Concurrent Signatures

Samir Benzammour

Algorithms and Computational Complexity
RWTH Aachen University

27th April 2020

Overview

σ: $\langle s, h_1, f \rangle$

Overview

σ: $\langle s, h_1, f \rangle$

S: $\langle \sigma, X_i, X_j, M \rangle$

Overview

σ: $\langle s, h_1, f \rangle$

S: $\langle \sigma, X_i, X_j, M \rangle$

queries:

- **KGen**
- **KReveal**
- **ASign**
- **AVerify / Verify**
- **Private Key Extraction**

Overview

σ: $\langle s, h_1, f \rangle$

S: $\langle \sigma, X_i, X_j, M \rangle$

queries:

- **KGen**
- **KReveal**
- **ASign**
- **AVerify / Verify**
- **Private Key Extraction**

spaces: $\mathcal{S} \equiv \mathcal{F} = \mathbb{Z}_q$ and $\mathcal{M} \equiv \mathcal{K} = \{0,1\}^*$