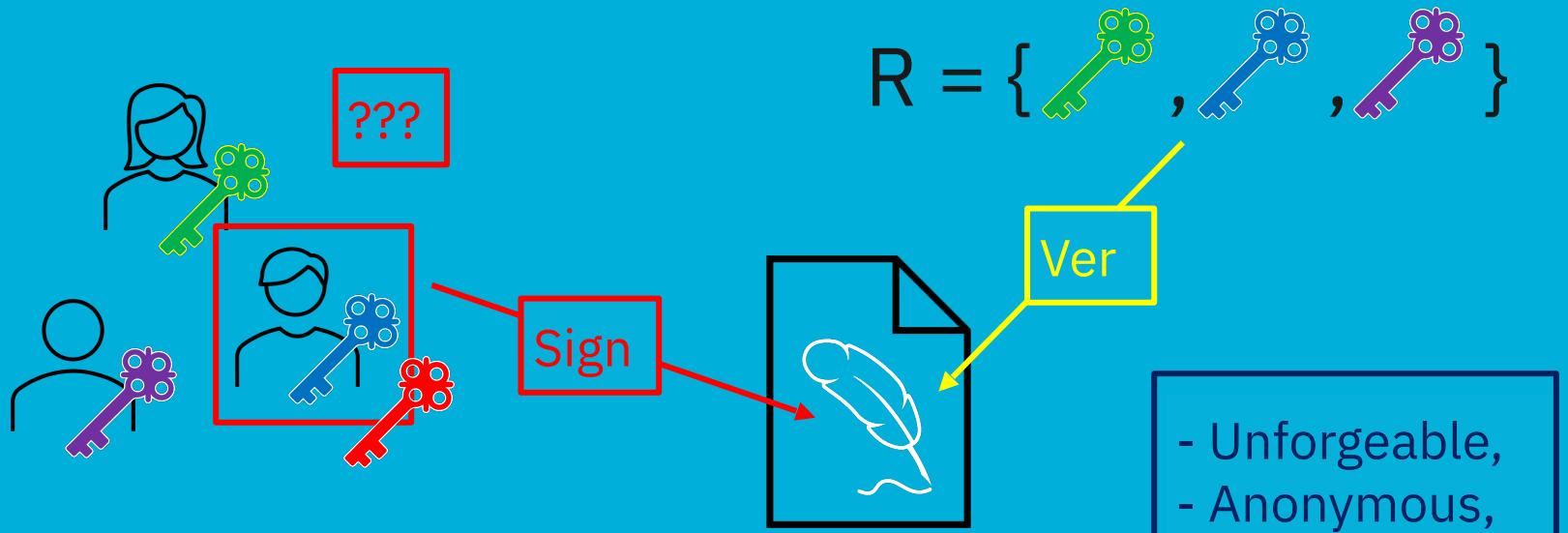
Erebor & Durian

Full Anonymous Ring Signatures from Quaternions and Isogenies

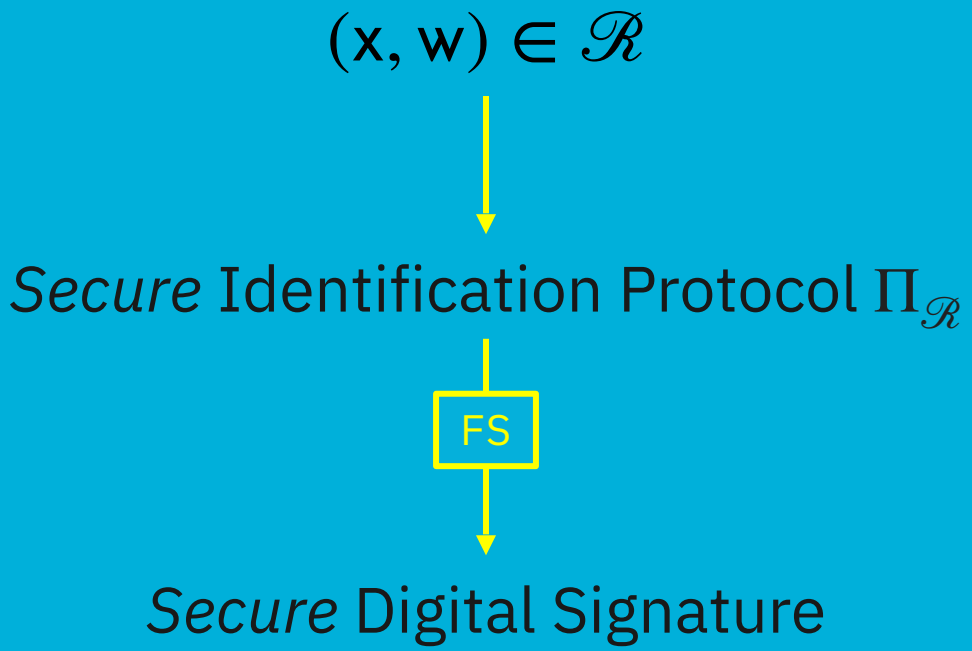
Giacomo Borin, YiFu Lai, Antonin Leroux

Opinions are my own!

Full-Anonymous
Linear
Ring Signatures



Full-Anonymous Linear **Ring Signatures**



Full-Anonymous Linear **Ring Signatures**

$$\mathcal{R}_{\mathrm{OR}} = \left\{((i, \mathrm{w}), (\mathrm{x}_1, \ldots, \mathrm{x}_N)) \mid (\mathrm{w}, \mathrm{x}_i) \in \mathcal{R}\right\}$$

Secure OR-Proof for $\mathcal{R}_{OR}$

Secure Ring Signature

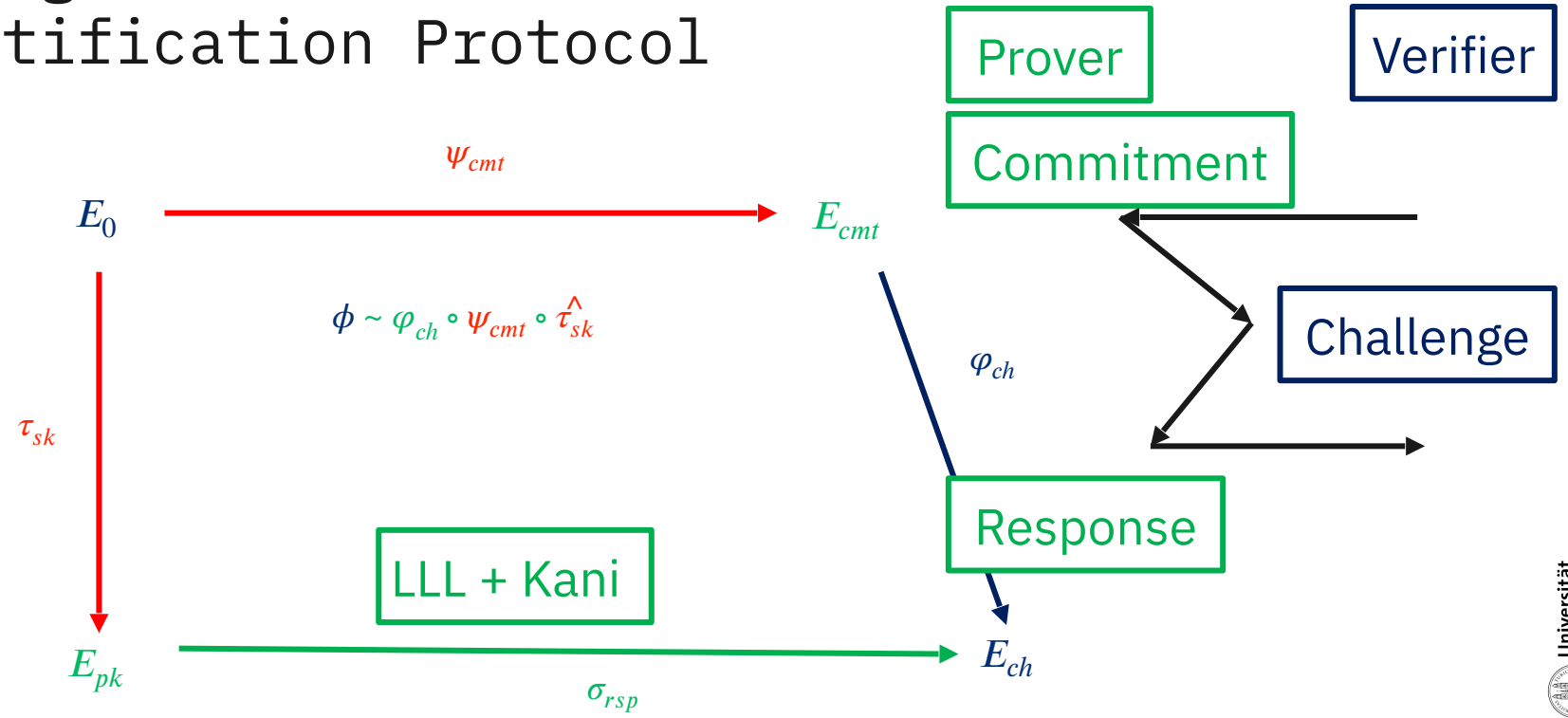
- Sequential,
- Parallel,
- Logarithmic

...

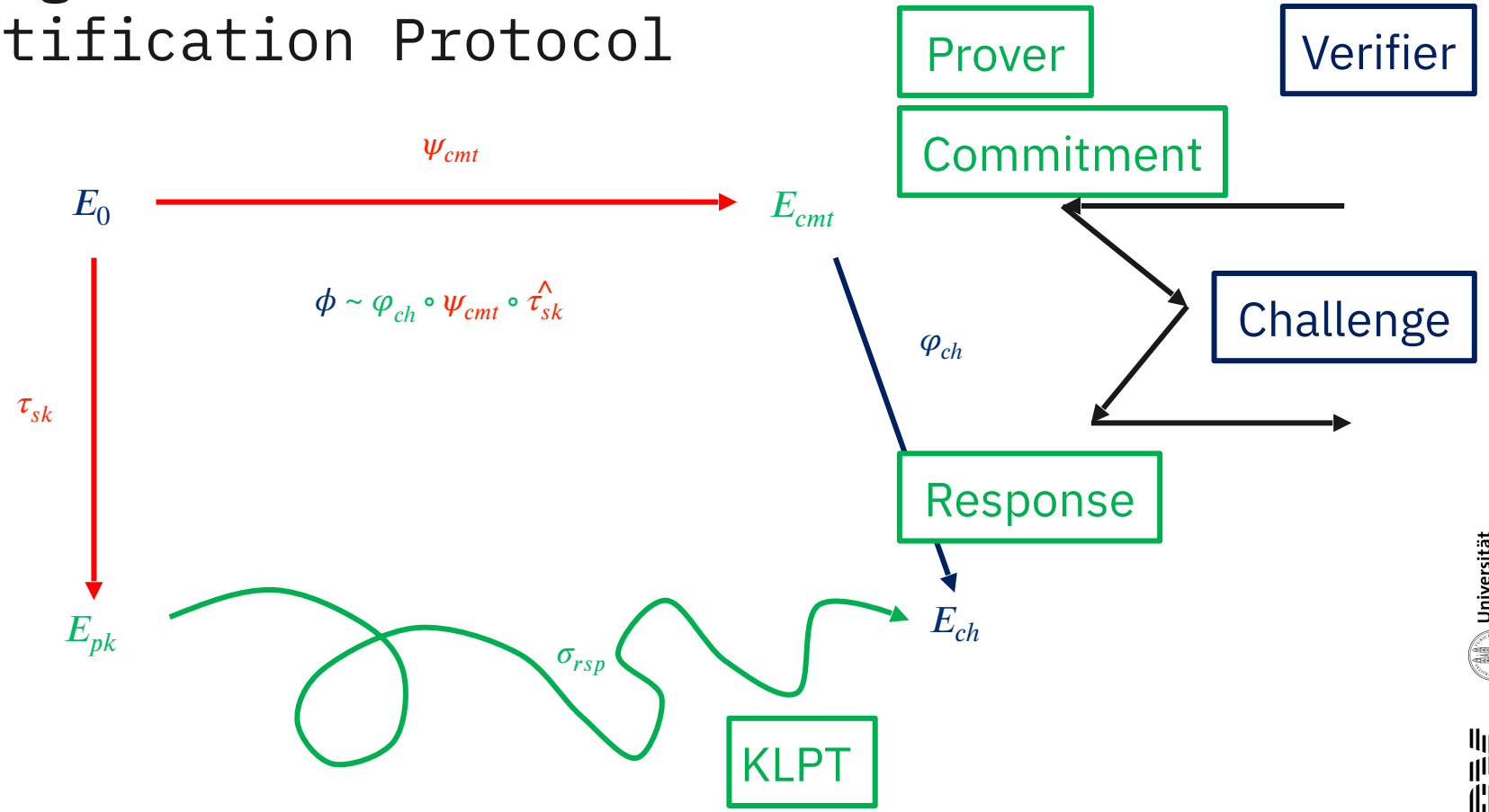
Sequential OR-Proofs

- Framework: **A**be, Masayuki, Miyako **O**hkubo, and Koutarou **S**uzuki. "1-out-of-n signatures from a variety of keys."
- Requires: Sigma Protocol Simulatable in PPT, with Special Honest-Verifier Zero Knowledge property.

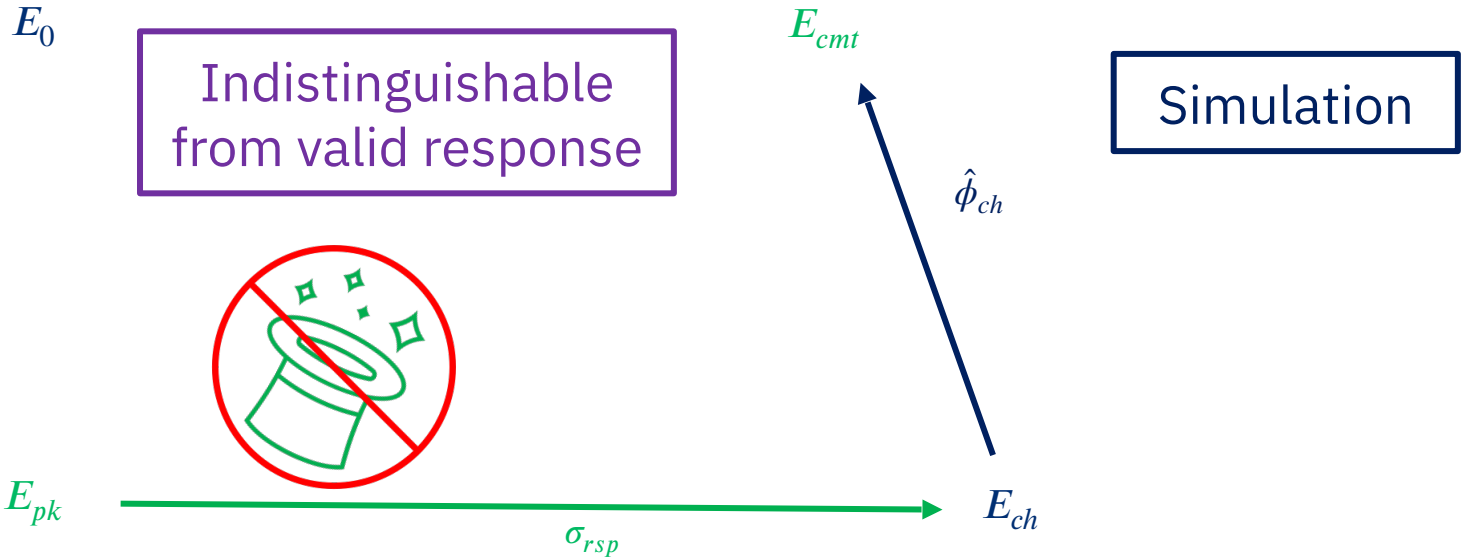
SQISign Identification Protocol



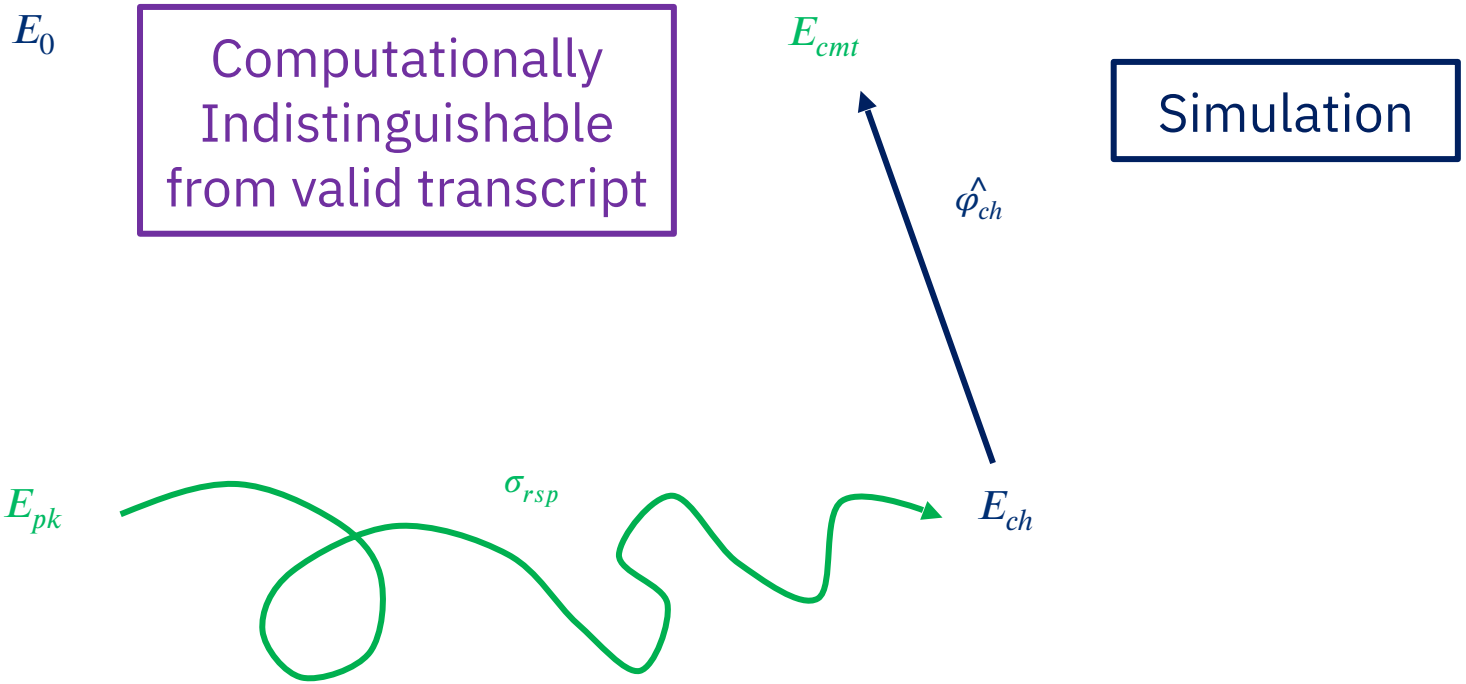
SQISign Identification Protocol



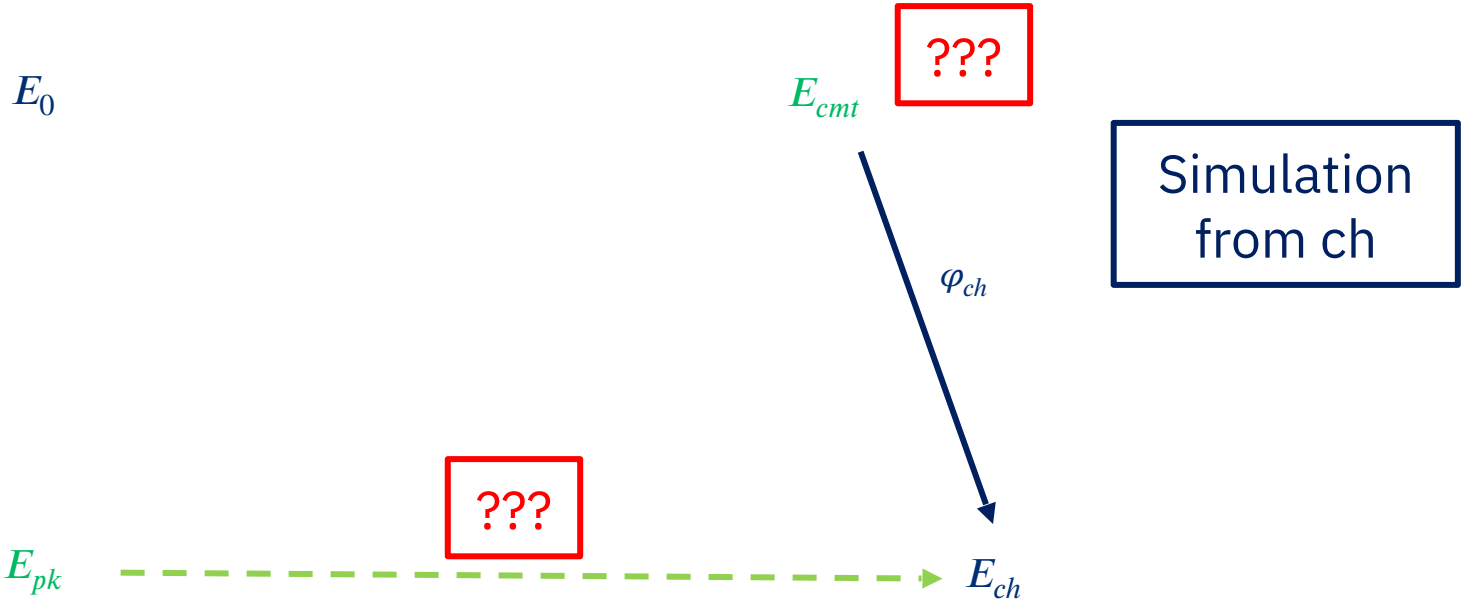
SQISign-HD
HVZK



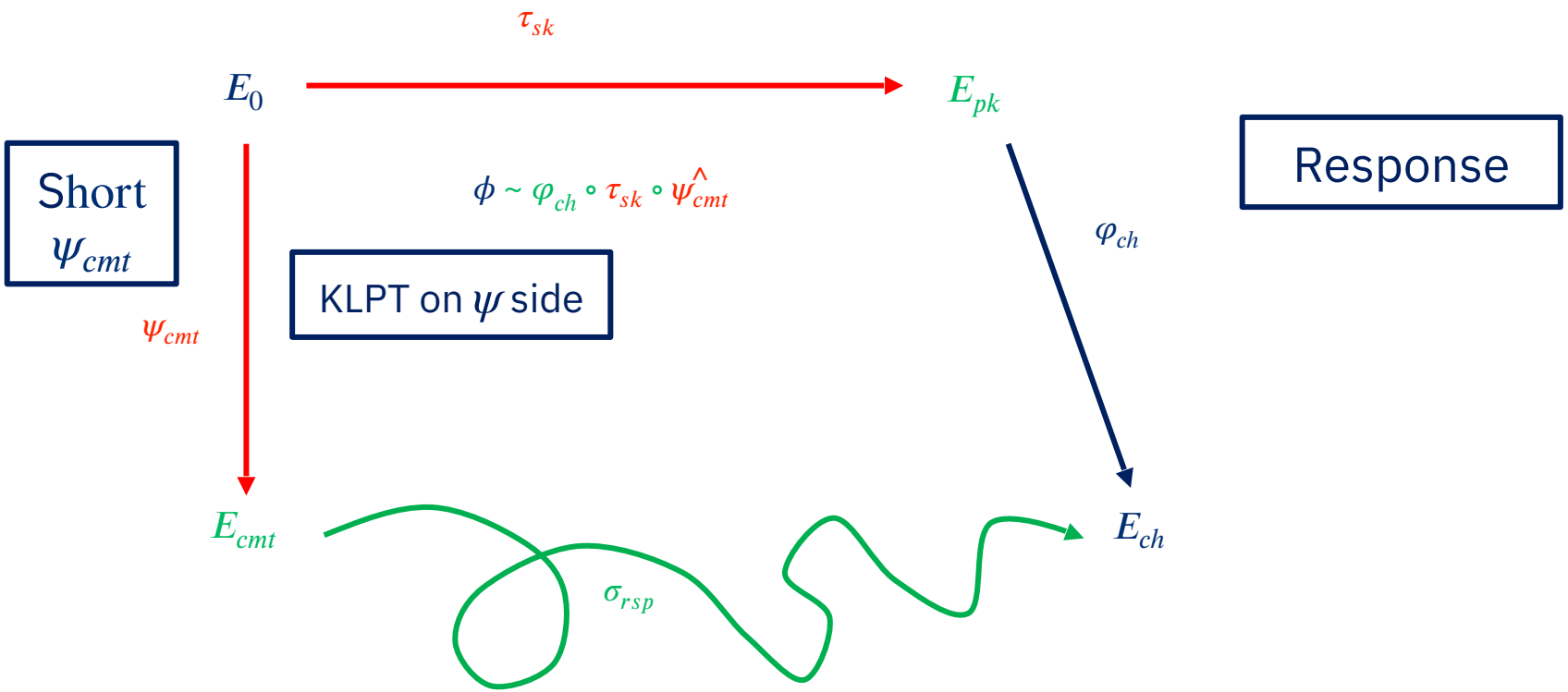
SQISign-KLPT
HVZK



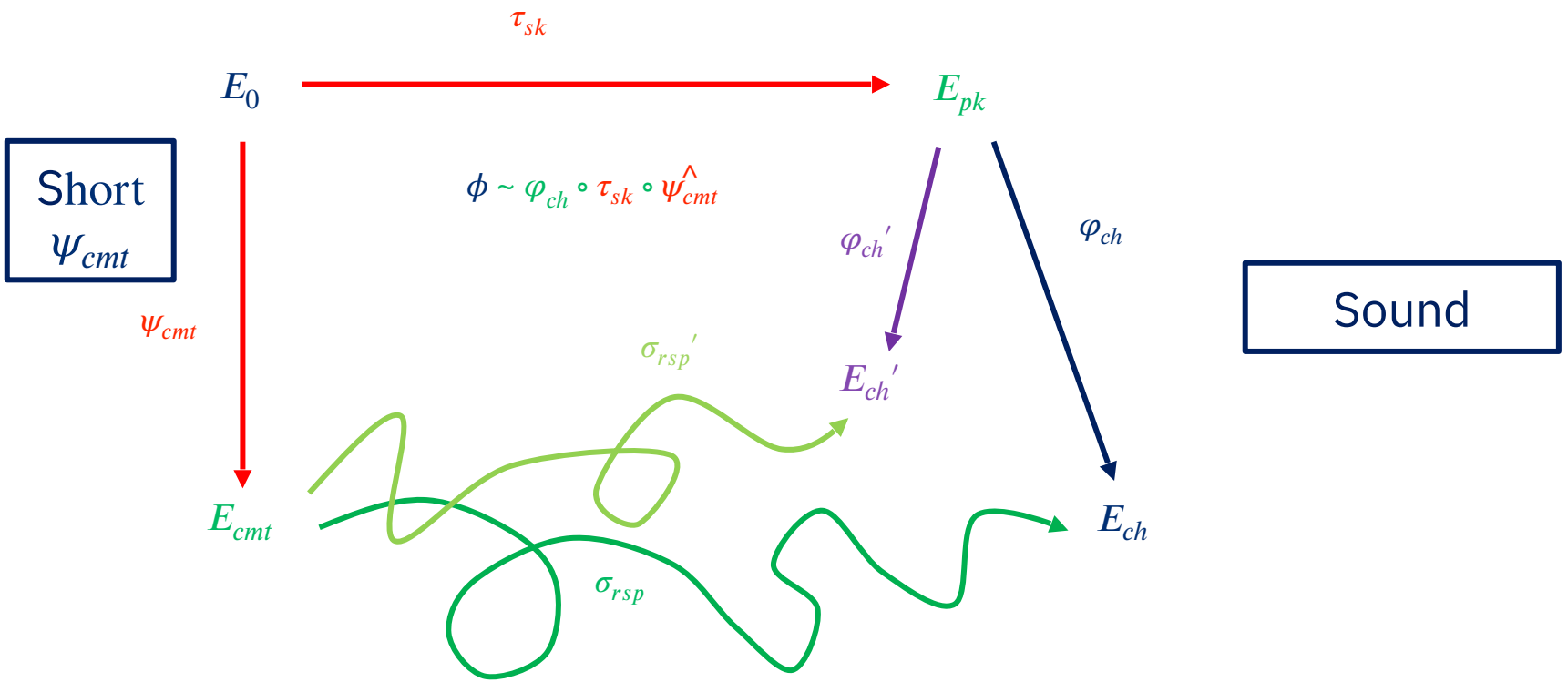
SQISign
Special HVZK



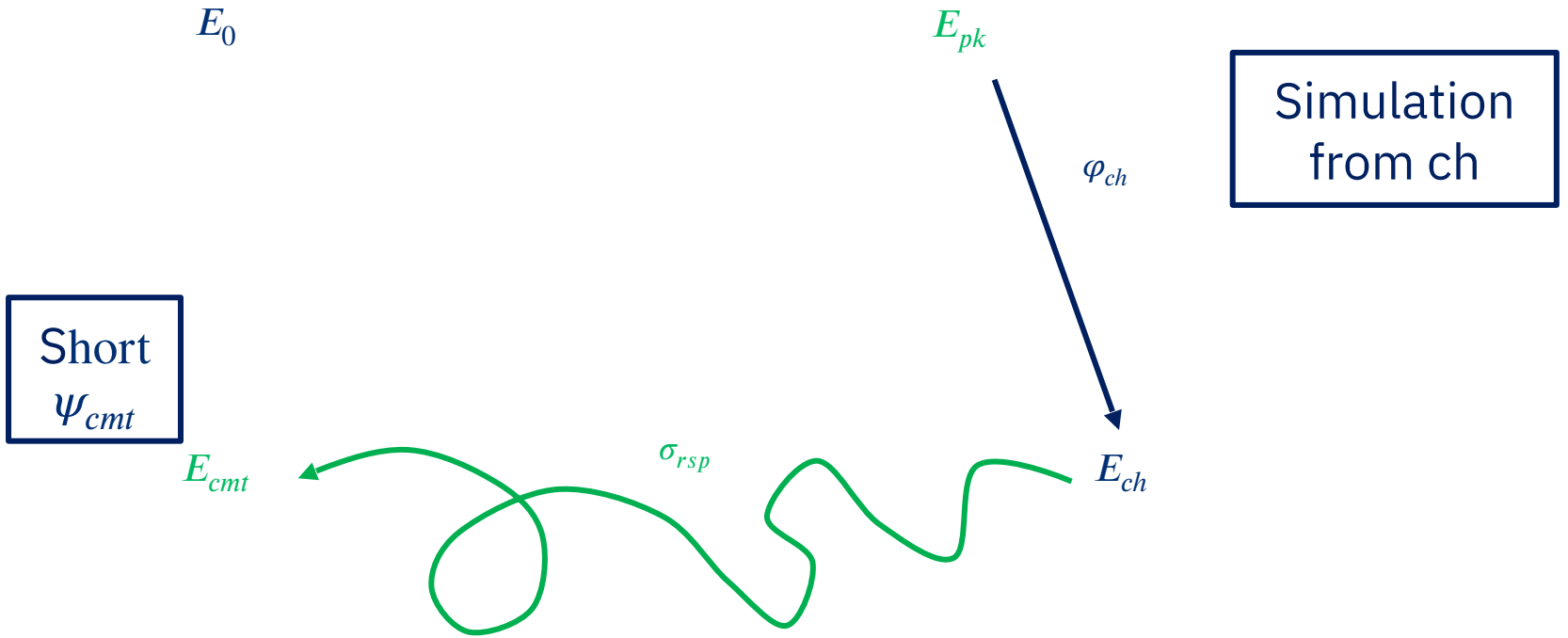
SQISign Modification



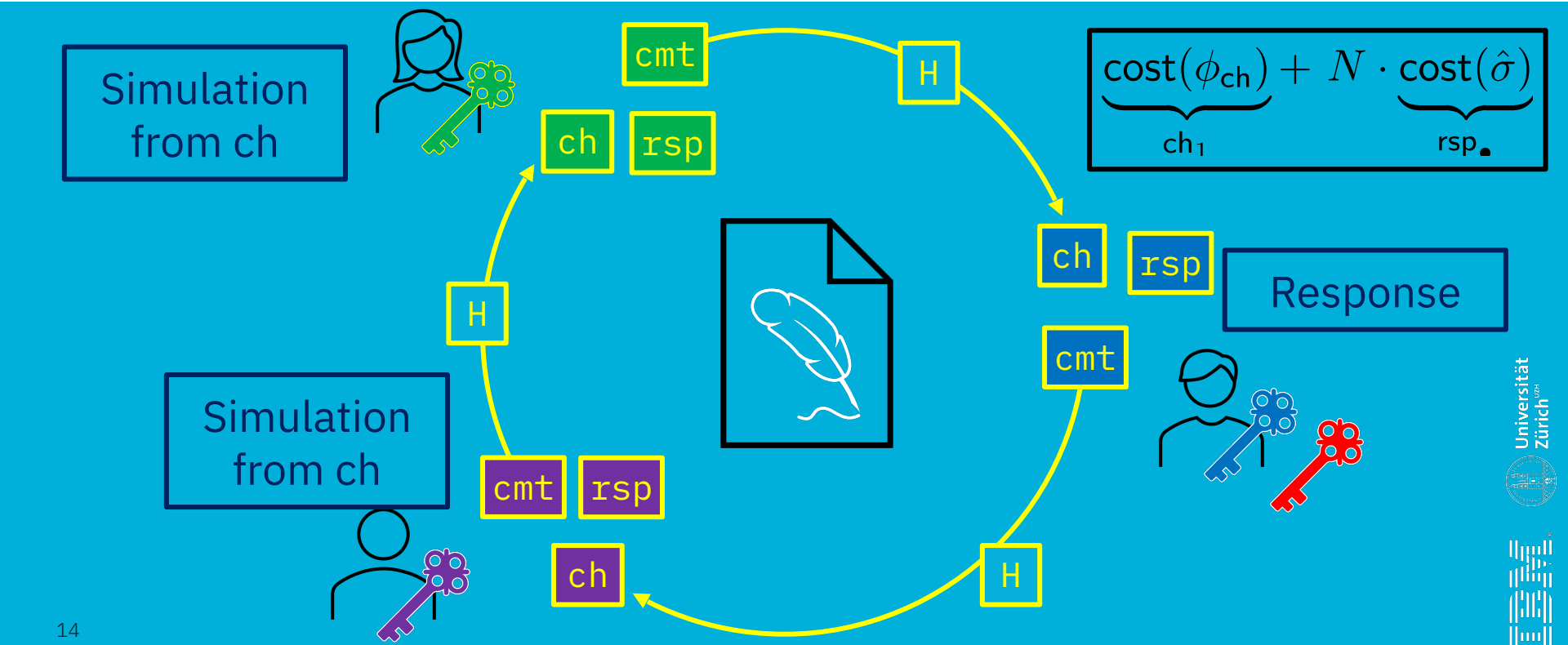
SQISign Modification



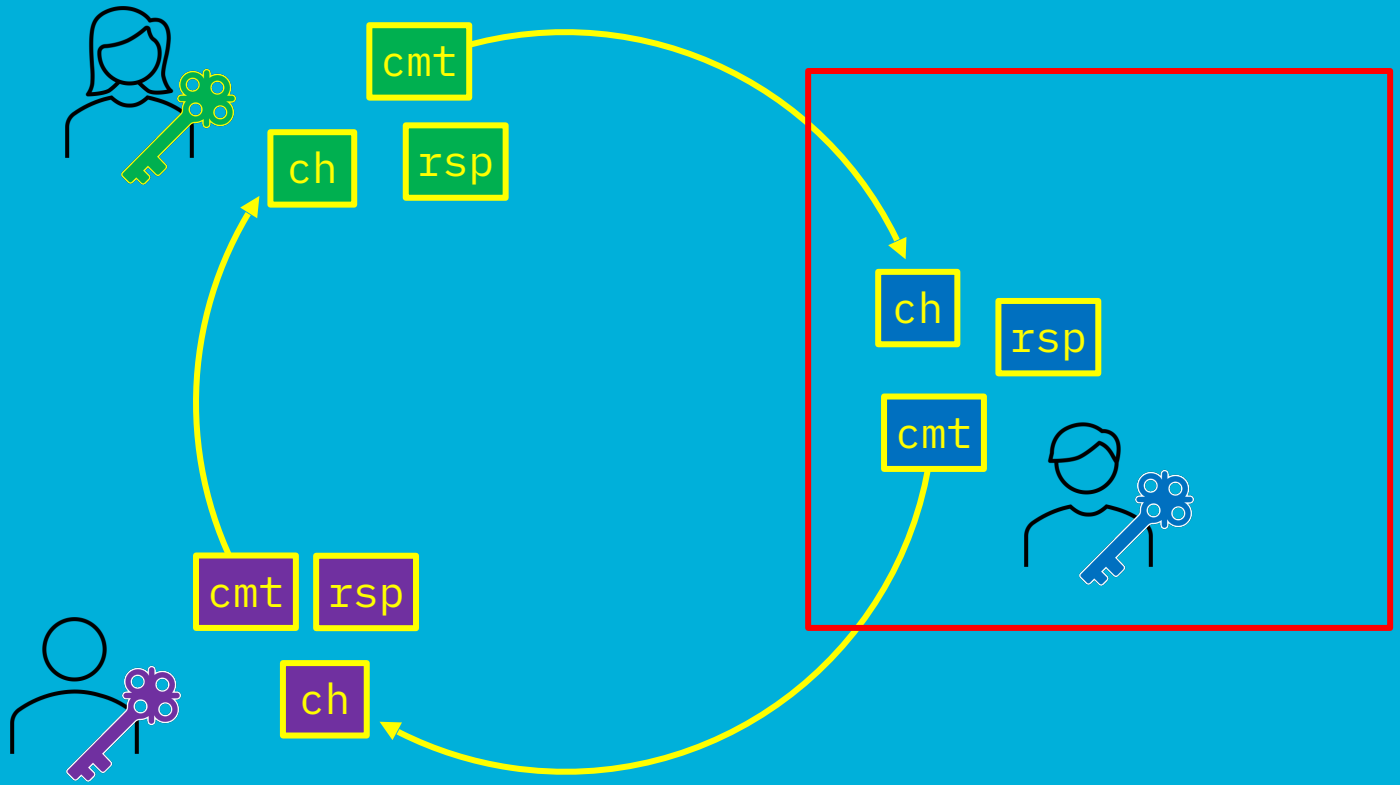
SQISign
Special HVZK



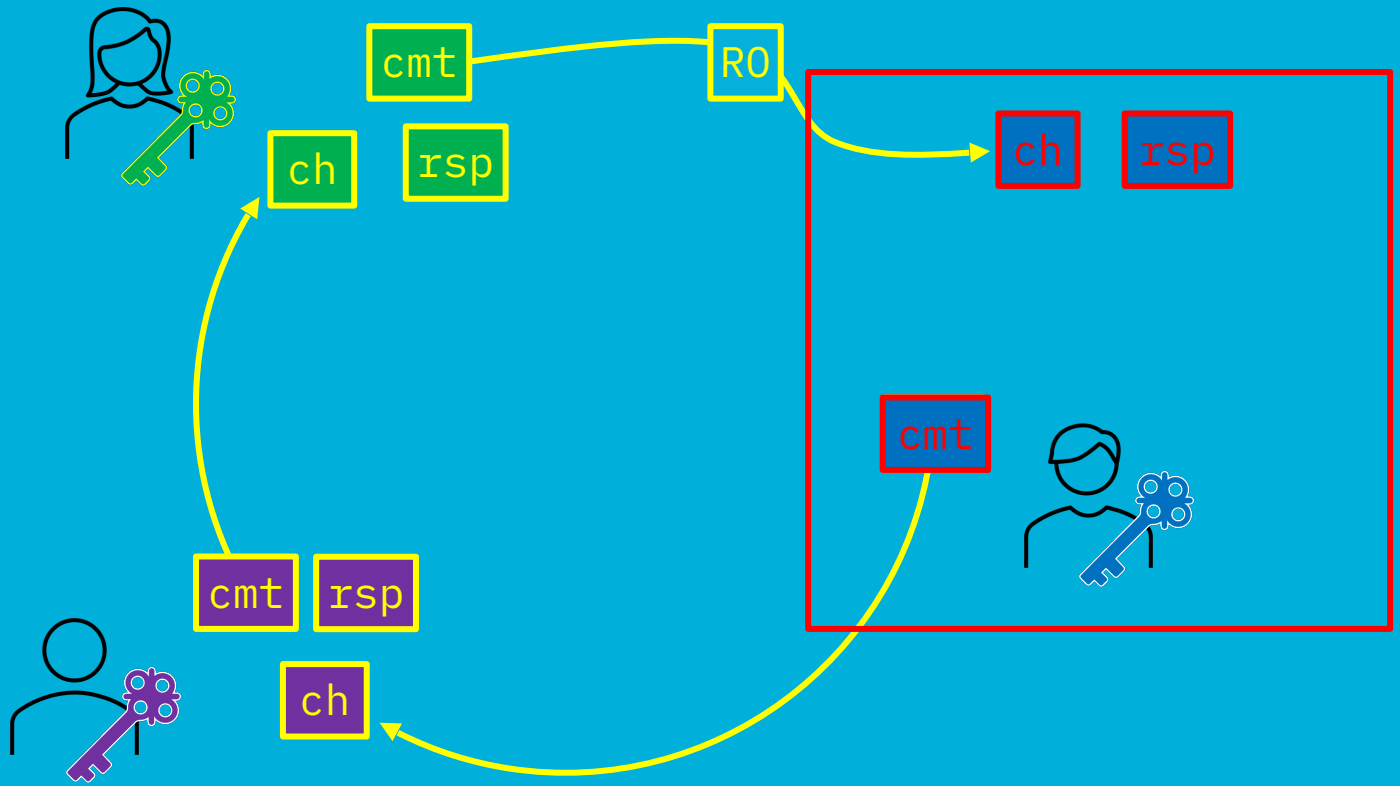
Full-Anonymous **Linear** Ring Signatures



Soundness & weak HVZK → Security against impersonation → Unforgeability

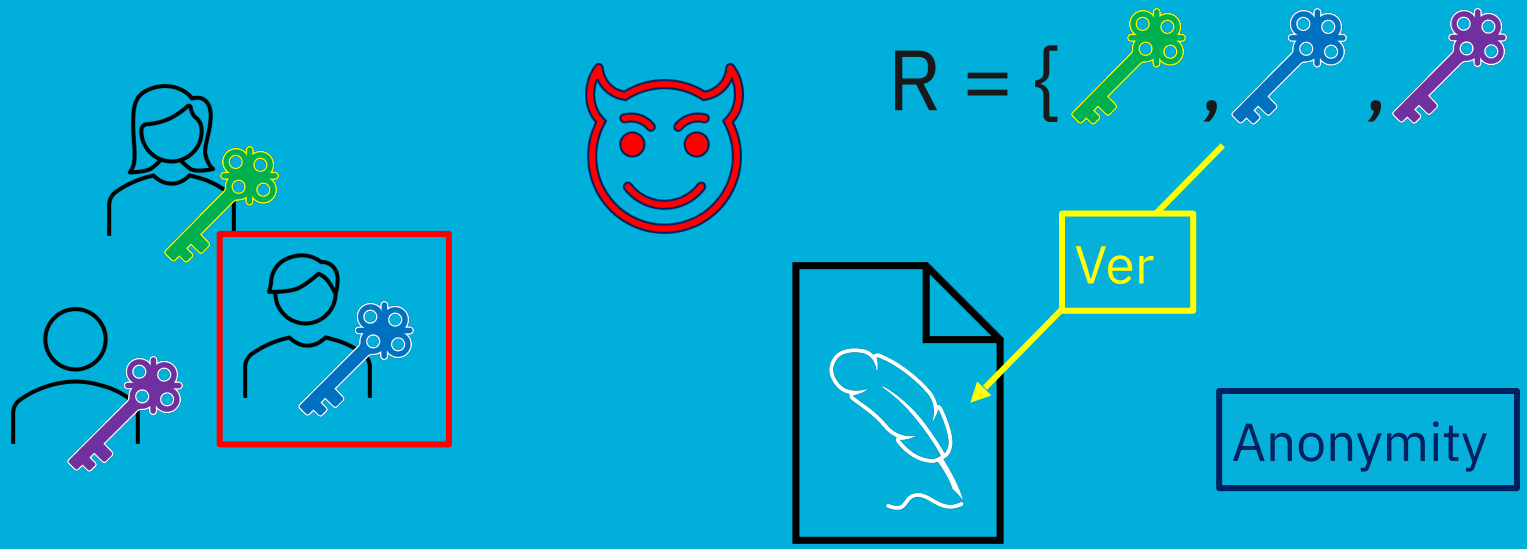


Soundness & weak HVZK → Security against impersonation → Unforgeability



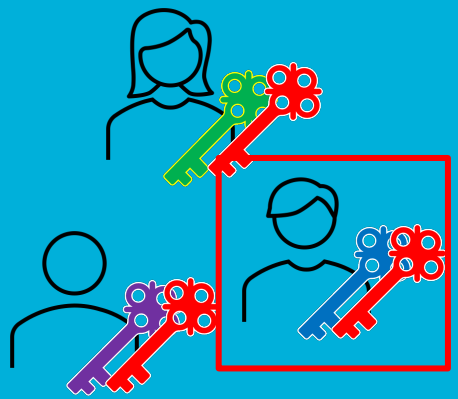
Full-Anonymous

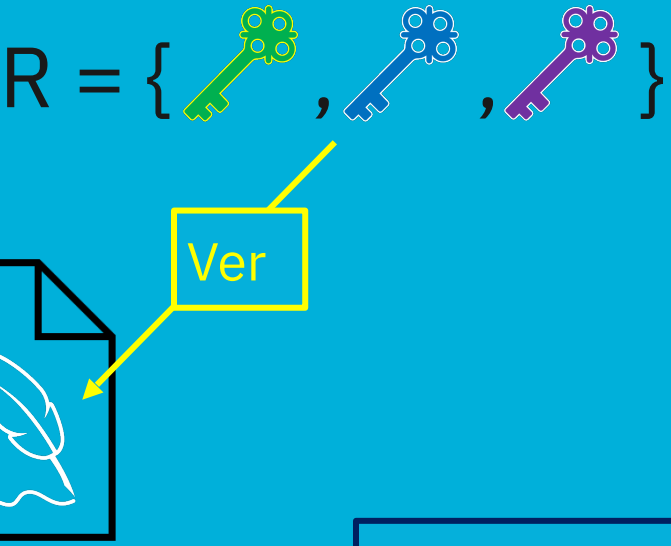
Linear
Ring Signatures



Full-Anonymous

Linear
Ring Signatures





Full Anonymity

Full-Anonymous Linear Ring Signatures

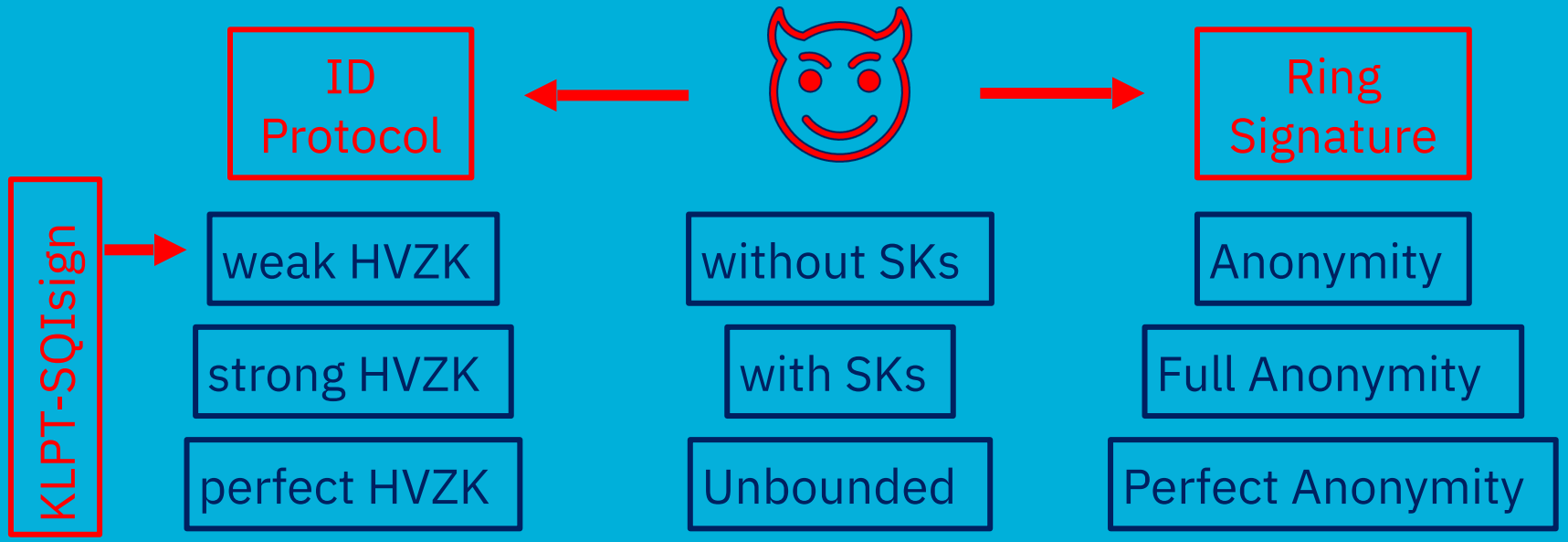
Relevant for:

- Designated Verifier Signatures;
- Deniable Key Exchanges;
- Deniable AKEM;

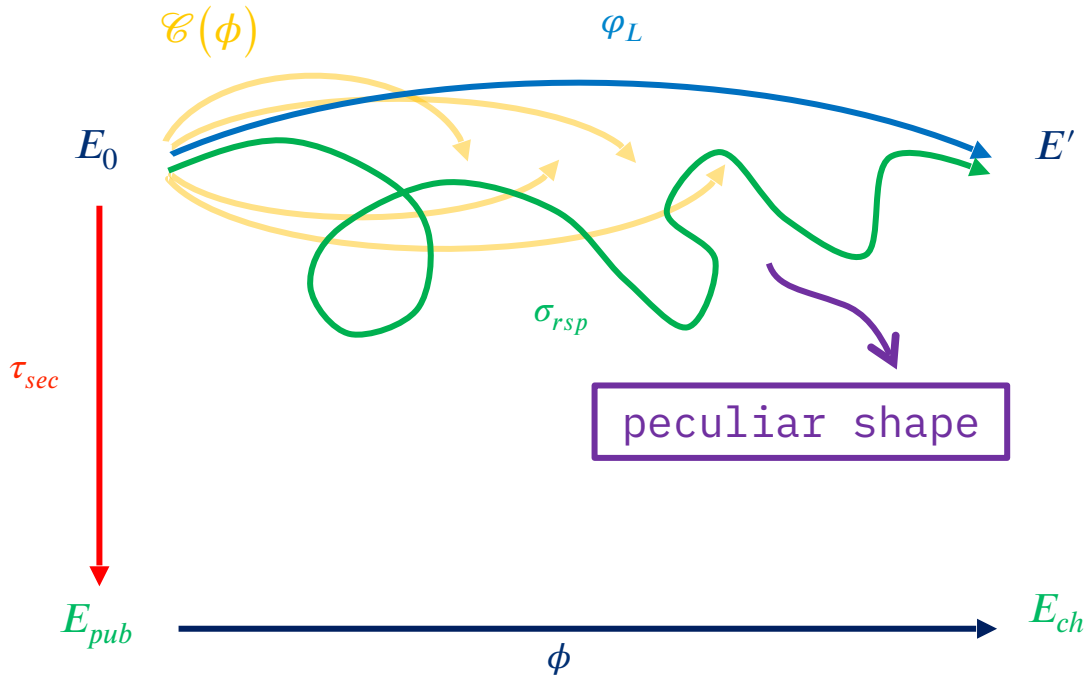
Some References:

- *Phillip Gajland, Jonas Janneck, and Eike Kiltz*. Ring signatures for deniable AKEM: Gandalf's fellowship.
- *Keitaro Hashimoto, Shuichi Katsumata, Kris Kwiatkowski, and Thomas Prest*. An efficient and generic construction for Signal's handshake(X3DH): Post-quantum, state leakage secure, and deniable.
- *Jacqueline Brendel, Rune Fiedler, Felix Günther, Christian Janson, and Douglas Stebila*. Post-quantum asynchronous deniable key exchange and the Signal handshake

Full-Anonymous
Linear
Ring Signatures



KLPT machinery



Geometric World

Supersingular Curves

Isogenies

Endormorphisms

Deuring Correspondence

$$i^2 = -1$$
$$j^2 = -p$$
$$ij = -ji$$

Quaternion World

Geometric World

Maximal Orders in the Algebra

Ideals

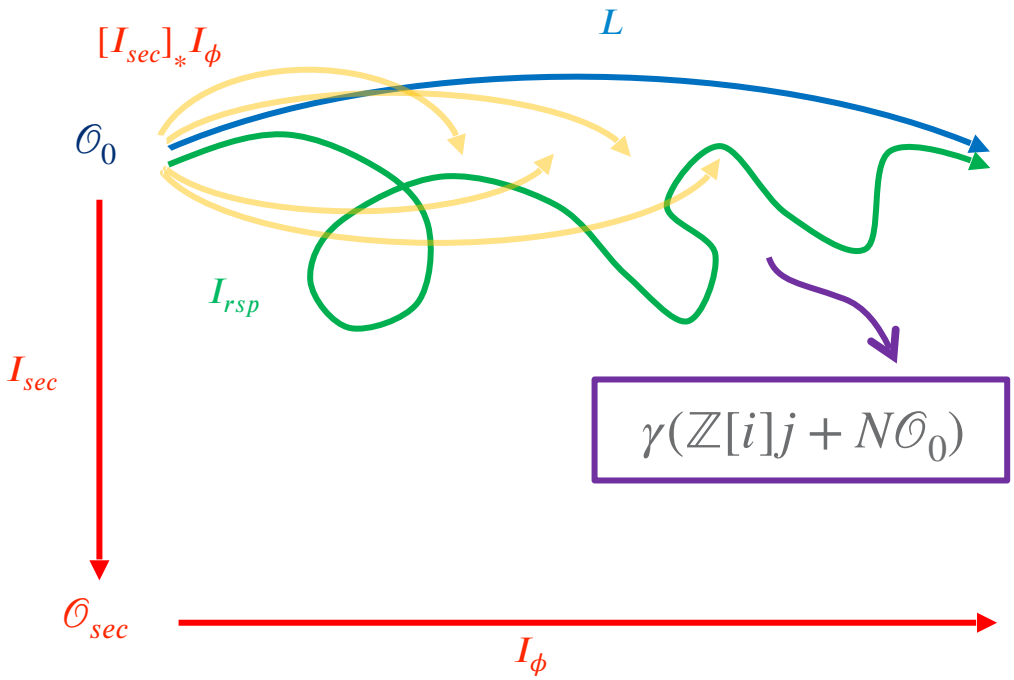
Quaternions

Supersingular Curves

Isogenies

Endormorphisms

KLPT machinery



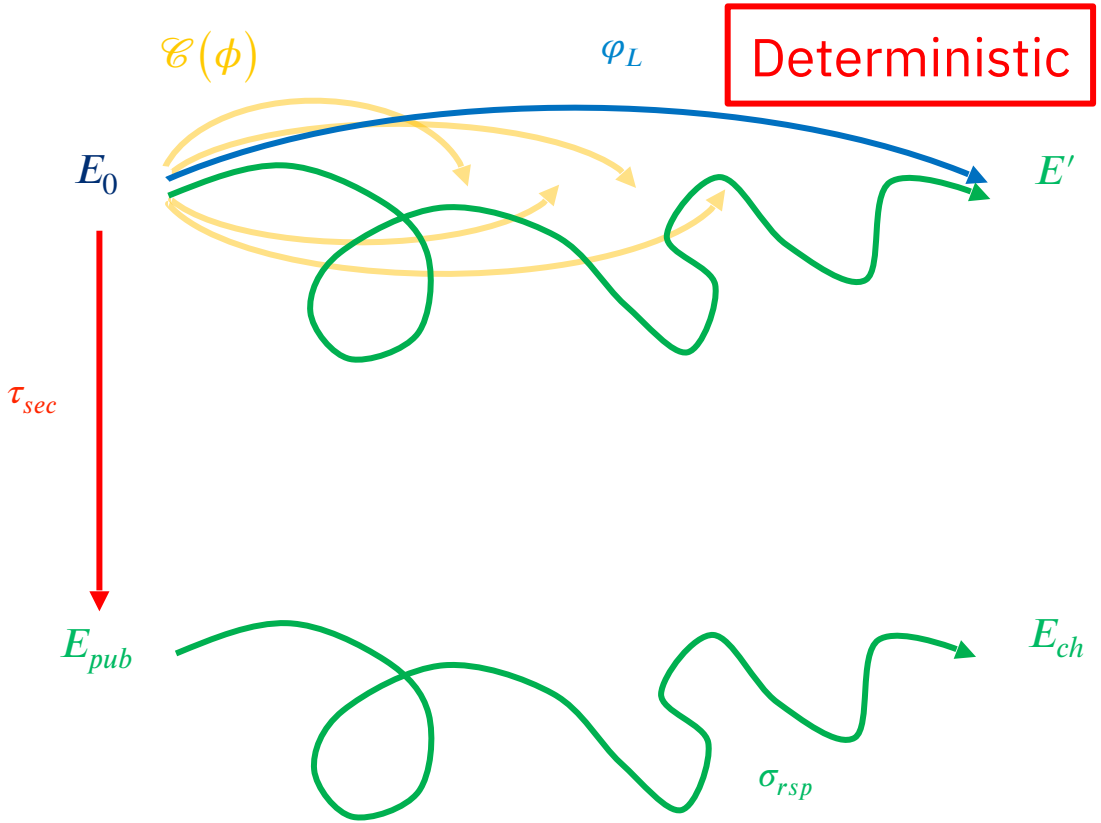
Quaternion World

Maximal Orders in the Algebra

Ideals

Quaternions

KLPT Distinguisher



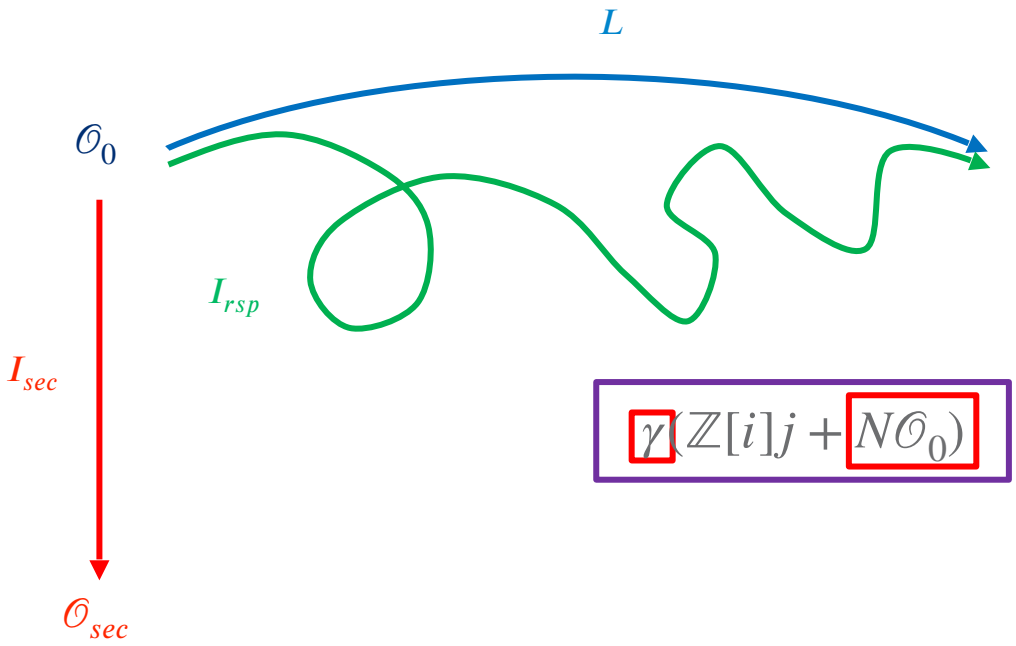
Geometric World

Supersingular Curves

Isogenies

Endormorphisms

KLPT Distinguisher



Quaternion World

Maximal Orders in the Algebra

Ideals

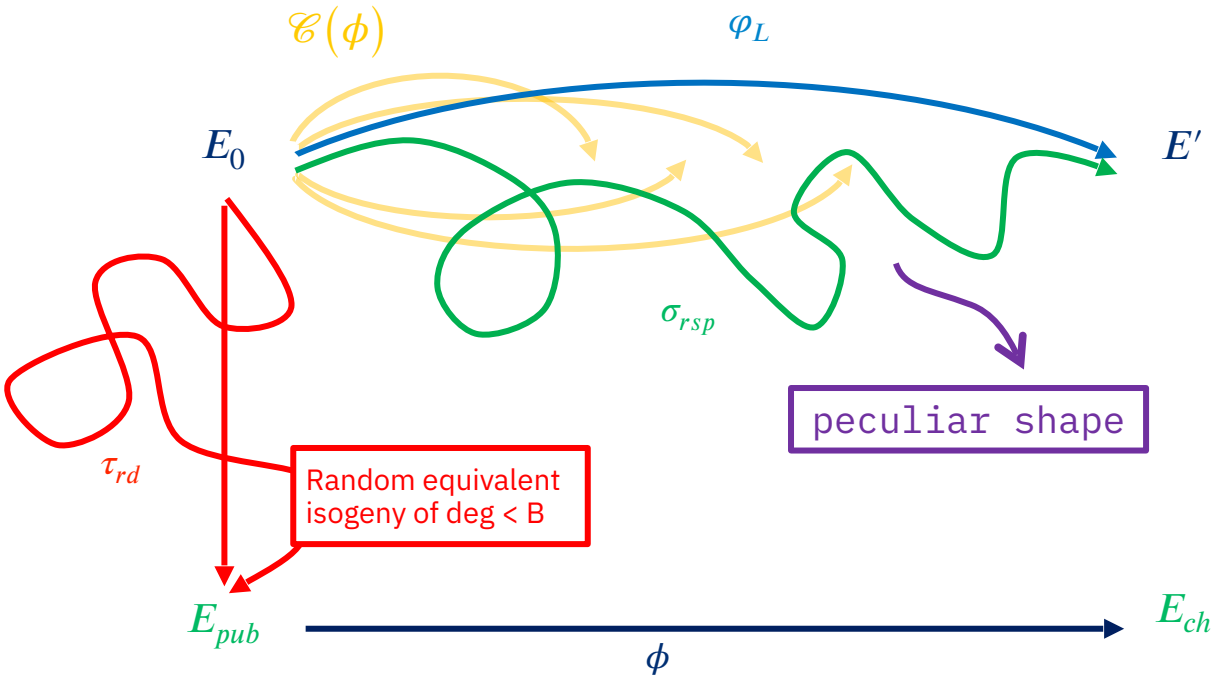
Quaternions

Full-Anonymous Linear Ring Signatures

Problems:

- knowledge of the Eichler Order
- knowledge of the *Class* in which we are working on
- `EquivalentPrimeIdeal(`*Class*`)` is a deterministic KLPT step

Randomized KLPT



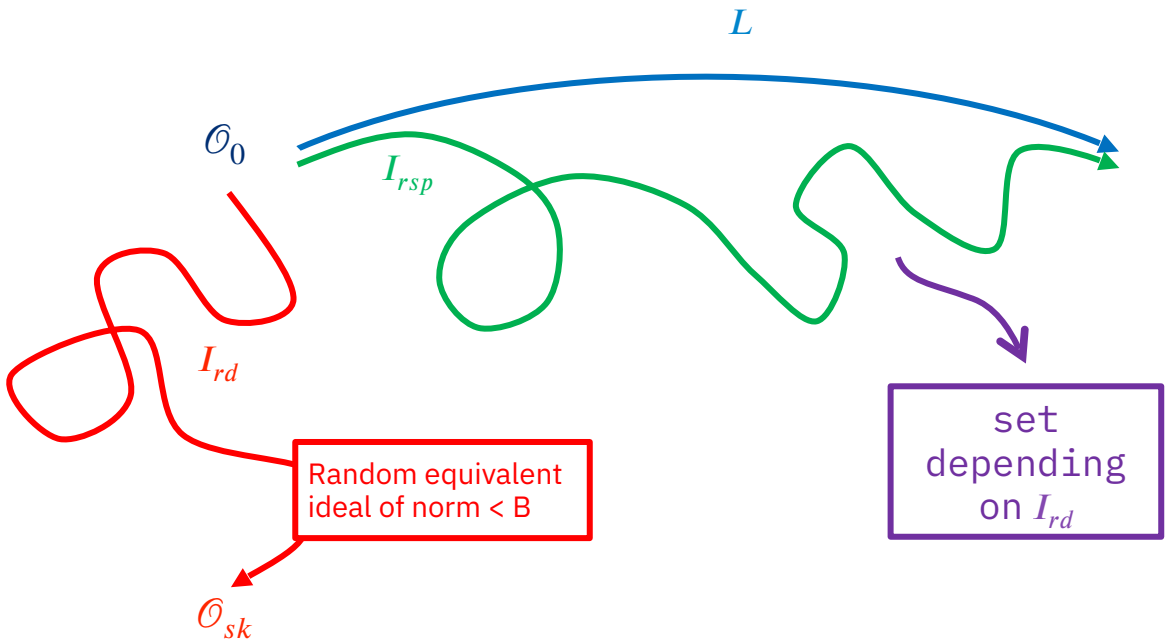
Geometric World

Supersingular Curves

Isogenies

Endormorphisms

Randomized KLPT



Quaternion World

Maximal Orders in the Algebra

Ideals

Quaternions

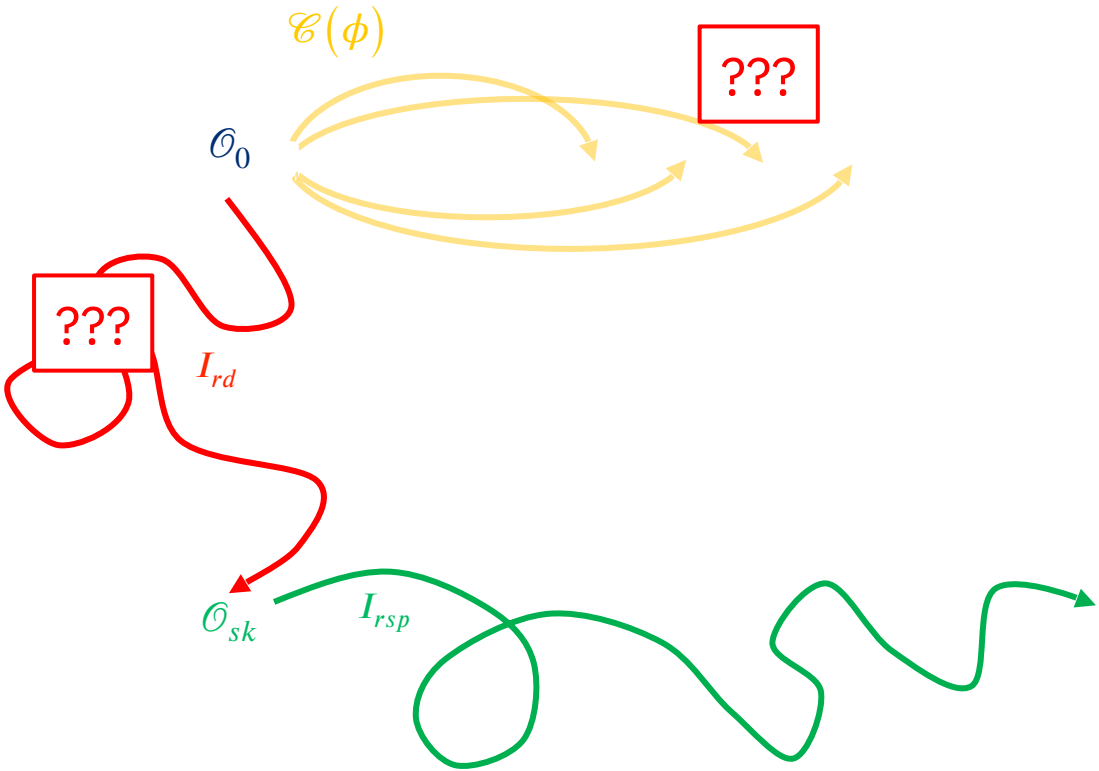
More formally…

Given E, a random curve of known endomorphism ring $\mathcal{O}$, test if a cyclic left $\mathcal{O}$-ideal I_η of norm D lie in the union:

$$\left\{ [I_\psi]_* I_\iota \mid \iota \in \mathcal{P}_{\deg(\psi)}, \boxed{\psi \in \texttt{Iso}_B(E_0, E)} \right\} ;$$

where $\mathcal{P}_{\deg(\psi)}$ is defined as in SQIsign.

Randomized KLPT



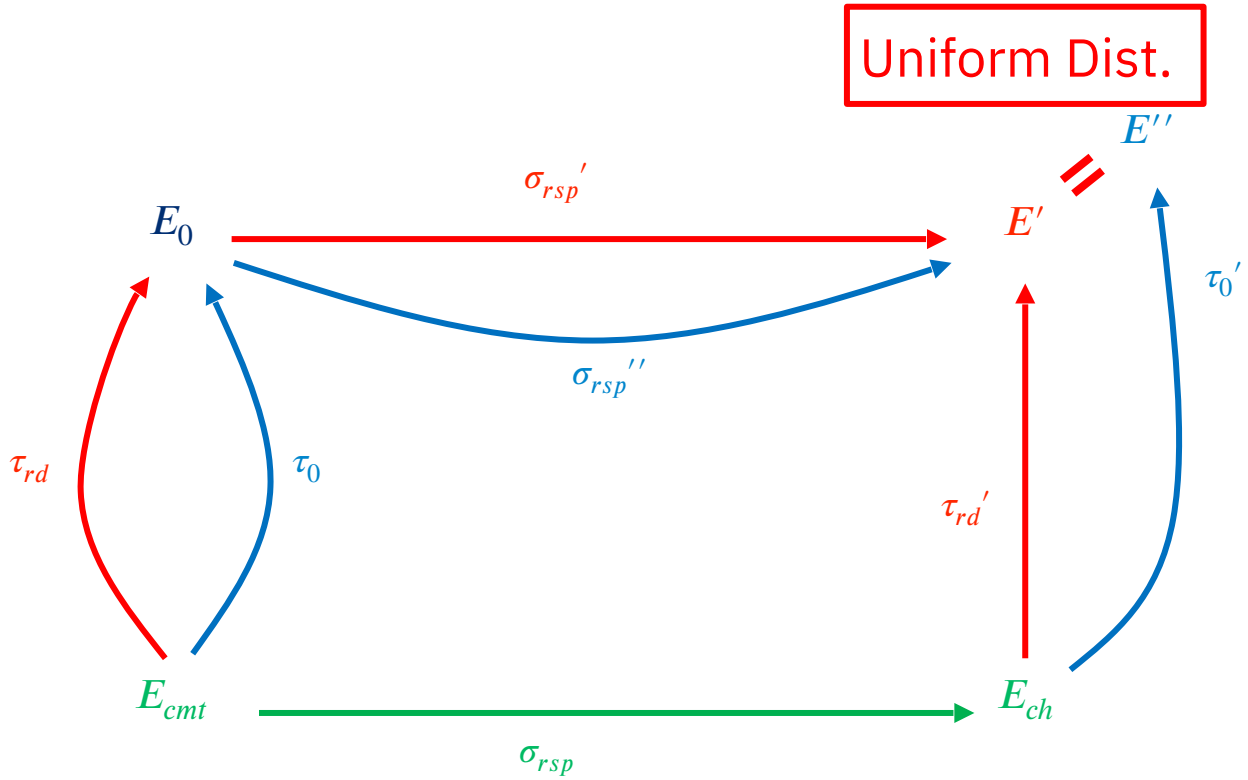
Quaternion World

Maximal Orders in the Algebra

Ideals

Quaternions

Randomized KLPT



Geometric World

Supersingular Curves

Isogenies

Endormorphisms

Instantiations: Fixing the parameters

Random Ideal Degree Bound B

$$\#\mathtt{Iso}_B(E_0, E) = \frac{0.61}{\log(B)} \frac{B^2}{p} \approx 2^\lambda$$

$$B \geq 2^{\frac{\lambda}{2}} p^{\frac{1}{2}}$$

Instantiations: Fixing the parameters

Resp Isogeny Degree Bound D

$$D = 3\log(p) + 3\log(B) + O\left(\log\log(p)\right)$$

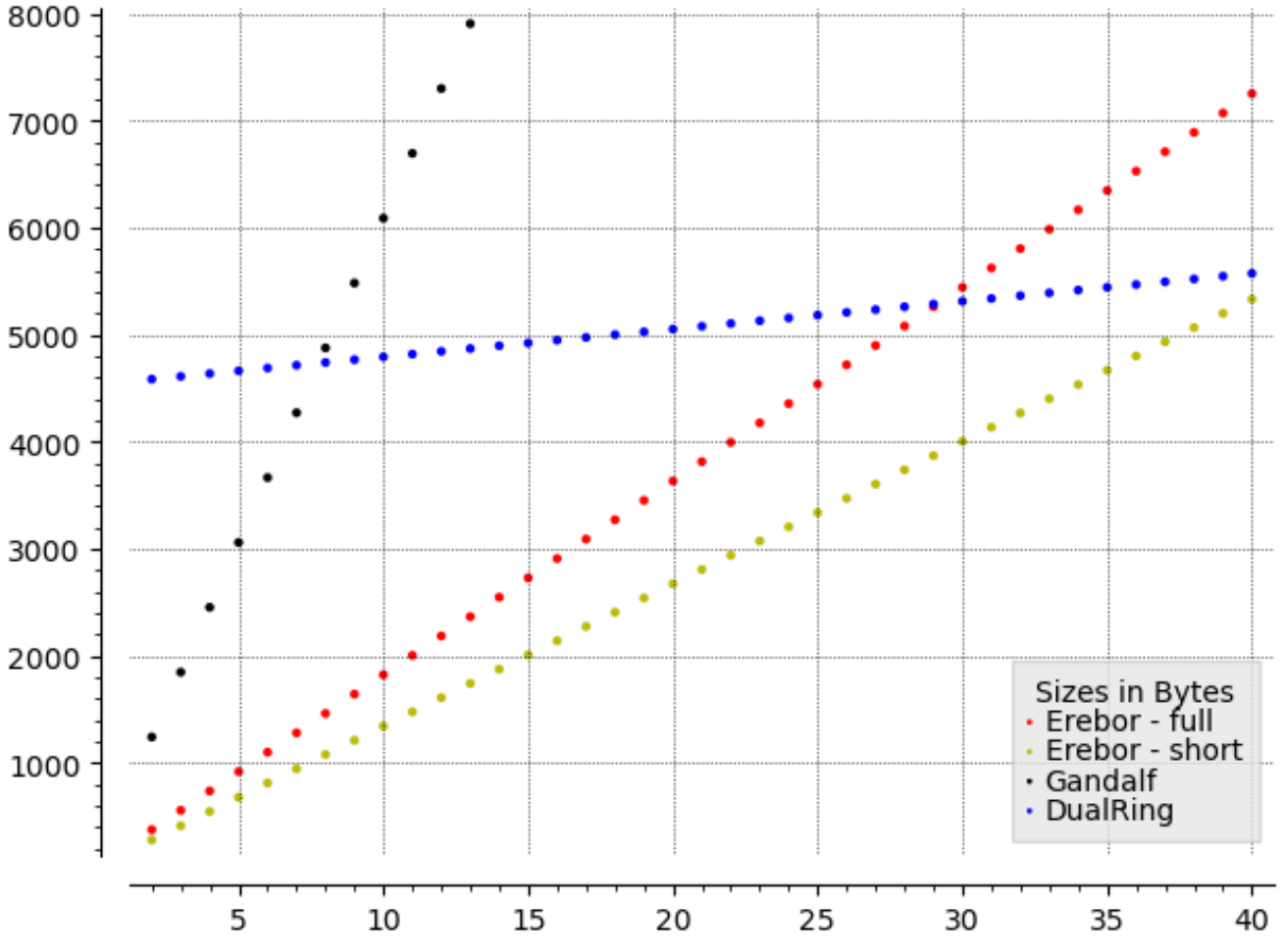
$$\log(D) \approx \frac{9}{2}\log(p) + 3\frac{\lambda}{2} + O\left(\log\log(p)\right) \approx \frac{21}{4}\log(p)$$

+ 40% wrt SQIsign (3.75log(p))

Instantiations: Final Results

NIST I	**Signing** (MC)	**Ver.** (MC)	**Signature size** (B)
Erebor-*full*	$(N-1)\cdot 42 + 3203$	$N \cdot 42$	$16 + N \cdot 181$
Erebor-*short*	$(N-1)\cdot 30 + 2408$	$N \cdot 30$	$16 + N \cdot 133$

Instantiations: Comparisons



Logarithmic-sized Perfect-Anonymous Ring Signature: Durian

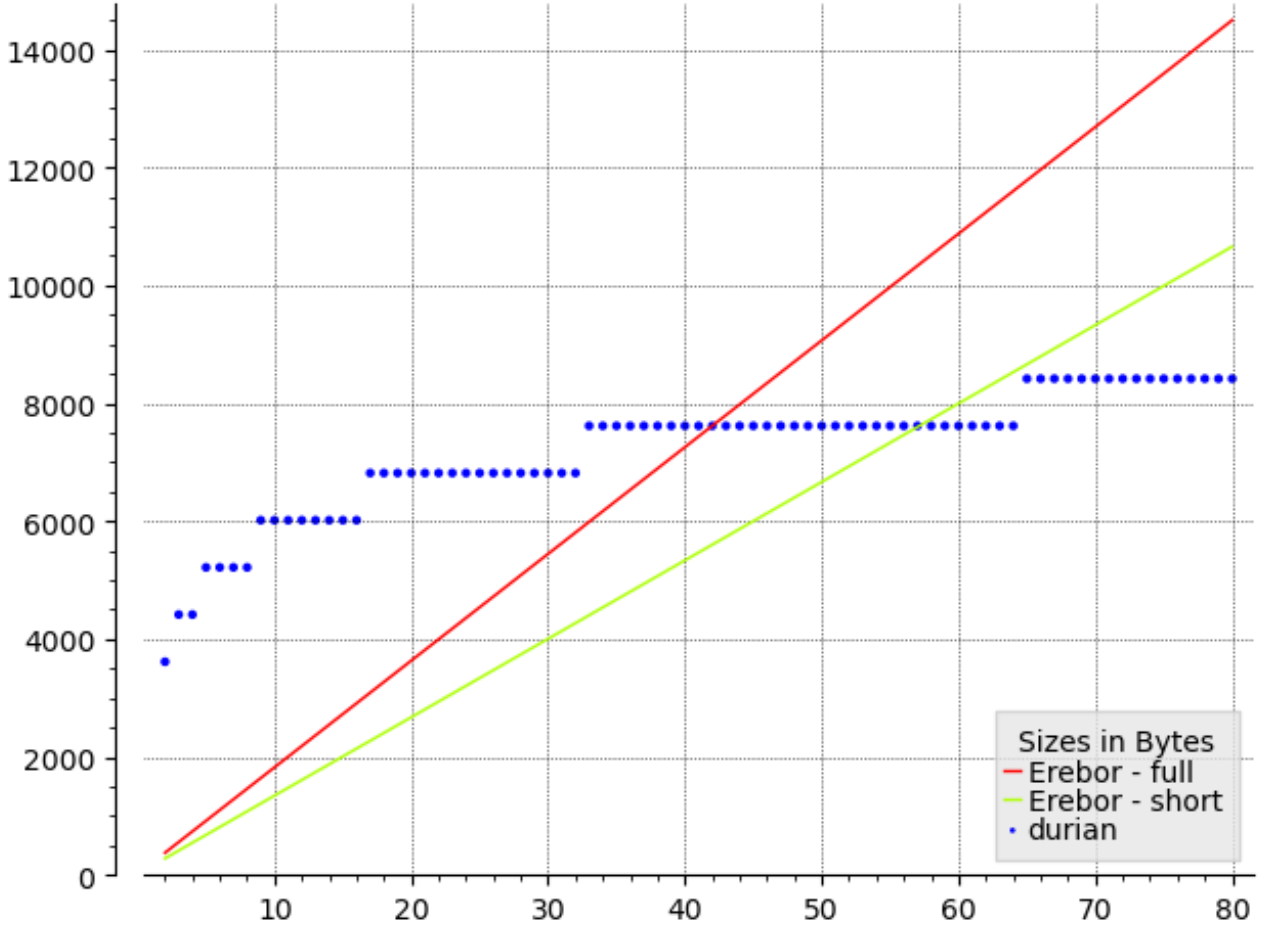
Combine the GPS signature with the framework from Calamari and Falafl

Improve the GPS signature base construction

Best full-anonymous log-size isogeny Ring Signature for NIST I:

4.08 KB for 2 users,
6.29 KB for 8 users,
9.87 KB for 1024 users

Erebor vs Durian: Sizes Comparisons



193 rounds

2024/1185

gbor.in/
erebor