ReSolveD: Shorter Signatures from Regular Syndrome Decoding and VOLE-in-the-Head

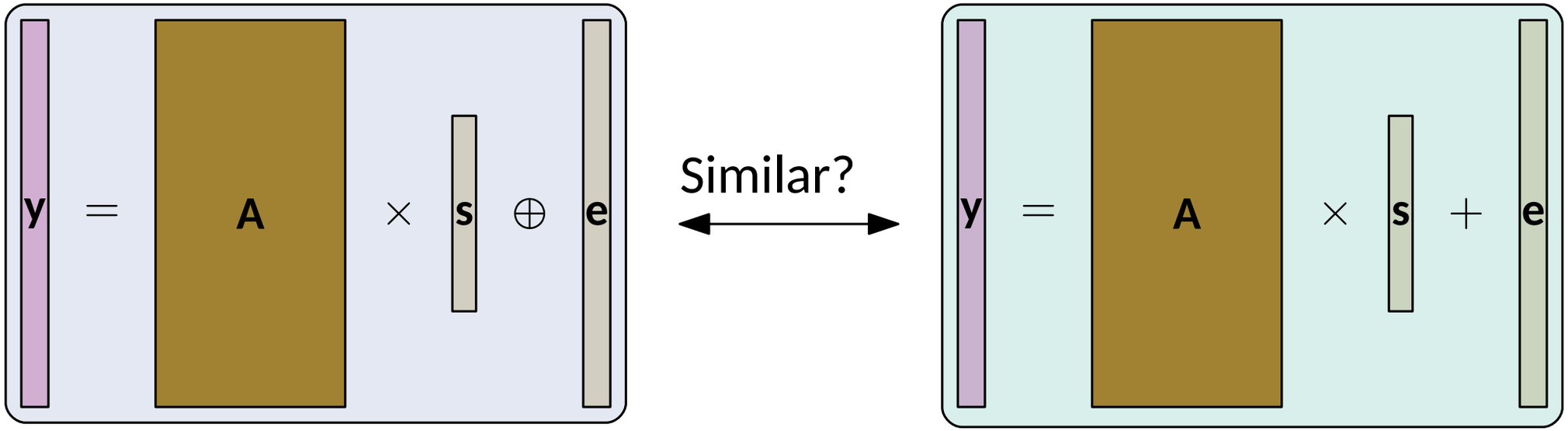
Hongrui Cui, Shanghai Jiao Tong University
Joint work with

Hanlin Liu, Shanghai Qi Zhi Institute
Di Yan, State Key Laboratory of Cryptology
Kang Yang, State Key Laboratory of Cryptology
Yu Yu, Shanghai Jiao Tong University
Kaiyi Zhang, Shanghai Jiao Tong University

In Submission

Motivations

- Consider **L**earning **P**arity with **N**oise (aka, **S**yndrome **D**ecoding.)
- $(\mathbf{A}, \mathbf{y}) \approx (\mathbf{A}, U)$, for low-Hamming weight $\mathbf{s}, \mathbf{e}$



LPN: over $\mathbb{F}_2$ LWE: over $\mathbb{F}_q$

- We have very efficient LWE-based signatures ([GPV08, Lyu12, ...])
- How about LPN-based?

Motivations

- Rejection sampling does not work on Hamming metric
- Nor do we know how to place a trapdoor in **A**
- So what now?

Motivations

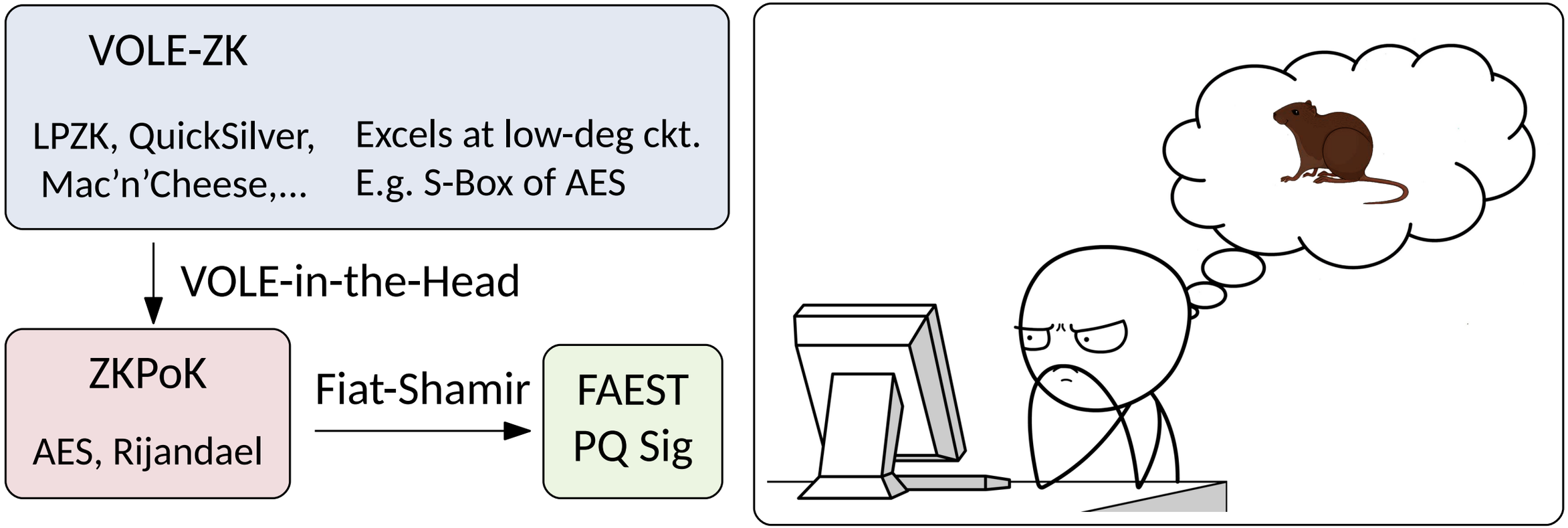
- Rejection sampling does not work on Hamming metric
- Nor do we know how to place a trapdoor in **A**
- So what now?

- Luckily, arithmetic over $\mathrm{GF}(2)$ is friendly to MPC

- A number of existing works with increasingly better efficiency…
- e.g. [GPS21, FJR21, BGKM22, FJR22, CCR23]

Exciting New Tools: VOLEitH

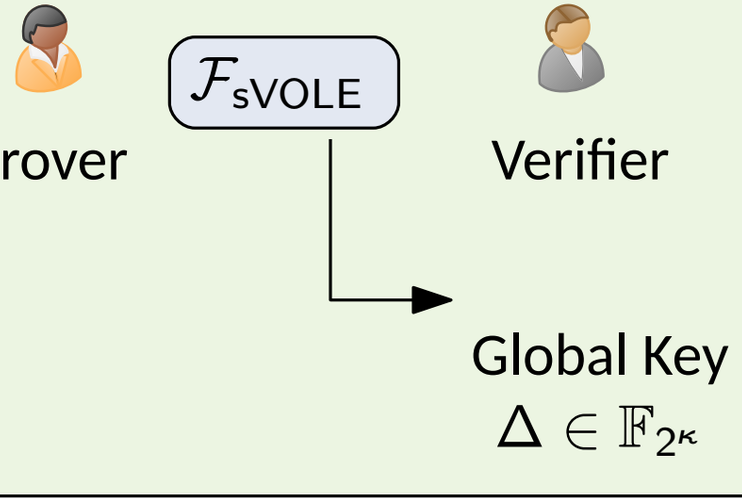
- Provides new method to convert VOLE-ZK to ZKPoK



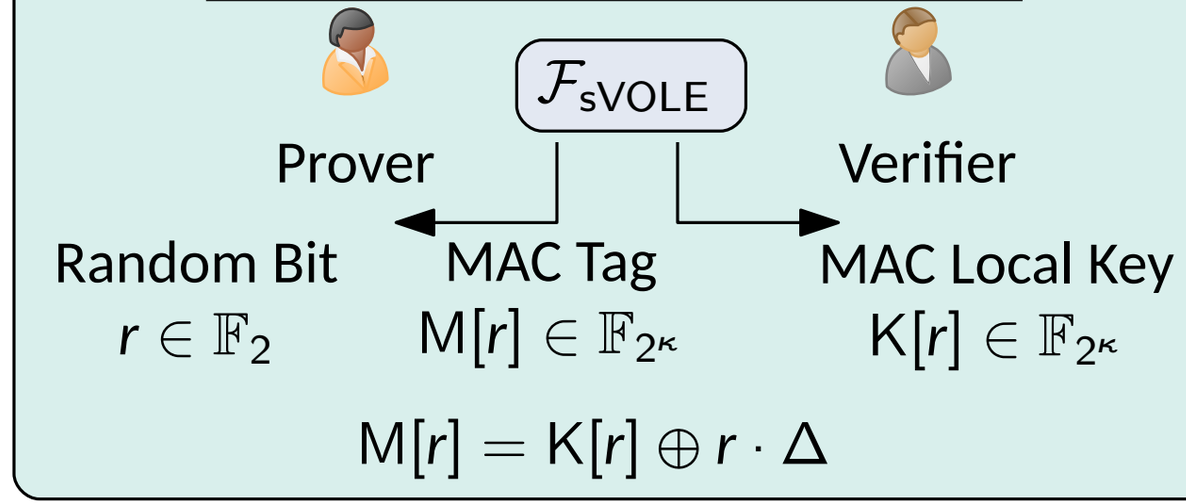
- BBD+23: Publicly Verifiable Zero-Knowledge and Post-Quantum Signatures from VOLE-in-the-Head (Crypto 2023)

(The Only) Preliminary

Initialization

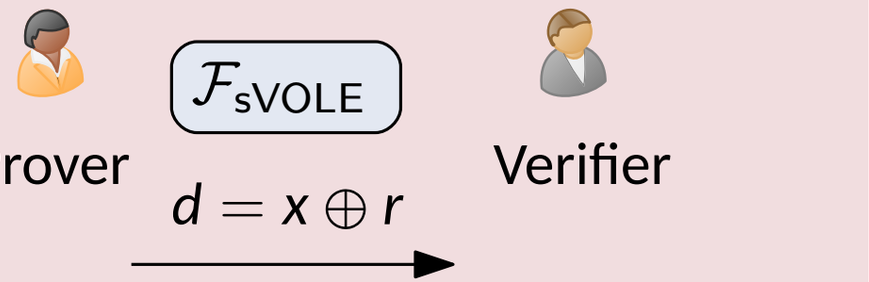


Generating Random Correlations



$$M[r] = K[r] \oplus r \cdot \Delta$$

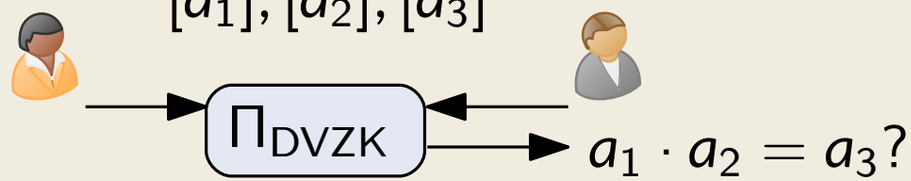
Input Commitment



commit to x by sending diff.

$$M[x] = M[r] \qquad K[x] = K[r] \oplus d \cdot \Delta$$

Proving AND Relation

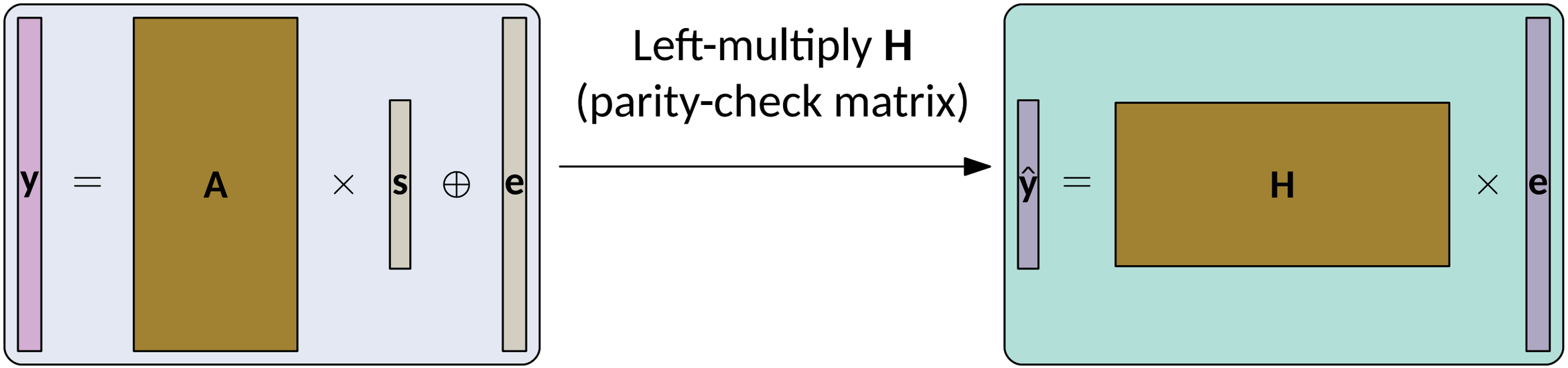


$$K_1K_2 \oplus \Delta K_3 = (a_1a_2 \oplus a_3)\Delta^2$$
$$\oplus\,(a_1M_2 \oplus a_2M_1 \oplus M_3)\Delta \oplus M_1M_2$$

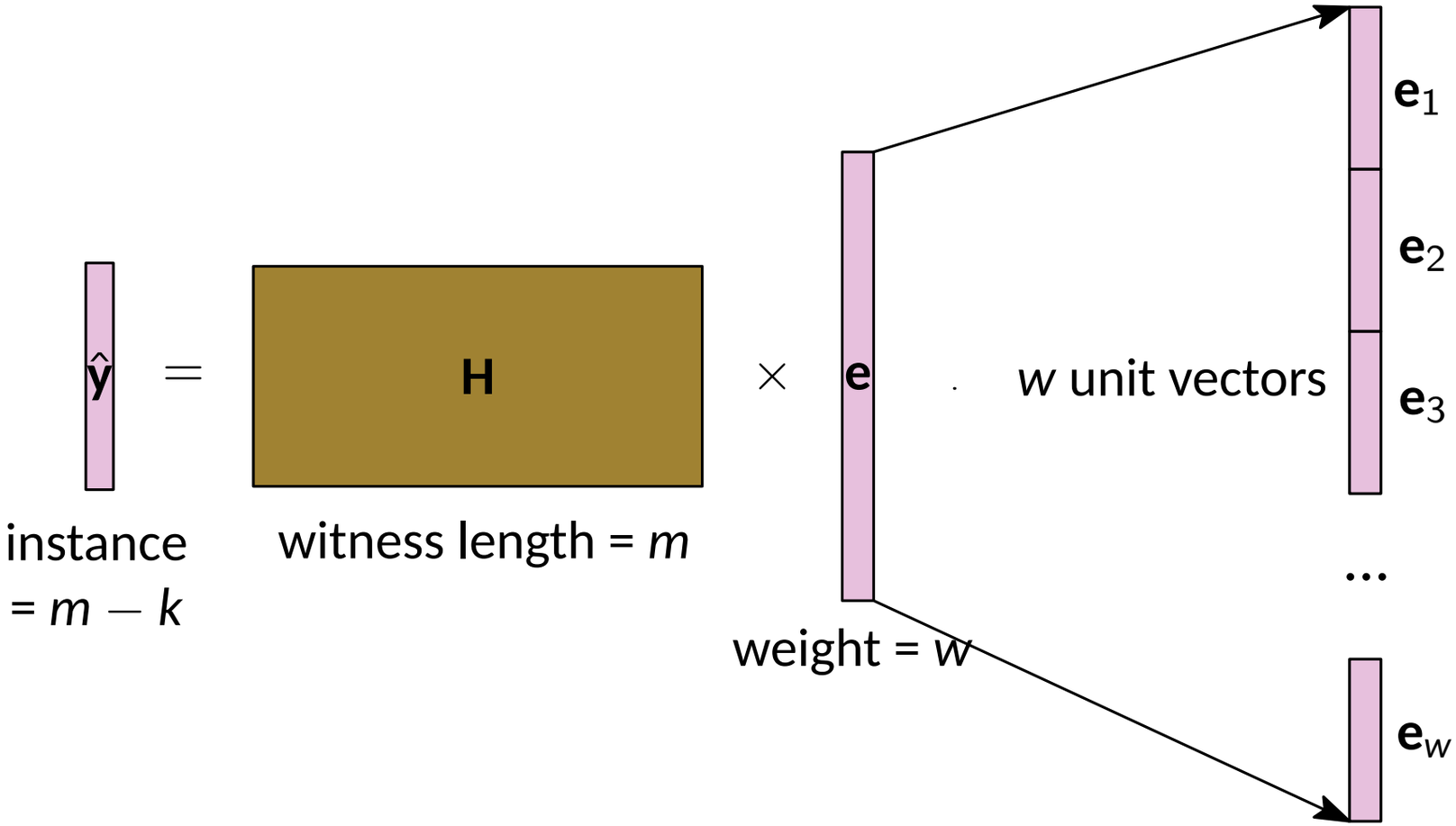
Let’s try it on LPN/SD

- Main technical challenge:
- Proving low-hamming weight of **e**

- Step 1: Convert LPN to dual form

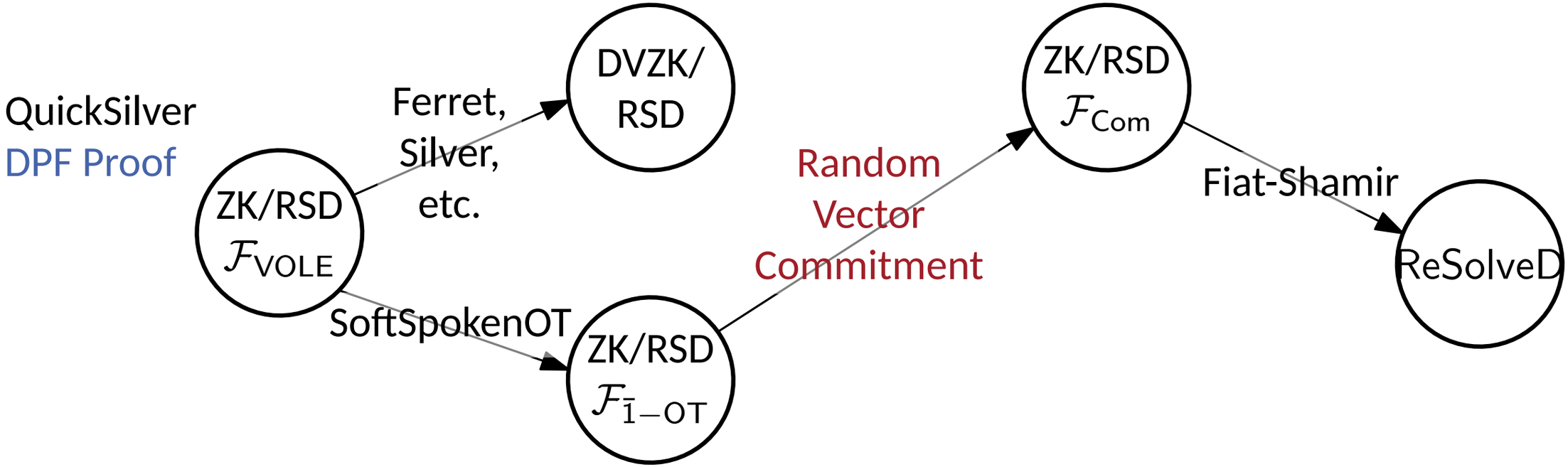


To Make our Life Easier...



- Systematic Form: $\mathbf{H} = [\mathbf{I}_{m-k} \| \mathbf{H_B}]$
- $\hat{\mathbf{y}} = \mathbf{H} \cdot \mathbf{e} = \mathbf{e}_A + \mathbf{H_B} \cdot \mathbf{e}_B$
- We only commit and get $[\mathbf{e}_B]$ and reconstruct $[\mathbf{e}] = [\hat{\mathbf{y}} - \mathbf{H_B} \cdot \mathbf{e}_B \| \mathbf{e}_B]$

Contributions



- Contribution 1: Combine DPF proof with VOLE-in-the-Head
- Contribution 2: Use half-tree to optimize computational performance

Thanks for your listening

Long Live the Code-based Crypto