On the security of SQIsign and the AIM

Marius A. Aardal

The Isogeny Club

October 21, 2025

Papers presented

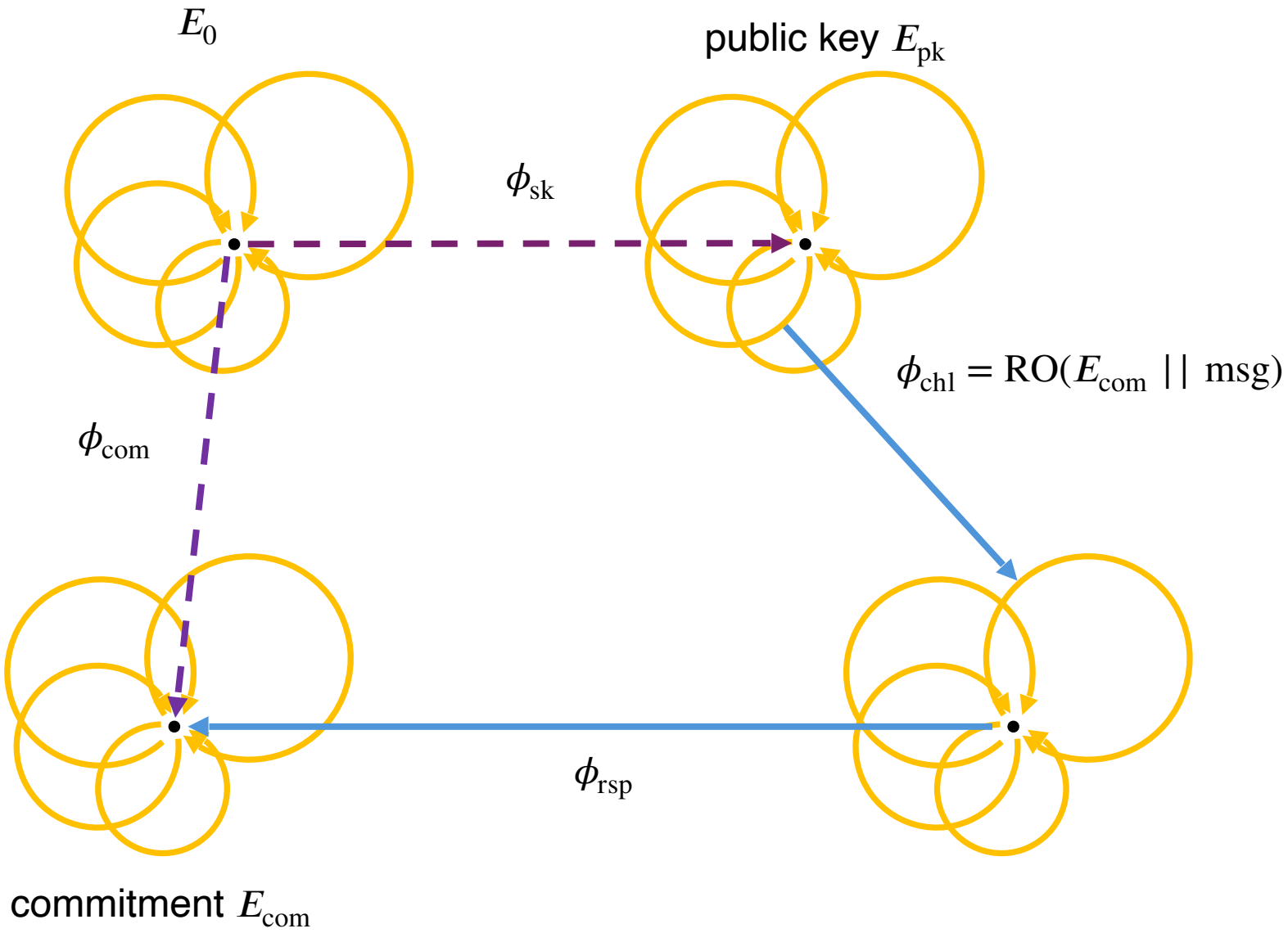
- **A Complete Security Proof of SQIsign**
  Marius A. Aardal, Andrea Basso, Luca de Feo, Sikhar Patranabis and Benjamin Wesolowski (CRYPTO'25)
  https://eprint.iacr.org/2025/379

- **The Algebraic Isogeny Model: A General Model with Applications to SQIsign and Key Exchanges**
  Marius A. Aardal, Andrea Basso and Doreen Riepel
  (Soon on eprint)


Part 1: Classical
security (in the ROM)

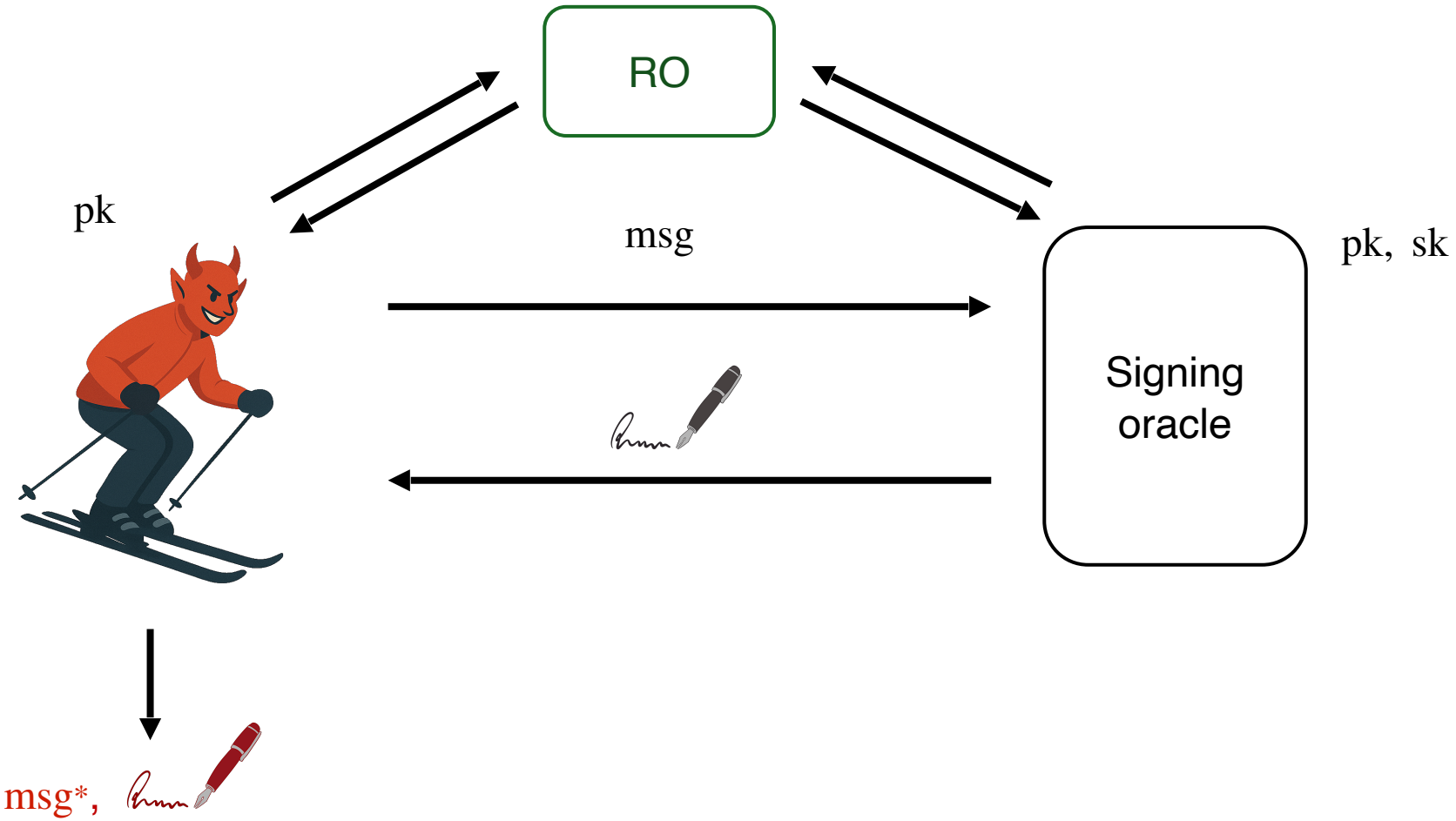
SQIsign

- Round 2 NIST submission
- Fiat-Shamir of Σ-protocol
- signature = $\left(E_{\text{com}},\ \phi_{\text{chl}},\ \phi_{\text{rsp}}\right)$



Security definition

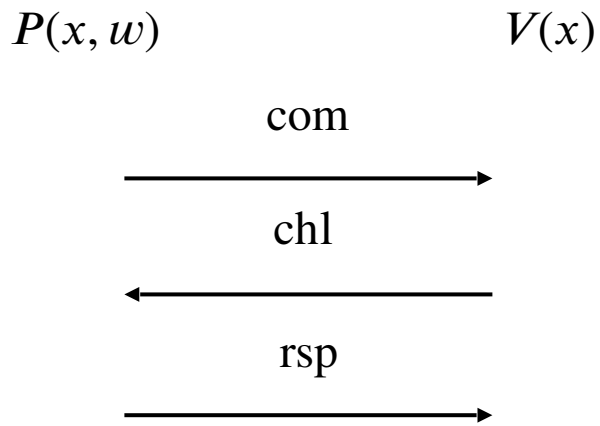
Existential Unforgeability under Chosen Message Attacks (EUF-CMA)



Blueprint

- Σ-protocol for a relation R
- Check-list:

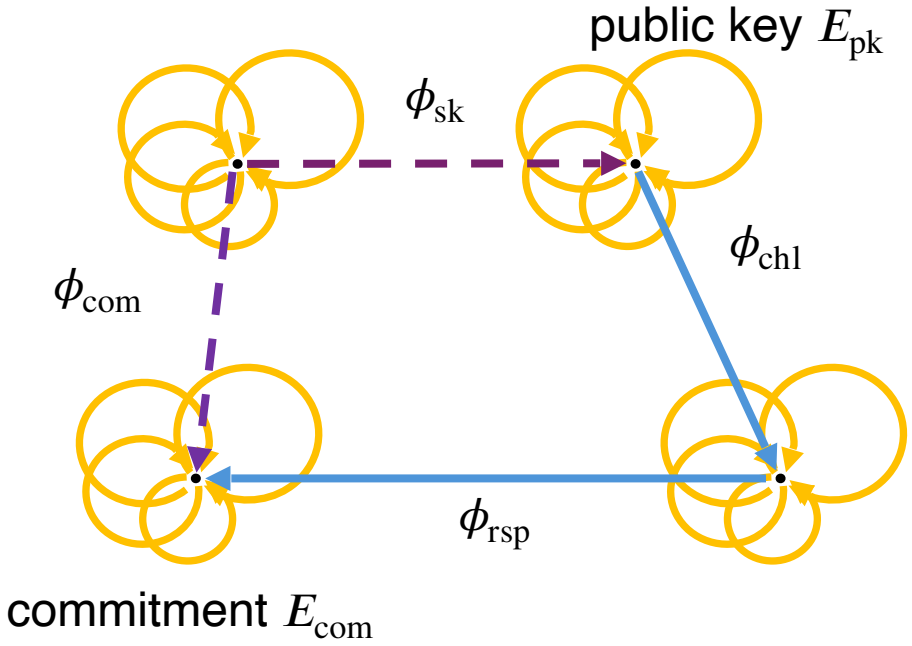
- = Fiat-Shamir signature is EUF-CMA-secure in the ROM



Blueprint

- Σ-protocol for a relation R_{EndRing}
- Check-list:

- = SQIsign is EUF-CMA-secure in the ROM



Knowledge soundness

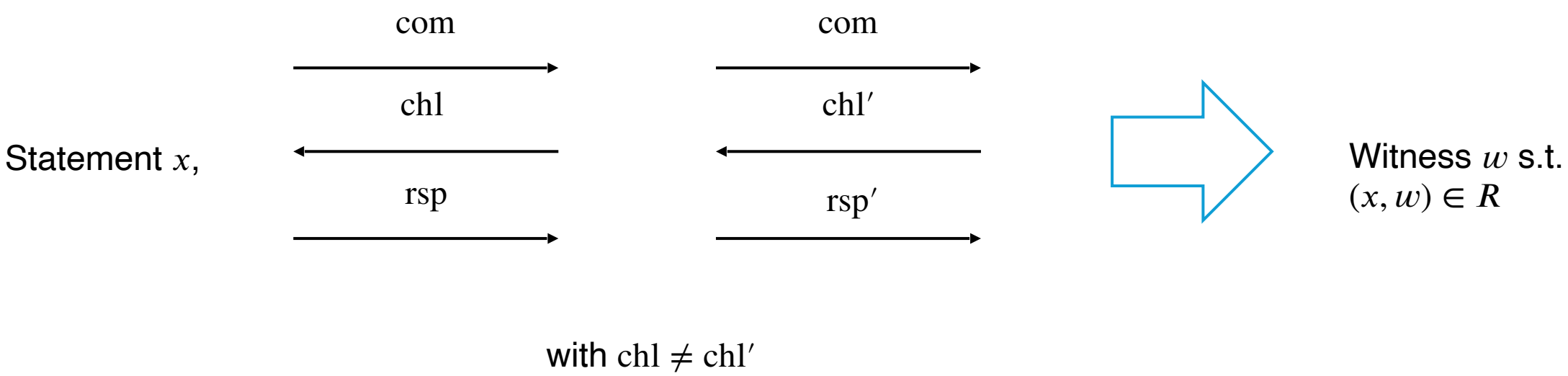
Intuition: “A successful prover  for Σ must know a witness for the statement”

Definition: There is an efficient extractor  s.t. for every statement x and prover 

$$\Pr\left[(x,w) \in R \;\middle|\; w \leftarrow \mathcal{E}^{\;x,}\right] \approx \Pr(\text{convinces the verifier})$$

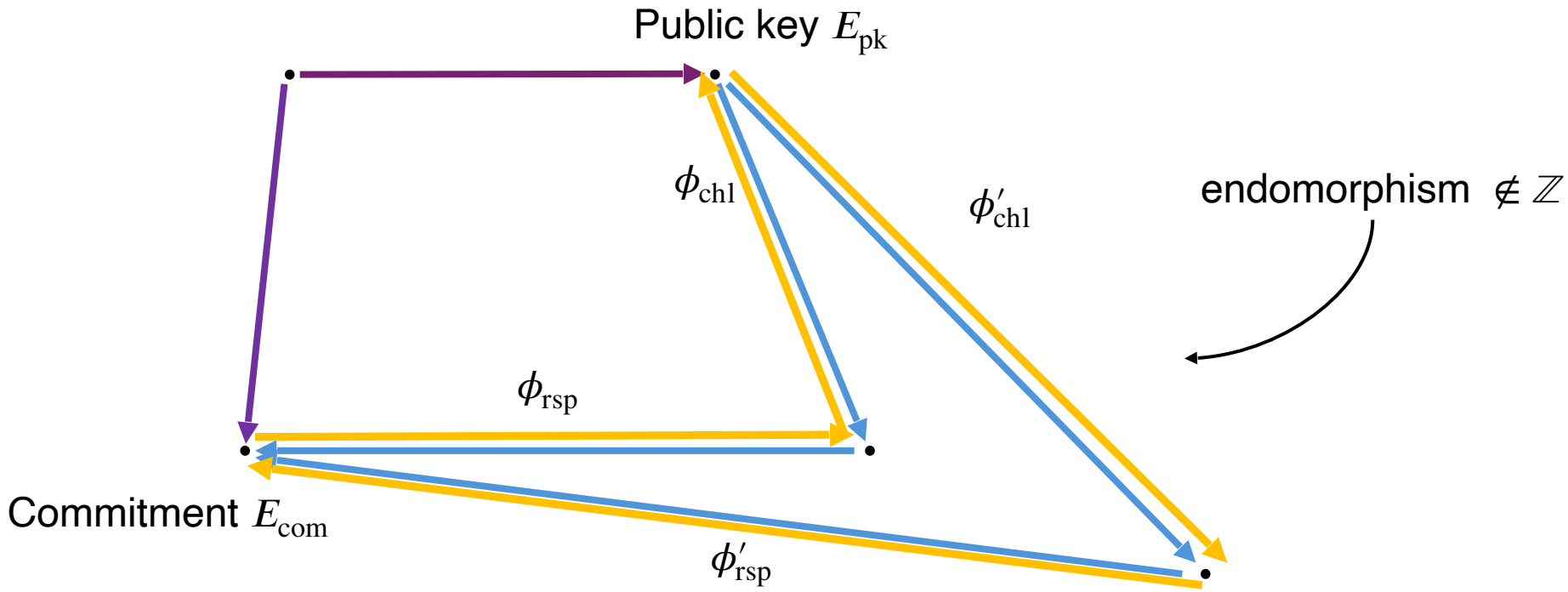
Special soundness

Classically: Special soundness ⇒ Knowledge soundness



with $\mathrm{chl} \neq \mathrm{chl}'$

Special soundness of SQIsign

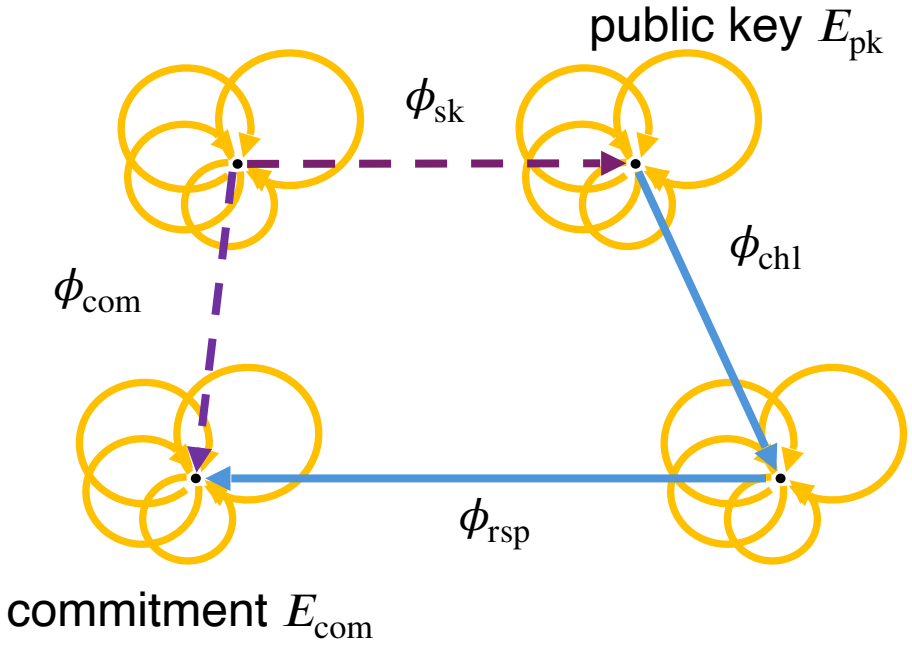


OneEnd $\Leftrightarrow$ EndRing

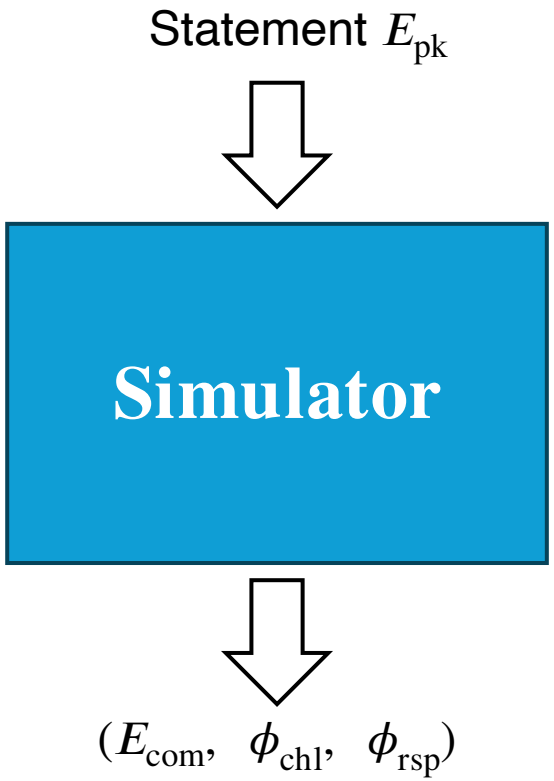
Page and Wesolowski (2024)

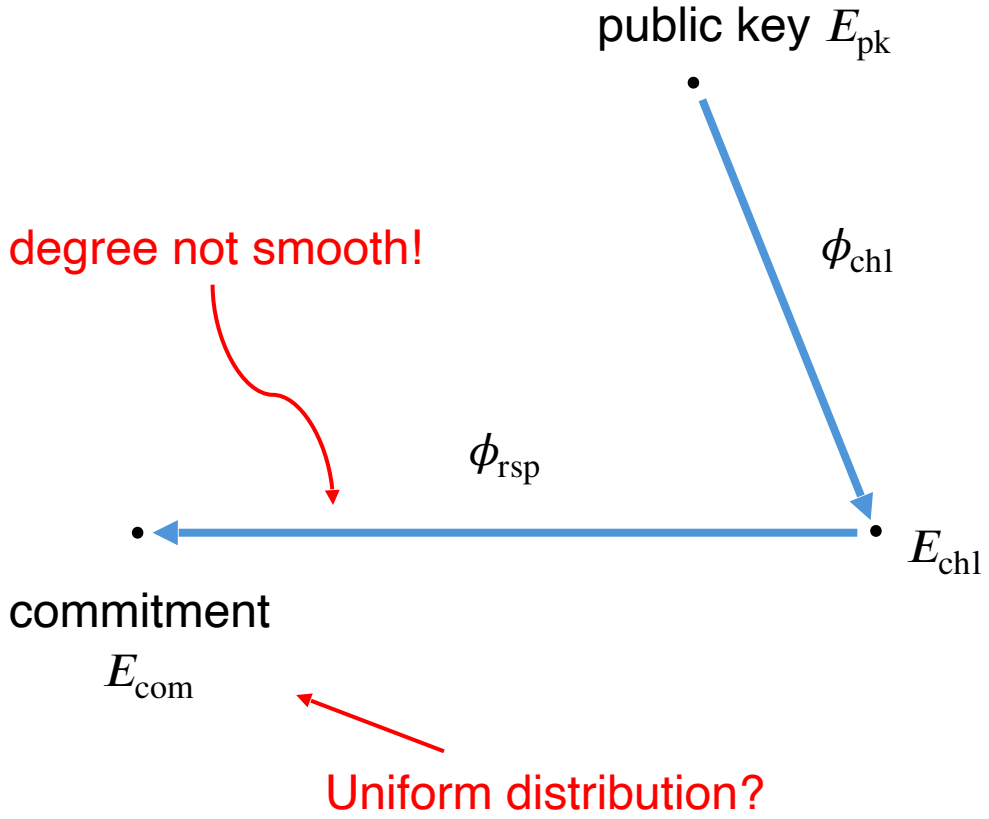
Blueprint

- Σ-protocol for a relation R_{EndRing}
- Check-list:
  - ☑ Unpredictable commitments
  - ☑ Exponential #chl
  - ☑ R_{EndRing} is a hard relation
  - ☑ Knowledge soundness
- = SQIsign is EUF-CMA-secure in the ROM



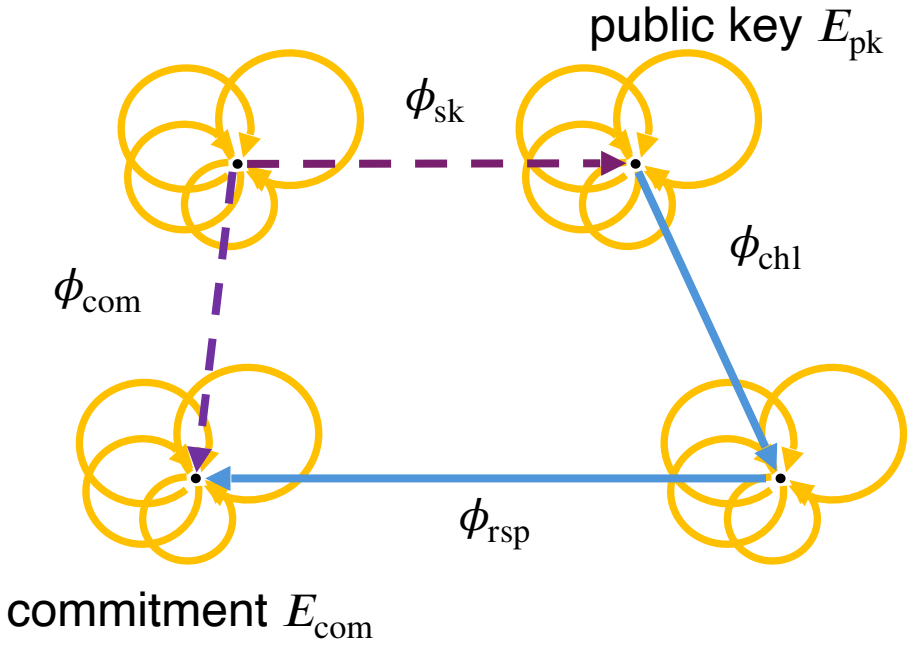
Honest-verifier zero-knowledge





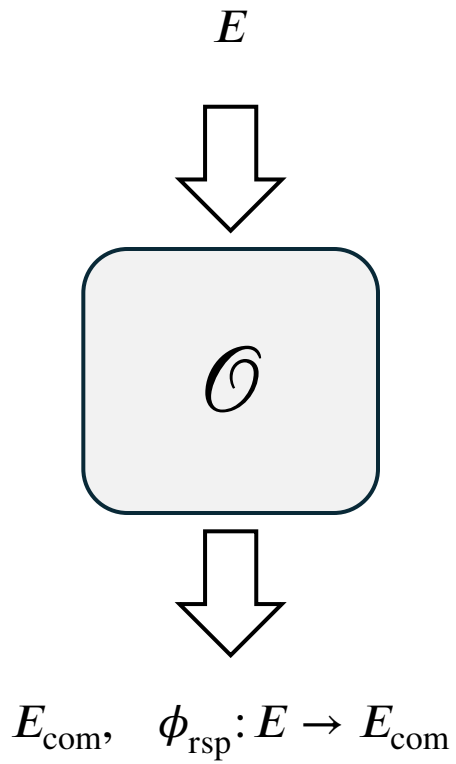
Blueprint

- Σ-protocol for a relation R_{EndRing}
- Check-list:
  - ☑ Unpredictable commitments
  - ☑ Exponential #chl
  - ☑ R_{EndRing} is a hard relation
  - ☑ Knowledge soundness
  - ☒ Honest-verifier zero-knowledge
- = SQIsign is EUF-CMA-secure in the ROM



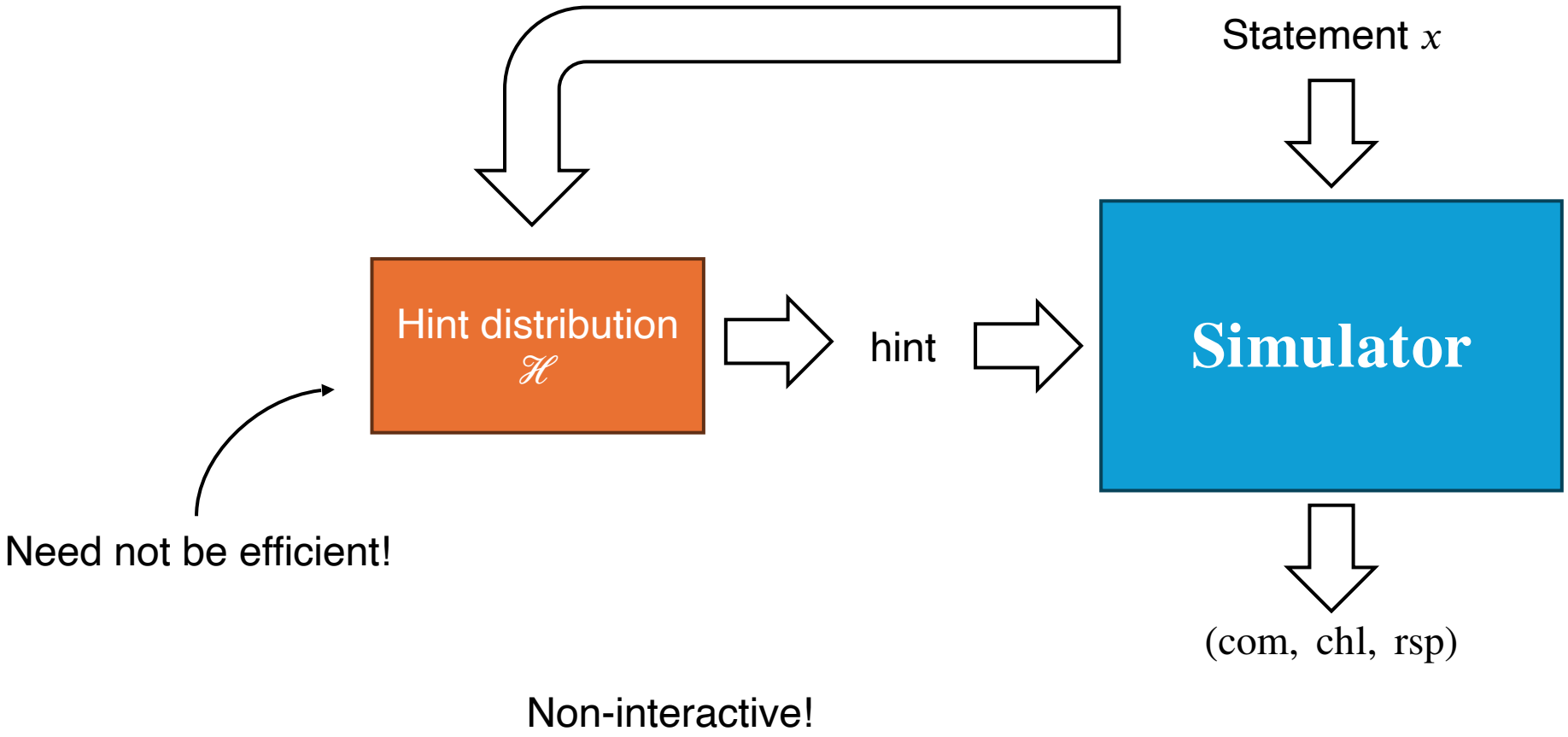
Previous approach

- SQIsign2D-West
- Assume oracle exists
- Pros:
  - HVZK is trivial
- Cons:
  - Security in ad-hoc idealized model
  - Oracle distribution strongly depends on secret, $\mathrm{End}(E)$



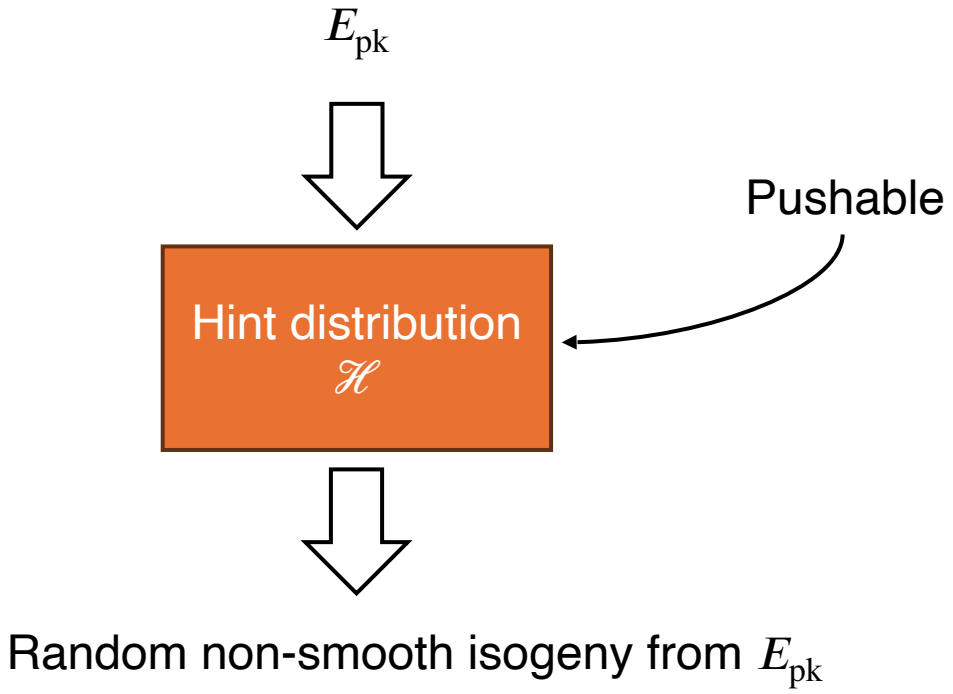
Fiat-Shamir with hints

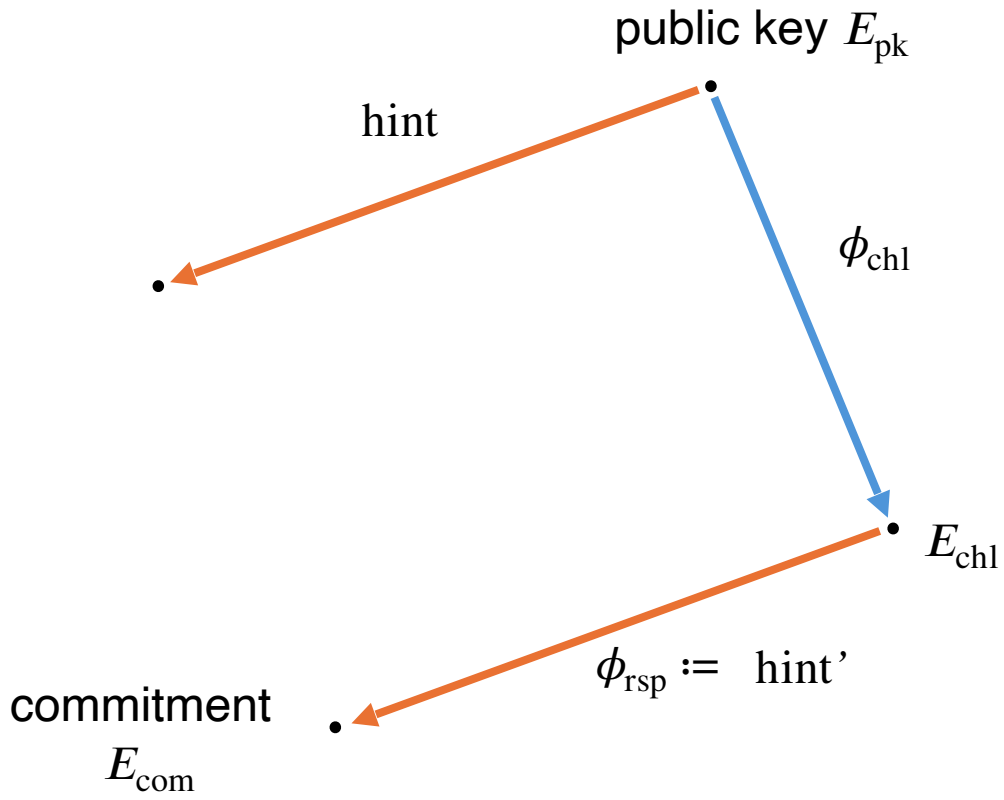
Hint-assisted HVZK



Non-interactive!

Hint distribution for SQIsign



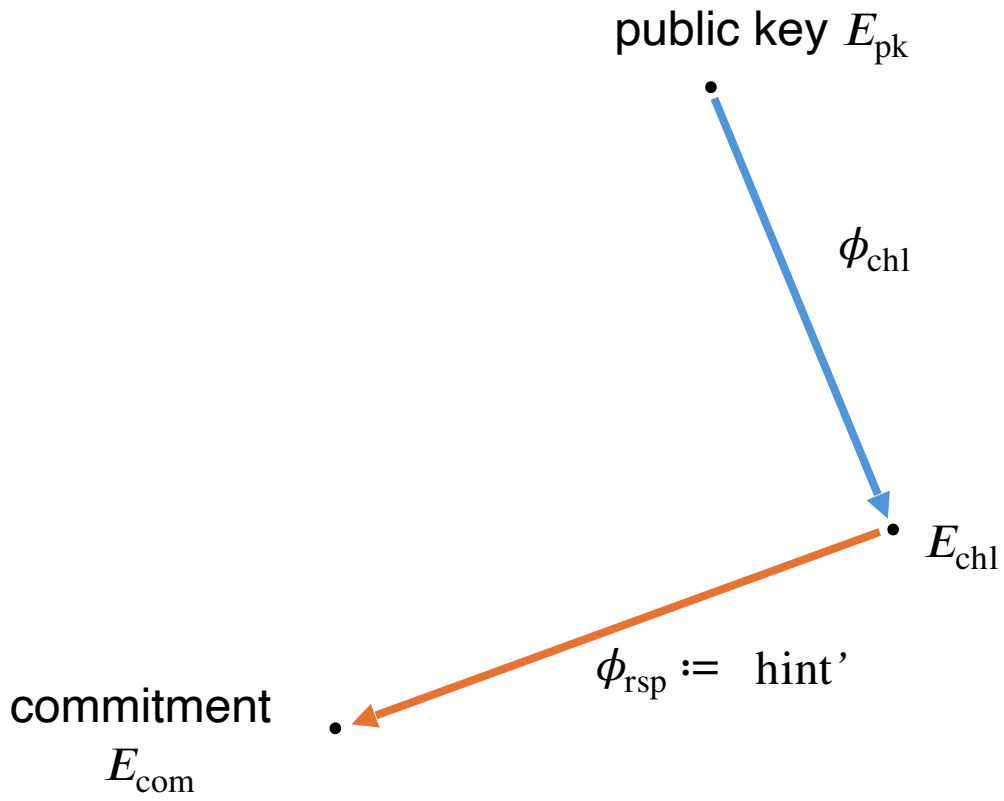


Hint distribution for SQIsign

New computational assumption

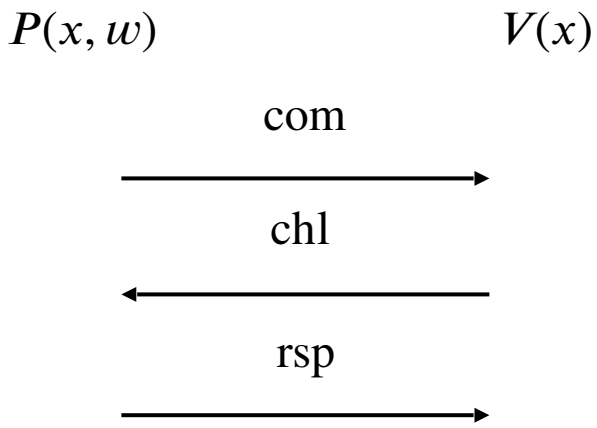
hint-dist

Target curve of hint is indist. from uniform random



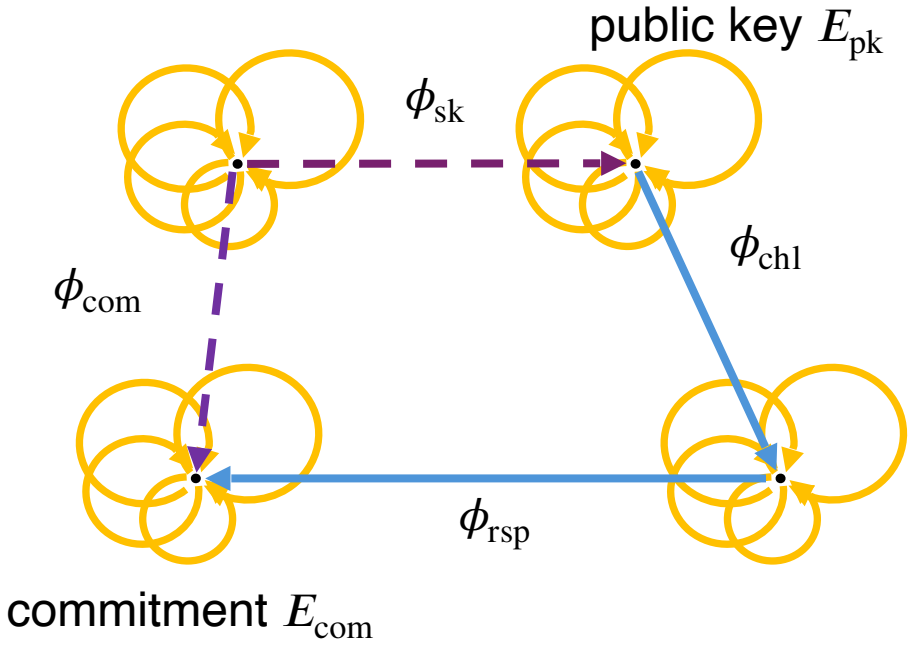
Fiat-Shamir with hints

- Σ-protocol for a relation R
- Check-list:
  - Unpredictable commitments
  - Exponential #chl
  - R is a hard relation **with hints**
  - Knowledge soundness **with hints**
  - **Hint-assisted HVZK**
- = Fiat-Shamir signature is EUF-CMA-secure in the ROM



Fiat-Shamir with hints

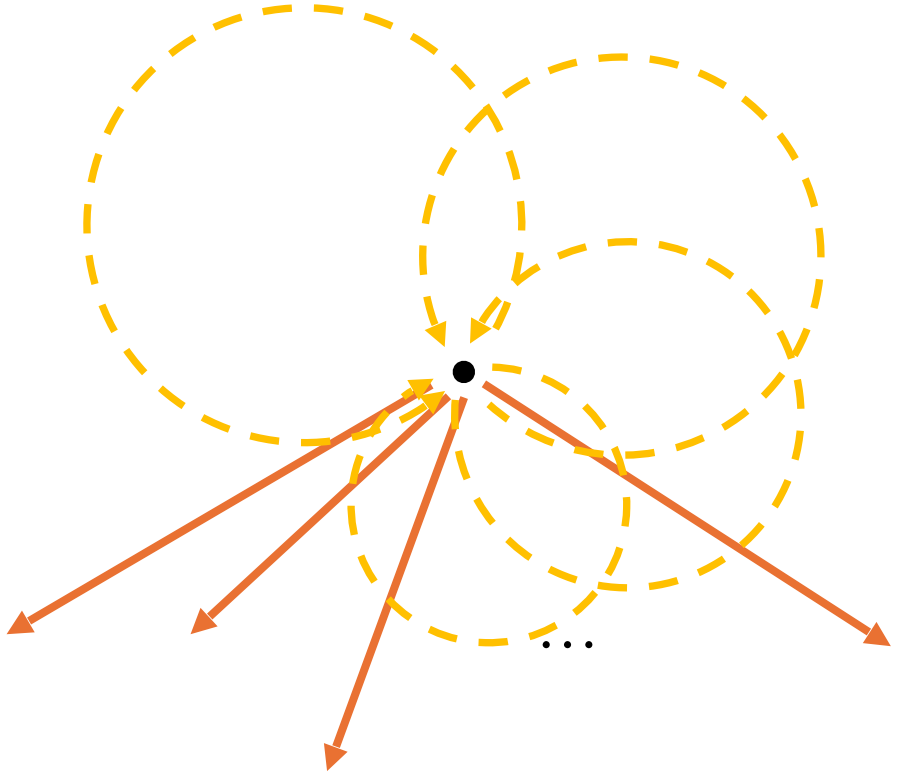
- Σ-protocol for a relation R_{EndRing}
- Check-list:
  - ☑ Unpredictable commitments
  - ☑ Exponential #chl
  - R_{EndRing} is a hard relation **with hints**
  - Knowledge soundness **with hints**
  - ☑ **Hint-assisted HVZK**(assuming hint-dist)
- = SQIsign is EUF-CMA-secure in the ROM



EndRing with hints

Given: $\mathrm{poly}(\lambda)$ hints

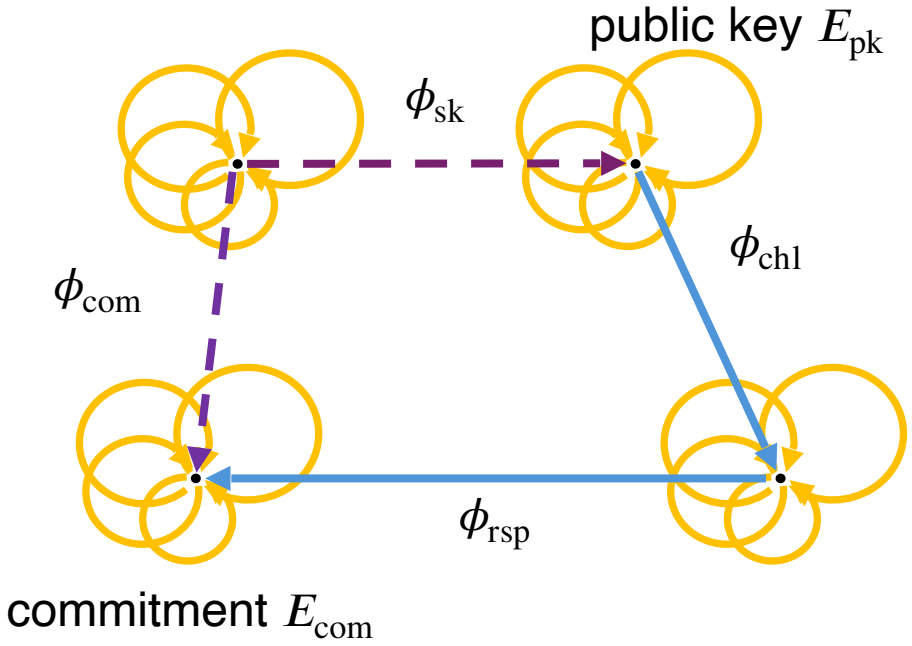
Goal: Compute EndRing



Intuition: Isogenies of non-smooth degree
do not provide more info than isogenies of smooth degree

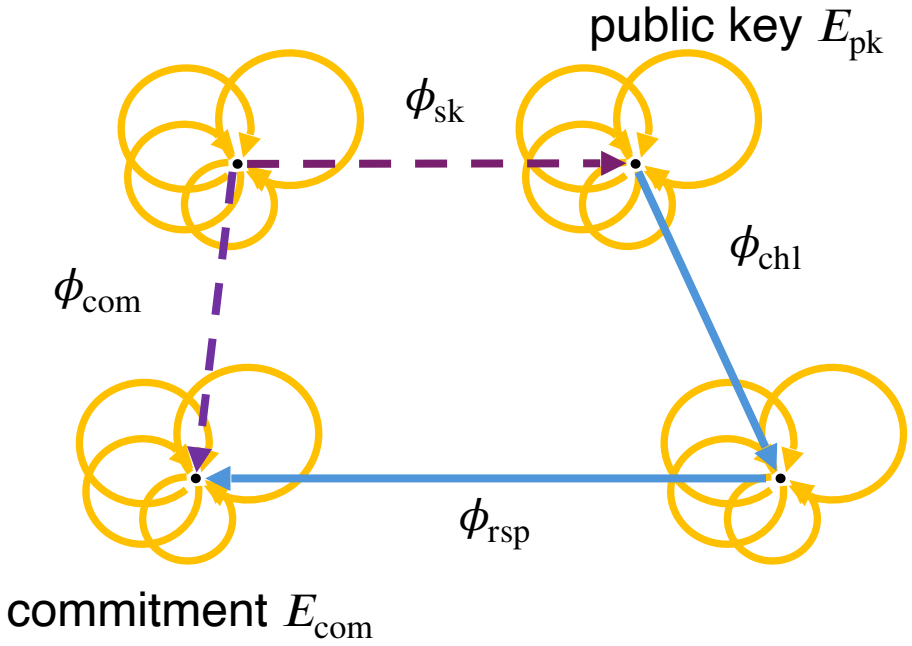
Fiat-Shamir with hints

- Σ-protocol for a relation R_{EndRing}
- Check-list:
  - ☑ Unpredictable commitments
  - ☑ Exponential #chl
  - ☑ R_{EndRing} is a hard relation **with hints**
  - ☑ Knowledge soundness **with hints**
  - ☑ **Hint-assisted HVZK** (assuming hint-dist)
- = SQIsign is EUF-CMA-secure in the ROM



Future work

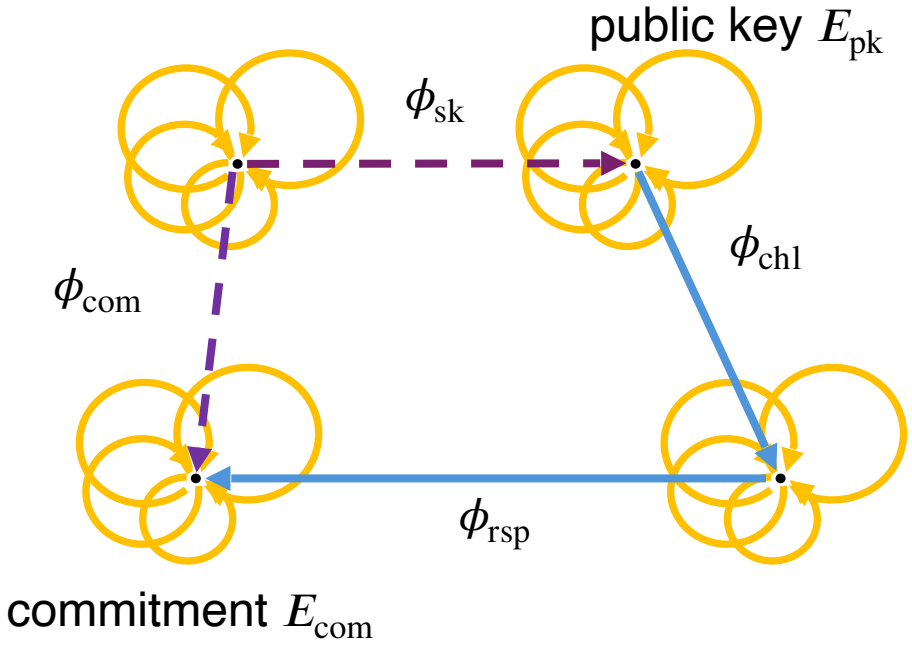
1. IdealToIsogeny
   - Need negligible failure probability
   - Qlapoti?
2. Degree of commitment isogeny
   - Recommend increasing from $\approx 2^{4\lambda}$ to $\approx 2^{8\lambda}$
   - Significantly tighter reduction
   - Change has almost no impact on signing time




Part 2: QROM security in the AIM

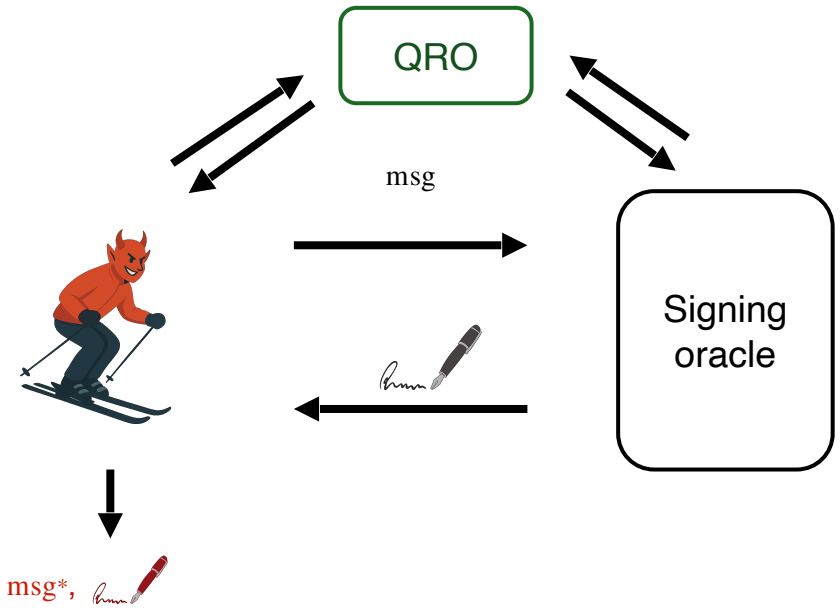
Fiat-Shamir with hints in the QROM

- Σ-protocol for a relation R_{EndRing}
- Check-list:
  - ☑ Unpredictable commitments
  - ☑ Exponential #chl
  - ☑ R_{EndRing} is a hard relation **with hints**
  - ☒ Knowledge soundness **with hints**
  - ☑ **Hint-assisted HVZK** (assuming hint-dist)
- = SQIsign is EUF-CMA-secure in the QROM



Partial QROM reduction

EUF-CMA

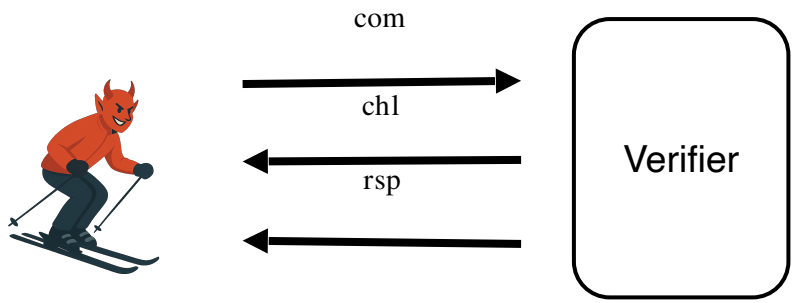


Unpredictable commitments

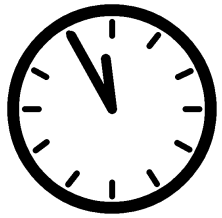
+ (hint-assisted) HVZK

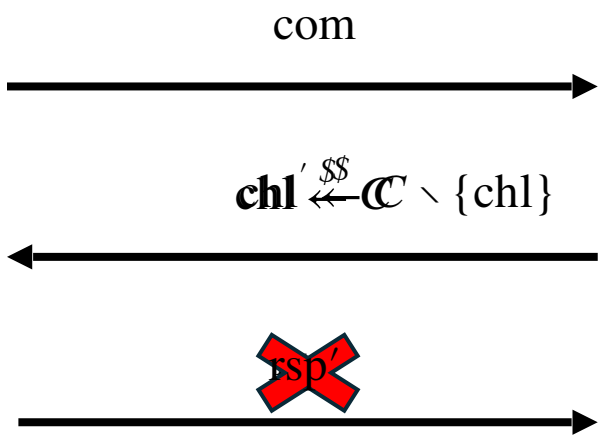
Soundness of

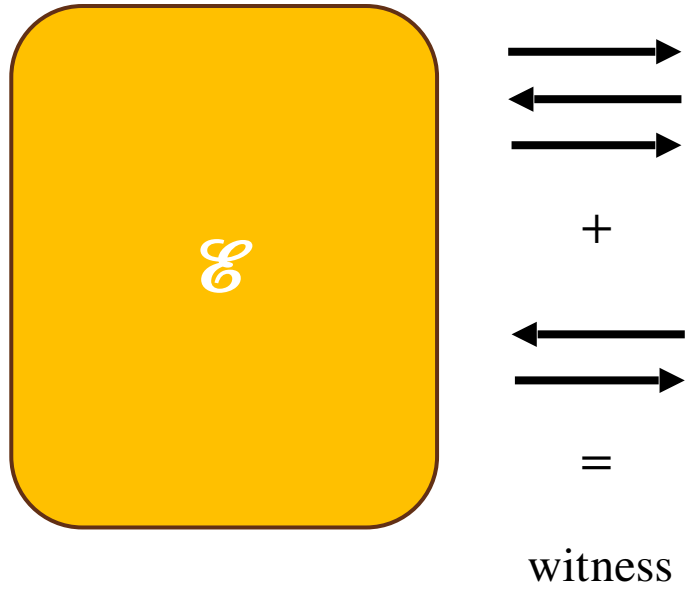
Σ



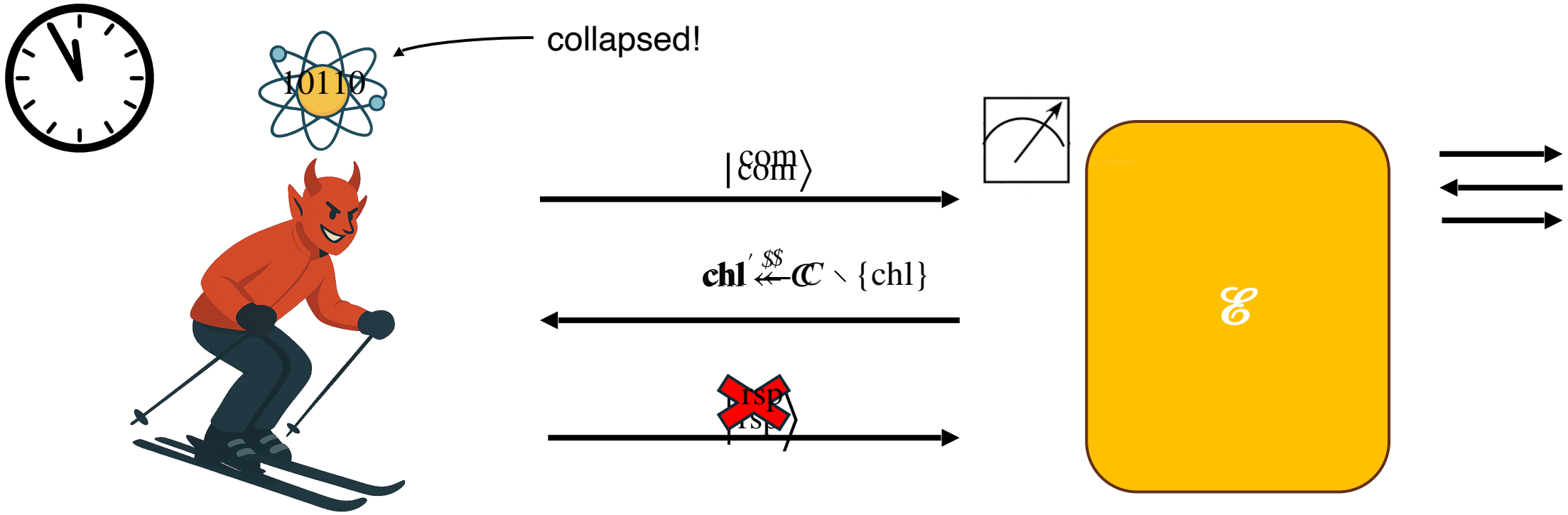
Classically: SS ⇒ KS







Quantumly: SS $\not\Rightarrow$ KS



Special soundness is not enough!

Ambainis, Rosmanis and Unruh (2014)

Quantum knowledge soundness

We know how to use quantum rewinding when:

1. The response is unique
2. The response is commited to with a collapse-binding commitment
3. Σ has an associated lossy function
4. …

None of these seem to apply to SQIsign!

1: Unruh (2012) 2: Unruh (2016) 3: Liu and Zhandry (2019)

The Algebraic Isogeny Model (AIM)

The Algebraic Group Model (AGM)

$g_0, \; g_1, \ldots, g_n$

h

$h = g_0^{e_0} \, g_1^{e_1} \cdots g_n^{e_n}$

Game

Intuition: Oblivious sampling is not useful

Fuchsbauer, Kiltz and Loss (2018)

The Algebraic Group Action Model (AGAM)

$E_0, \quad E_1, \ldots, E_n$

F

$F = [a] \star E_i$

Game

Only works with protocols based on (black-box) group actions

Duman, Hartmann, Kiltz, Kunzweiler, Lehmann, Riepel (2018)
Orsini, Zanotto (2023)

The Algebraic Isogeny Model (AIM)

Always receives a curve of known EndRing

$E_0, \quad E_1, \ldots, E_n$

F

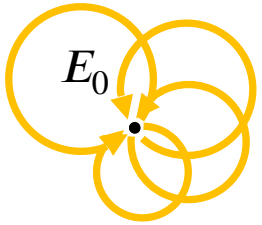
$\varphi: E_i \to F$

Game

No restriction on this isogeny!

Required to be in the 8D-representation

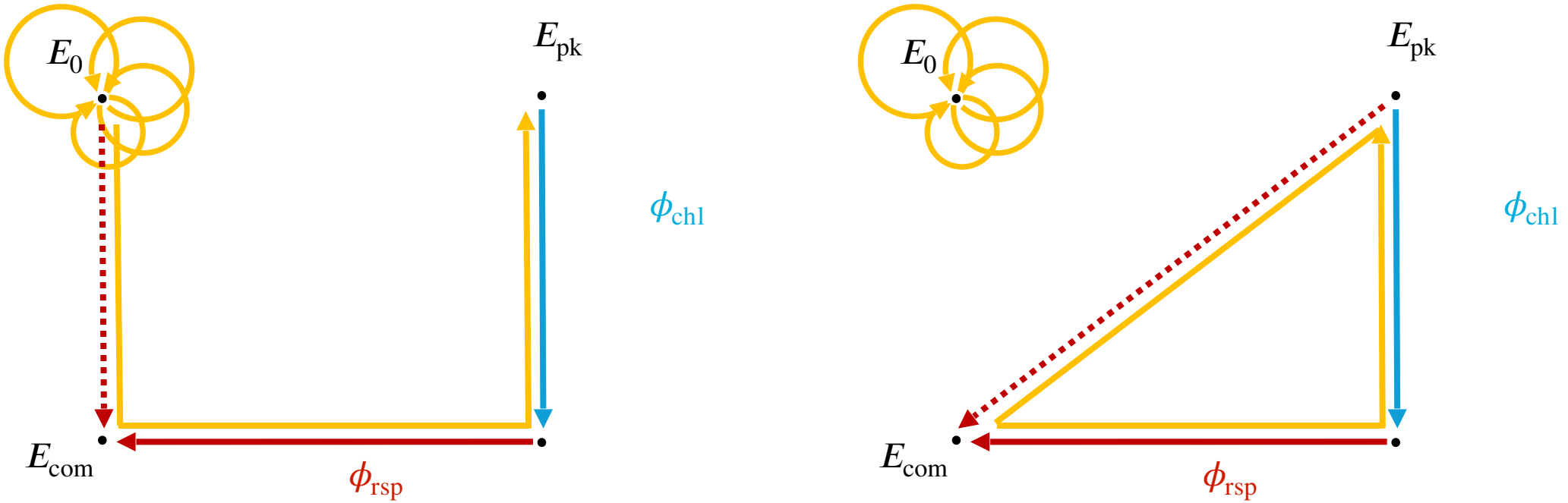
Soundness of SQIsign



E_{pk}

E_{com}

Soundness of SQIsign

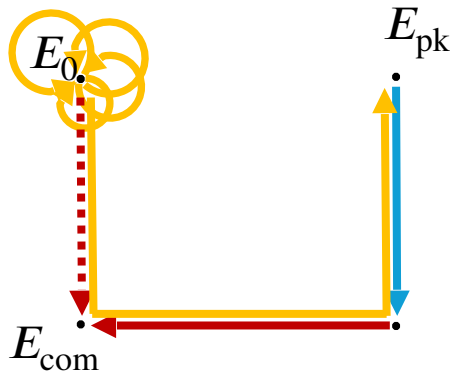


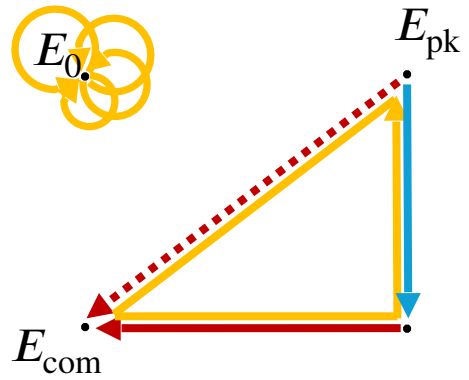
We obtain at least one non-scalar endomorphism (with high probability)!

Assuming that hint-EndRing and hint-dist are hard problems,
SQIsign is EUF-CMA-secure in the
AIM+QROM

Discussion

- Minimal QROM machinery
- Other SQIsign variants
- Oblivious sampling





Other results in the AIM

DLOG ≡ CDH
for all SIDH variants
(M-SIDH, terSIDH, …)

All results in the AGAM can
be lifted to the AIM

Stay tuned for the paper!


Thanks! Any questions?