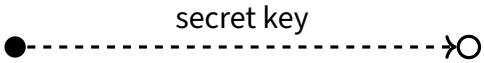
Propagating EndRing info

Propagating EndRing info

Propagating EndRing info

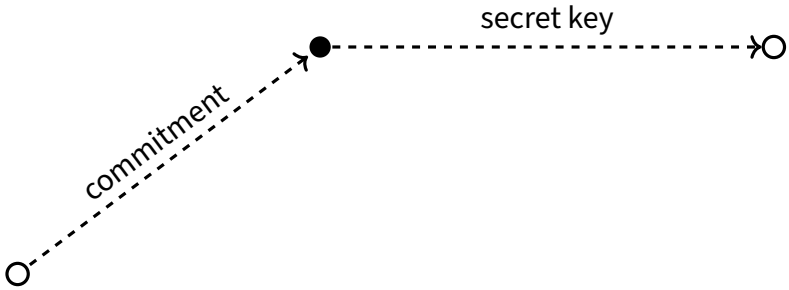


SQIsign



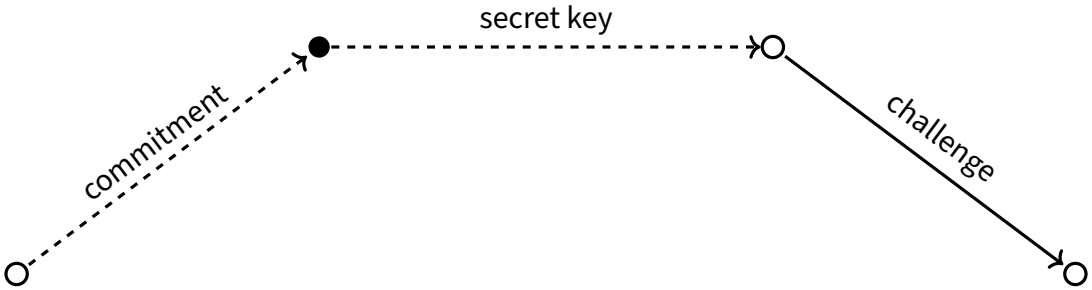
Legend: Known EndRing — public isogeny - - - - secret isogeny/ideal

SQIsign



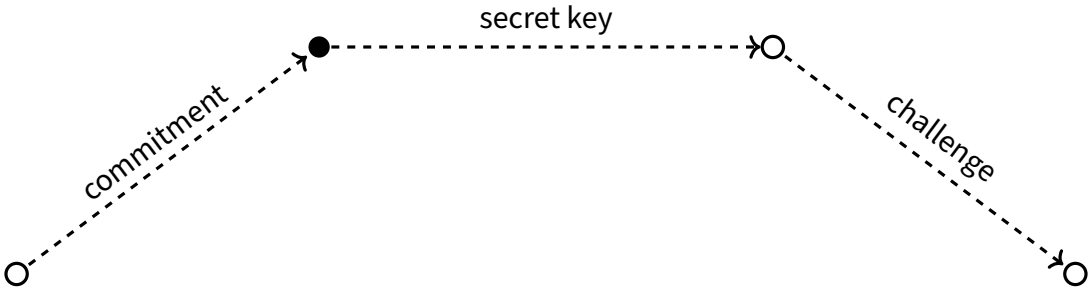
Legend: Known EndRing — public isogeny - - - secret isogeny/ideal

SQIsign



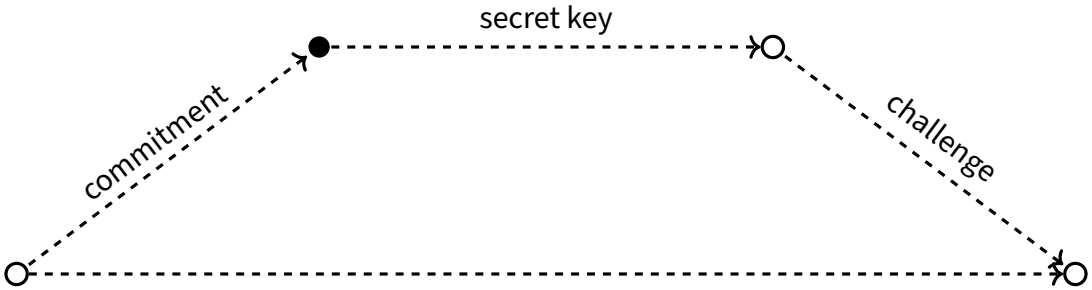
Legend: Known EndRing — public isogeny - - - secret isogeny/ideal

SQIsign



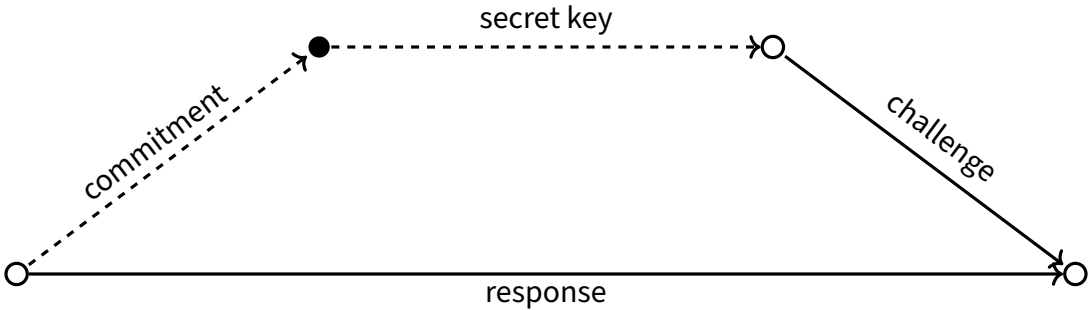
Legend: Known EndRing — public isogeny - - - secret isogeny/ideal

SQIsign



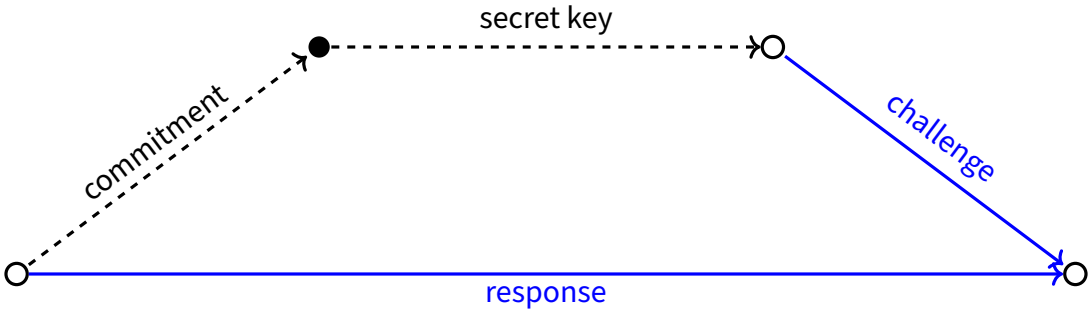
Legend: Known EndRing — public isogeny - - - secret isogeny/ideal

SQIsign



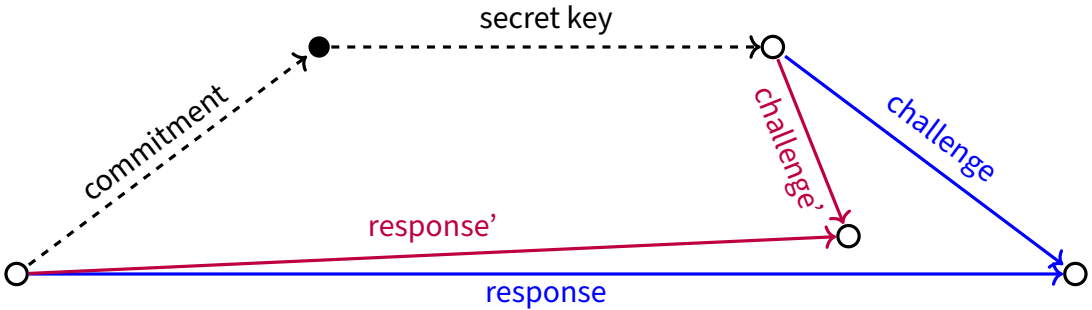
Legend: Known EndRing — public isogeny - - - secret isogeny/ideal

2-special soudness → OneEnd



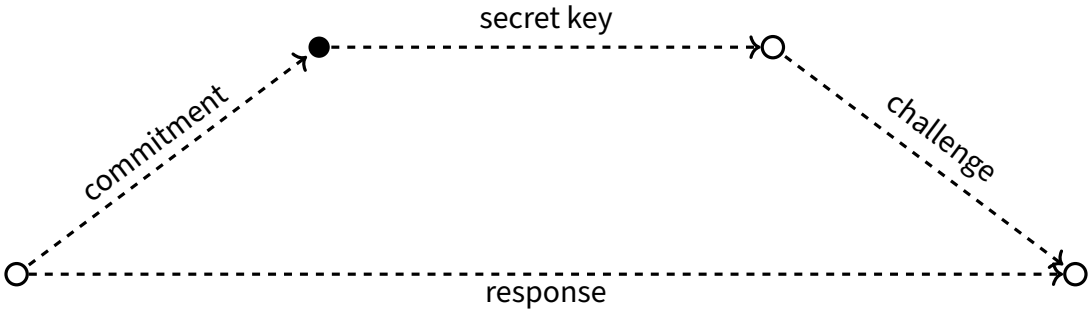
Legend: Known EndRing — public isogeny - - - secret isogeny/ideal

2-special soudness → OneEnd



Legend: Known EndRing — public isogeny - - - secret isogeny/ideal

What response?



SQIsigning like it’s the 80s

KLPT: translating quaternion ideals to smooth degree isogenies

Kohel, Lauter, Petit, Tignol (2014)

Input: a left ideal class of a special maximal order

Output: a unique representative of norm a power of 2

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

Input: a left ideal class of an arbitrary maximal order

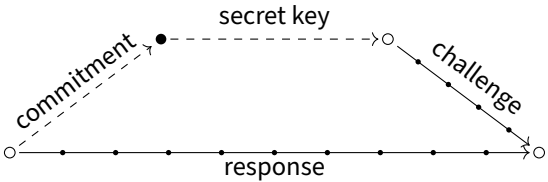
Output: a sort of random looking representative of norm a power of 2

Performance of SQIsign v1 (June 2023)

Bytes		Mcycles			
Public Key	Signature	Keygen	Sign	Verify	Security
64	177	3,728	5,779	108	NIST-1
96	263	23,734	43,760	654	NIST-3
128	335	91,049	158,544	2,177	NIST-5

Zero-Knowledge

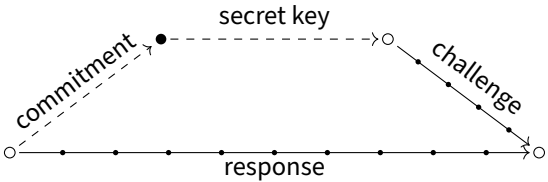
Real transcript:



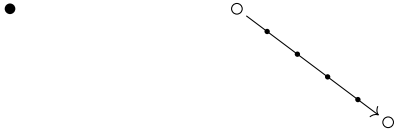
Simulated transcript:

Zero-Knowledge

Real transcript:

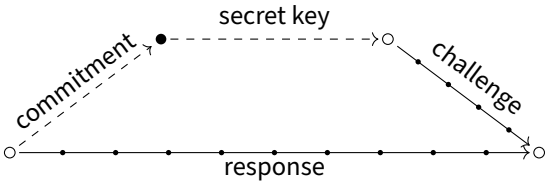


Simulated transcript:

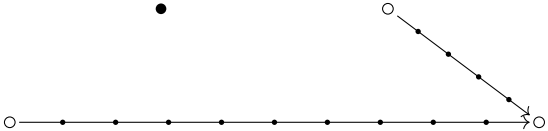


Zero-Knowledge

Real transcript:

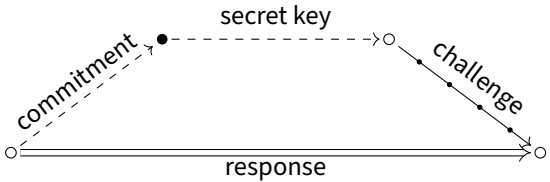


Simulated transcript:



Modern SQIsigning

SQIsignHD (Dartois, Leroux, Robert, Wesolowski 2023)



- Response encoded by interpolation points,
- Evaluate using 4D isogeny formulas,
- $++$ Fast signing,
- $++$ Shorter responses,
- $--$ Slow verification.

SQIsign2D (Basso, Dartois, De Feo, Leroux, Maino, Nakagawa, Onuki, Pope, Robert, Wesolowski 2023)

- Move from 4D to 2D isogeny representations.
- $++$ Fast signing,
- $++$ Shorter responses,
- $++$ Fast verification.

More on higher-dimensional isogenies

Translating ideals to isogenies

- Jonathan Komada Eriksen
  — *Translating ideals to isogenies*

Theta structures and isogenies:

- Maria Corte-Real Santos
  — *Computing two-dimensional isogenies for SQIsign*
- Max Duparc
  — *A Combinatorial Perspective on Theta Structures*
- Antoine Dequay
  — *Algorithms for moduli space of abelian varieties with level structure*

More variants of SQIsign:

- Hiroshi Onuki
  — *SQIsign2DPush*

Other topics

Better pairing computations:

- Alessandro Sferlazza
  — *Montgomery ladders already compute pairings*

Abstracting SQIsign for cryptography:

- Ilinca Radulescu
  — *Cryptographic Categories*

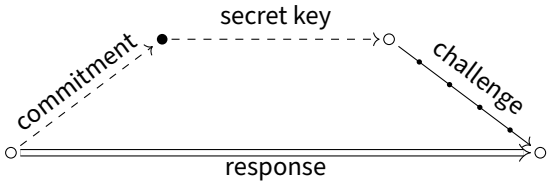
Performance of SQIsign v2 (February 2025)

Bytes		Mcycles			
Public Key	Signature	Keygen	Sign	Verify	Security
66	148	84	203	11	NIST-1
98	222	228	549	31	NIST-3
130	294	403	1021	62	NIST-5

More on performance and platform-specific implementations:

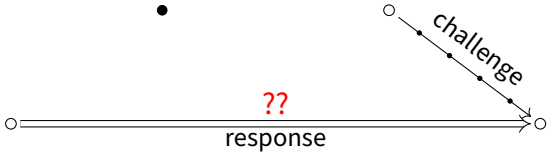
- Benjamin Smith
  — *Post-quantum signatures in practice: securing IoT software updates*
- Décio Gazzoni Filho
  — *Speeding up SQIsign verification on the ARM Cortex-M4*

Zero-knowledge



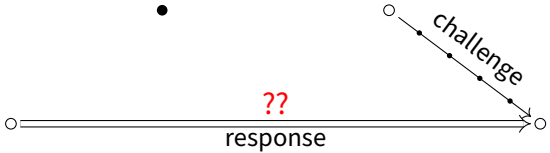
- HD response encoded by interpolation points

Zero-knowledge



- HD response encoded by interpolation points
- How to evaluate large degree isogenies without EndRing?
- *Ad-hoc* fix: give a magic box to simulator.

Zero-knowledge



- HD response encoded by interpolation points
- How to evaluate large degree isogenies without EndRing?
- *Ad-hoc* fix: give a magic box to simulator.
- Recent progress: Aardal, Basso, De Feo, Patranabis, Wesolowski (eprint 2025/379)

The future

Todos:

- Systematic analysis of variants
- Hardware accelerations

Challenges:

- Better security proof
- Constant time algorithms
- SQIsign needs stability

Looks tough:

- Meaningfully faster signatures

One may always dream:

- Meaningfully faster verification
- Better 1D SQIsign