(Full) Leakage Resilience of Fiat-Shamir Signatures over Lattices

Yuejun LIU, Yongbin ZHOU, Rui ZHANG, Yang TAO

Frontiers of Computer Science, DOI: 10.1007/s11704-021-0586-3

Problems & Ideas

- The security of lattice-based Fiat-Shamir signature (FS-Sig) schemes in the presence of leakage is a relatively under-explored topic.
  - Fiat-Shamir is a mainstream construction paradigm of lattice-based signature schemes.
  - Some side-channel attacks on lattice-based FS-Sig schemes have been proposed since 2016, little work on the leakage resilience appears .
- The proof idea of the leakage resilience of FS-Sig schemes based on traditional number-theoretic assumptions does not apply to most lattice-based FS-Sig schemes.

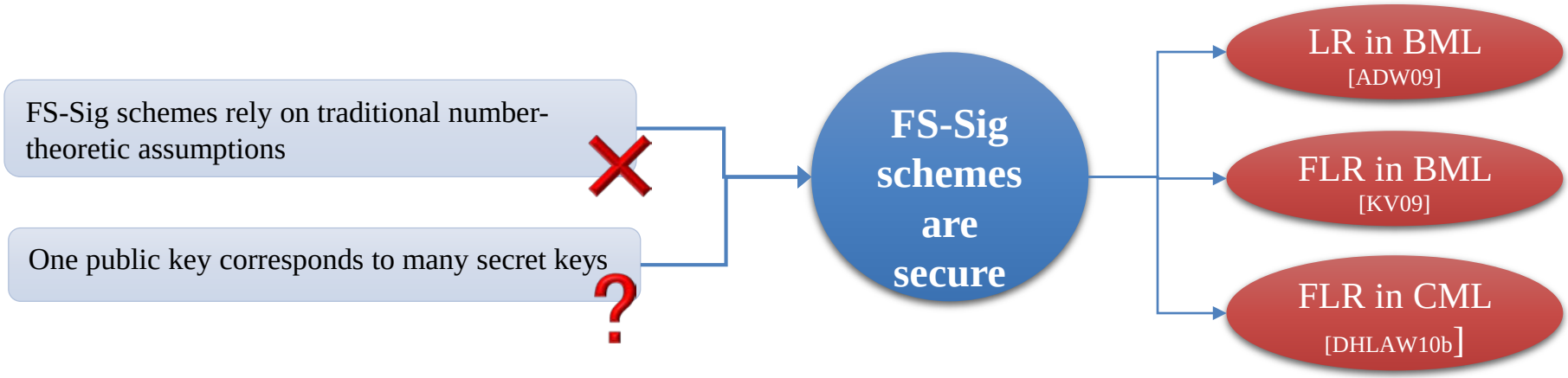

Fig.1 The Original Proof Idea in [ADW09, KV09, DHLAW10b]

Main Contributions

- **The work proposes a framework to construct fully leakage resilient lattice-based FS-Sig schemes in the bounded memory leakage (BML) model.**
  - First, the work constructs leakage resilient FS-Sig schemes in BML model from non-lossy or lossy identification (ID) schemes and instantiates ID schemes based on lattice assumptions.
  - Second, the work constructs fully leakage resilient FS-Sig schemes from leakage resilient ones.

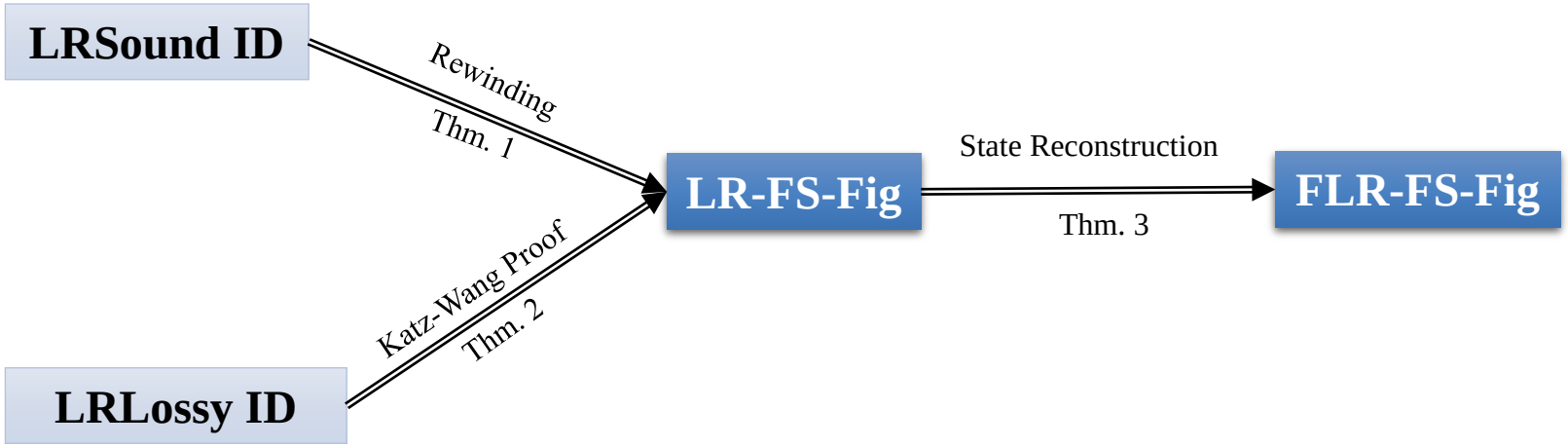

Fig.2 The High-Level Overview of Our Framework