

Compact Threshold Signatures from Pushforwards of Large-Degree Isogenies

Presented at : MPTS 2026: NIST Workshop on Multi-Party Threshold Schemes 2026 - Regular Talk
Date : 2026-01-29

Presented by : **Giacomo Borin**, IBM Research Zurich, University of Zurich
joint work with Andrea Basso, Riccardo Invernizzi, Luciano Maino, Robi Pedersen, Maria Corte-Real Santos

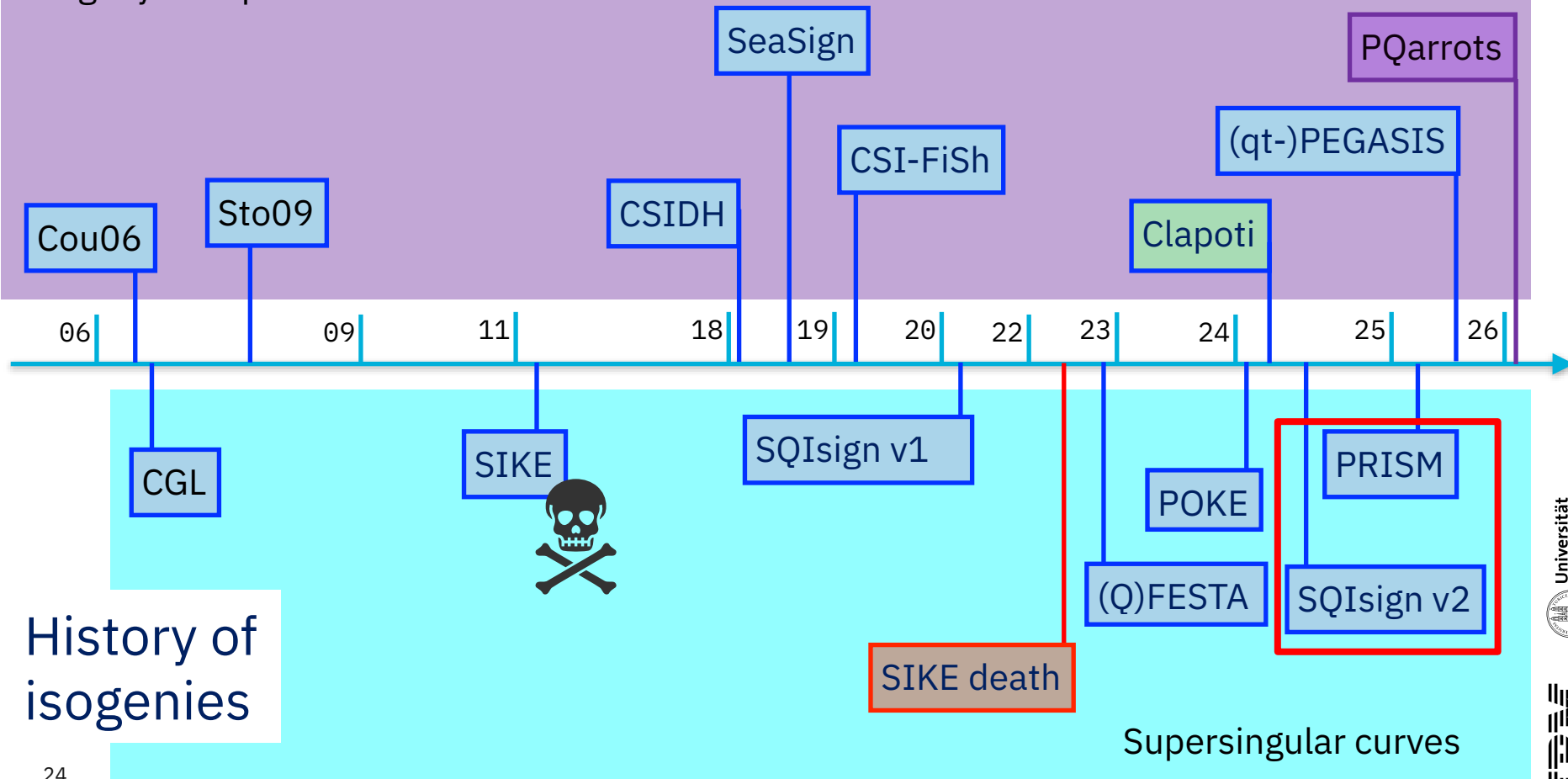


Universität
Zürich^{UZH}



Can we get a quantum safe
and compact threshold
signing procedures?

Isogeny Group Action



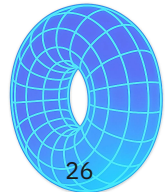
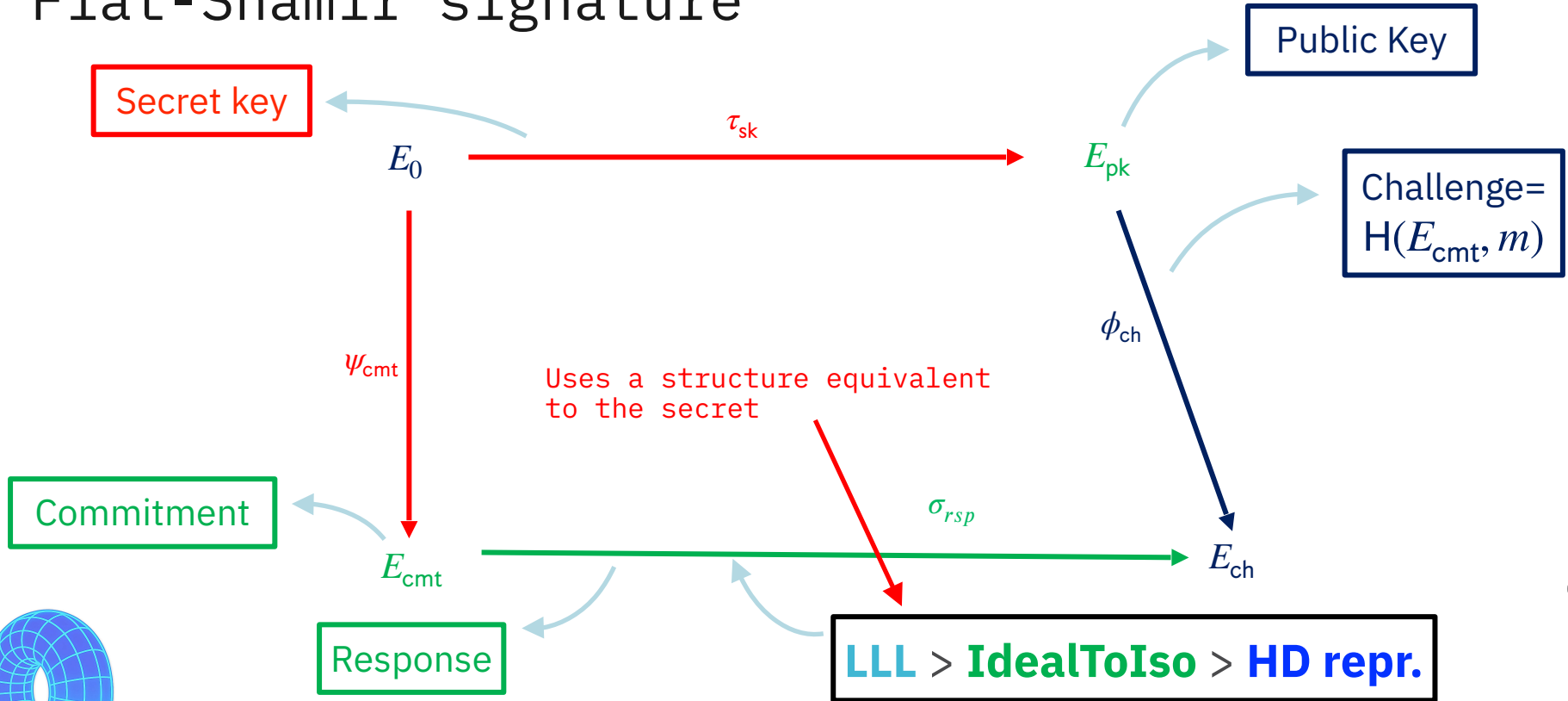
History of isogenies

ATTENTION:



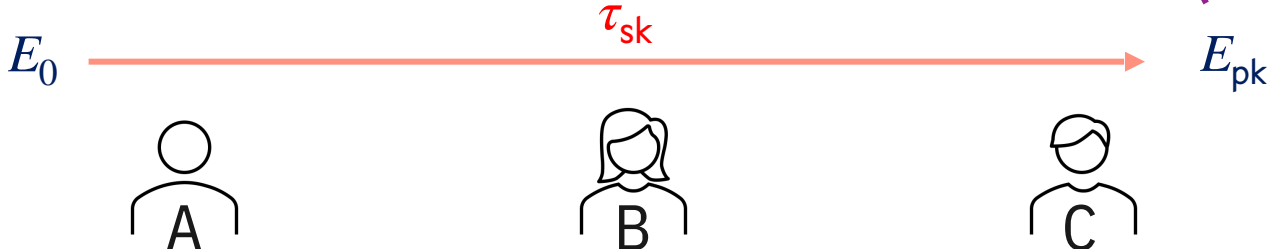
ISOGENIES ARE COMING!

SQIsign Fiat-Shamir signature

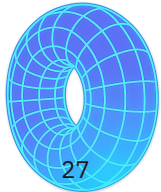


PRISM Hash and Sign Signature Scheme

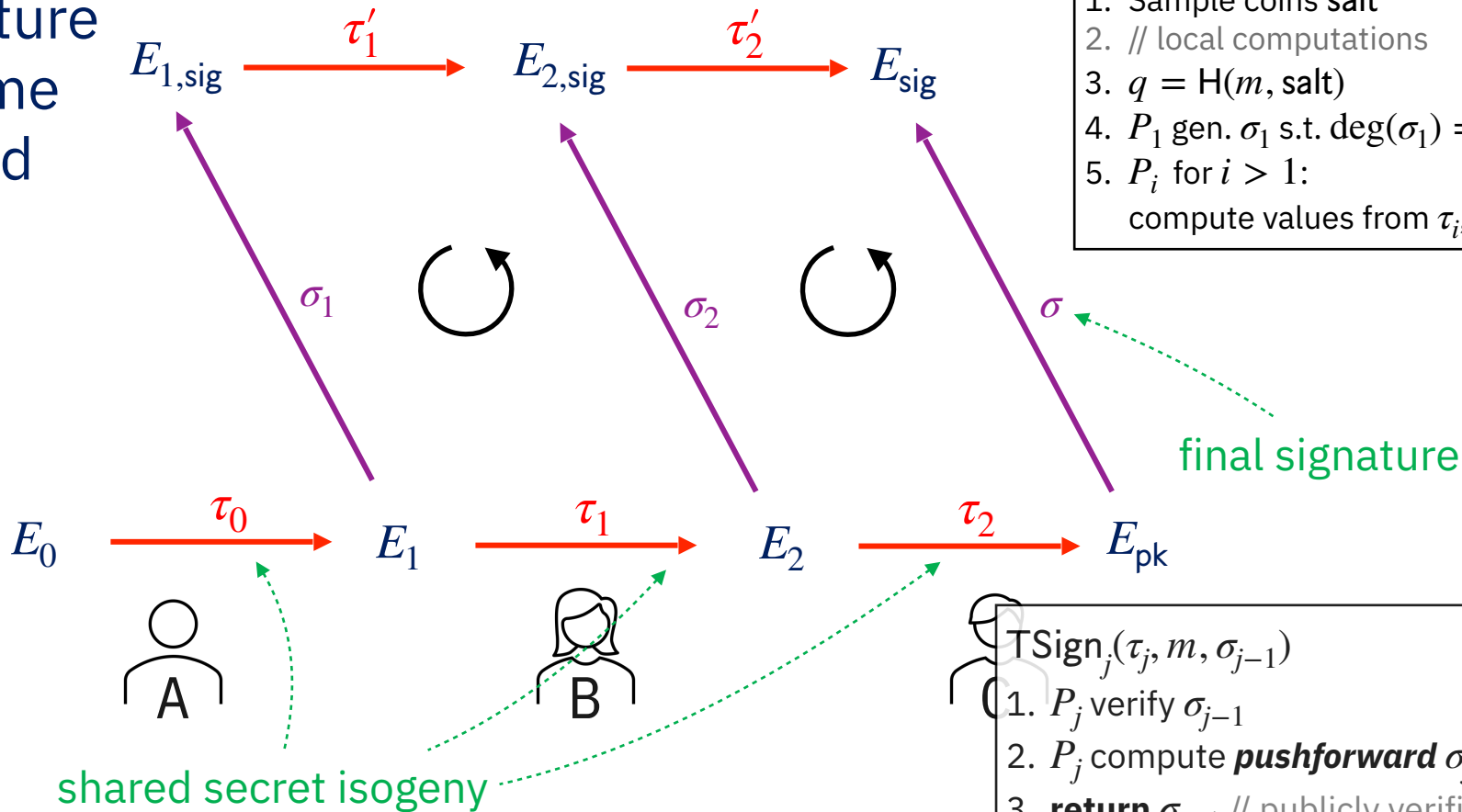
- $\text{Sign}(\tau_{sk}, m)$
1. sample salt, $q \leftarrow H(m, \text{salt})$
 2. // q is a large prime
 3. gen. isogeny σ s.t. $\text{deg}(\sigma) = q$
 4. **return** σ, salt



Can we distribute this?



PRISM Signature Scheme Shared



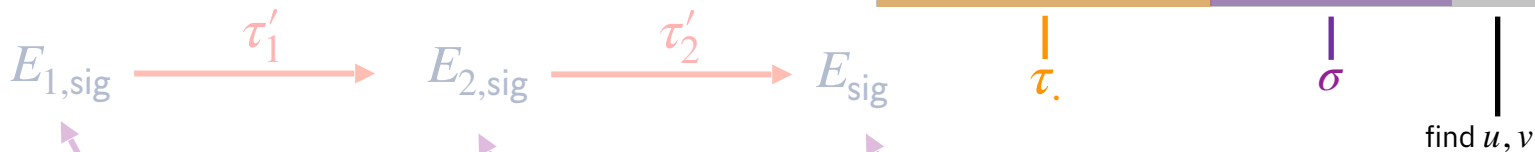
$T\text{Sign}_1(\tau_i, m)$

1. Sample coins salt
2. // local computations
3. $q = H(m, \text{salt})$
4. P_1 gen. σ_1 s.t. $\deg(\sigma_1) = q$
5. P_i for $i > 1$:
compute values from τ_i, q

$T\text{Sign}_j(\tau_j, m, \sigma_{j-1})$

1. P_j verify σ_{j-1}
2. P_j compute **pushforward** σ_j
3. **return** σ_{j+1} // publicly verifiable

Open Isogeny Questions



Act as a push-oracle

Strong and new assumption

Need to hide $\deg(\tau_i)$

E_0

τ_0

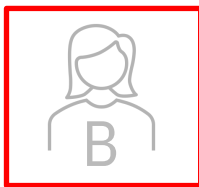
E_1

τ_1

E_2

τ_2

E_{pk}



σ_1



σ_2



σ

Limits:

1. Randomised equation
2. Larger base prime
3. 4D isogenies

Find good u, v s.t.
 $u \deg(\tau_i) + vH(m, \text{salt}) = 2^e \approx p$

CALL FOR FEEDBACKS

Disadvantages

- **New security assumption**
- No offline/online split
- **Sequential** operations
- Complex signing
- **NO Distributed KeyGen**

Advantages

- Support general (T,N), up to 32, using Recursive Secret Sharing
- Public Verification of Partial Signatures
- Faster: $\approx T \cdot 110$ ms
- **Compact** Sigs, Pk, Communication

Prime	Supported Sigs	Pk. Size (B)	Sig. Size (B)	
			Compressed	Uncompressed
$2^{435} \cdot 91 - 1$	2^{64}	110	217	241
$2^{373} \cdot 121 - 1$	2^{32}	95	190	210