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

Hongrui Cui[1] **Hanlin Liu**[2] **Di Yan**[3] **Kang Yang**[3] **Yu Yu**[1,2] **Kaiyi Zhang**[1]

Shanghai Jiao Tong University[1] · Shanghai Qi Zhi Institute[2] · State Key Laboratory of Cryptology[3]

Apr. 16, 2024 · PKC 2024

Synopsis

- **Motivation**
- Vector-OLE in the Head
- Proving RSD in VOLE-hybrid Model
- Results

Motivation: Post-Quantum Signature

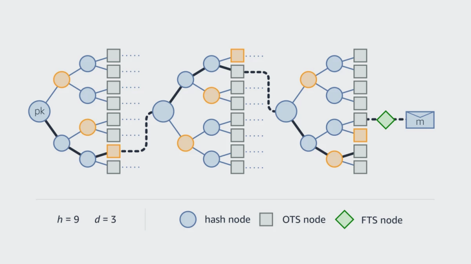
- Digital Signature is the backbone of the Internet
- Quantum computation threats traditional digital signatures
- NIST PQC Standardization Process

Algorithms to be standardized by NIST

- CRYSTALS-DILITHIUM
- FALCON
- SPHINCS+

FALCON

Fast-Fourier Lattice-based
Compact Signatures over NTRU



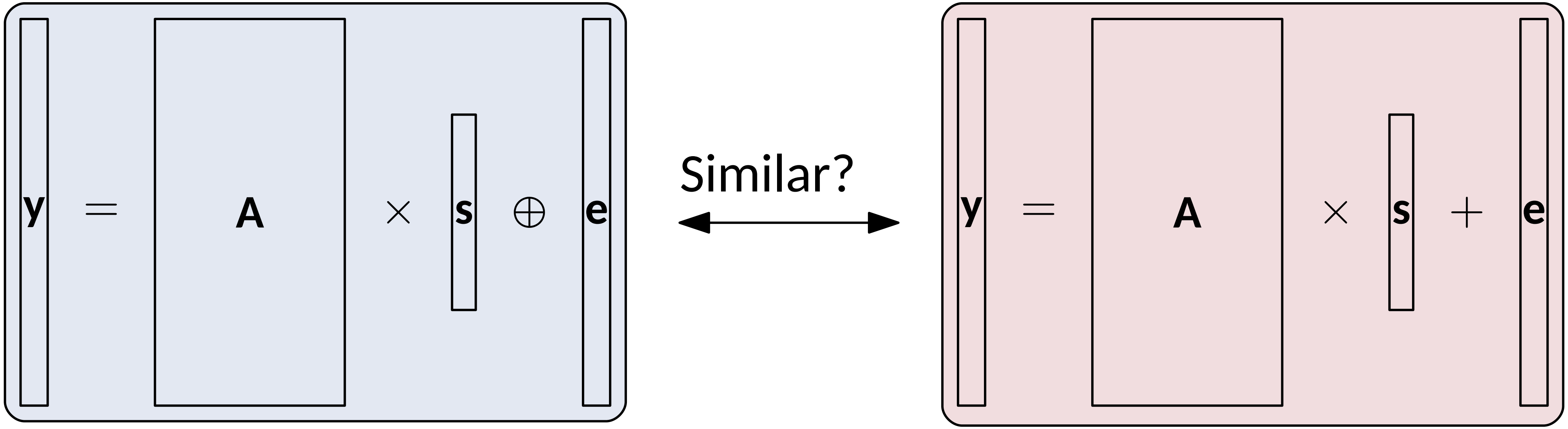
Lattice-based

Hash-based

- NIST Additional Round of Digital Signature Standardization

PQ-Sig from LPN?

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



LPN: over $\mathbb{F}_2$

LWE: over $\mathbb{Z}_p$

- LPN has a similar form compared to LWE (Hamming vs. L2)
- LWE and its variants allow very efficient PQ-Sig
- How about LPN-based signatures?

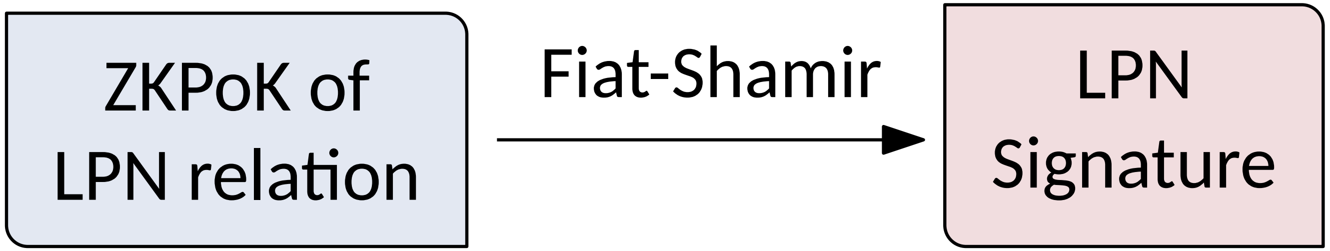
Unfortunately, LPN is very Different from LWE

- Rejection sampling does not work on Hamming metric
- Nor do we know how to embed trapdoor in $\mathbf{A}$
- So what now?

Unfortunately, LPN is very Different from LWE

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

- Digital Signature = ZK + OWF

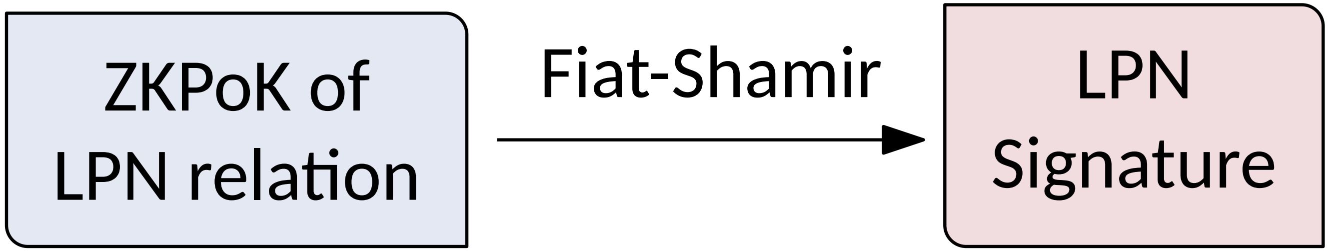

ZKPoK of LPN relation

Fiat-Shamir

LPN Signature

Unfortunately, LPN is very Different from LWE

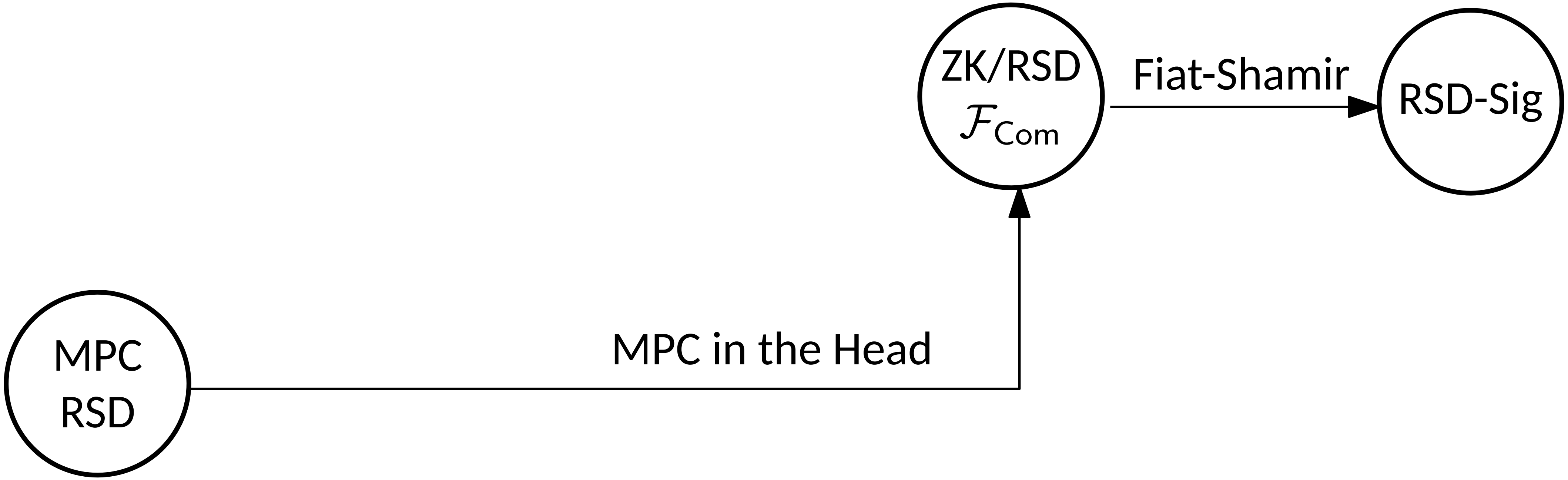
- Rejection sampling does not work on Hamming metric
- Nor do we know how to embed trapdoor in **A**
- So what now?
- Digital Signature = ZK + OWF



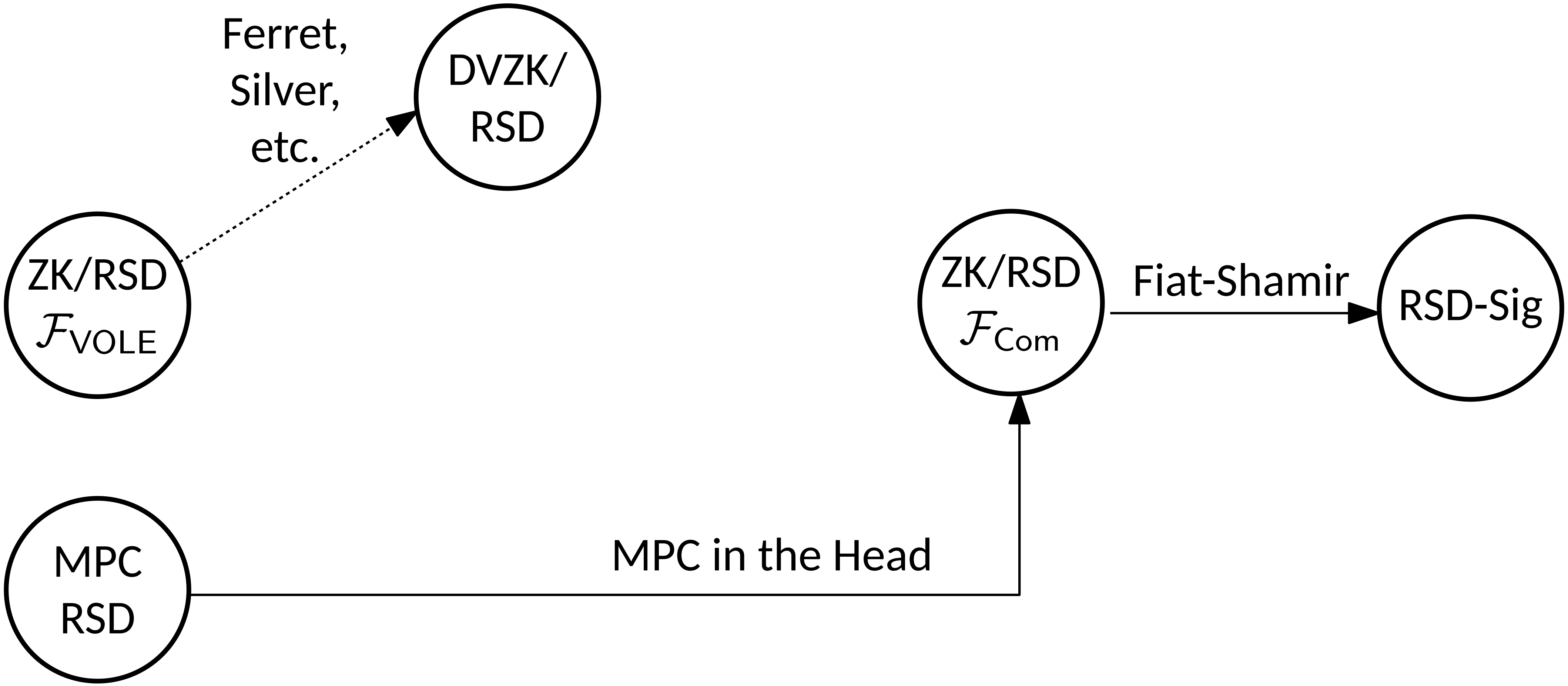
- GF(2) allows very efficient MPC
- “MPC in the Head” allows converting MPC into ZKP [IKOS07]

- A number of existing works with increasingly better efficiency...
- Papers: [GPS21, FJR21, BGKM22, FJR22, CCR23, AGHHJY23, FR23]
- NIST Submissions: SDitH

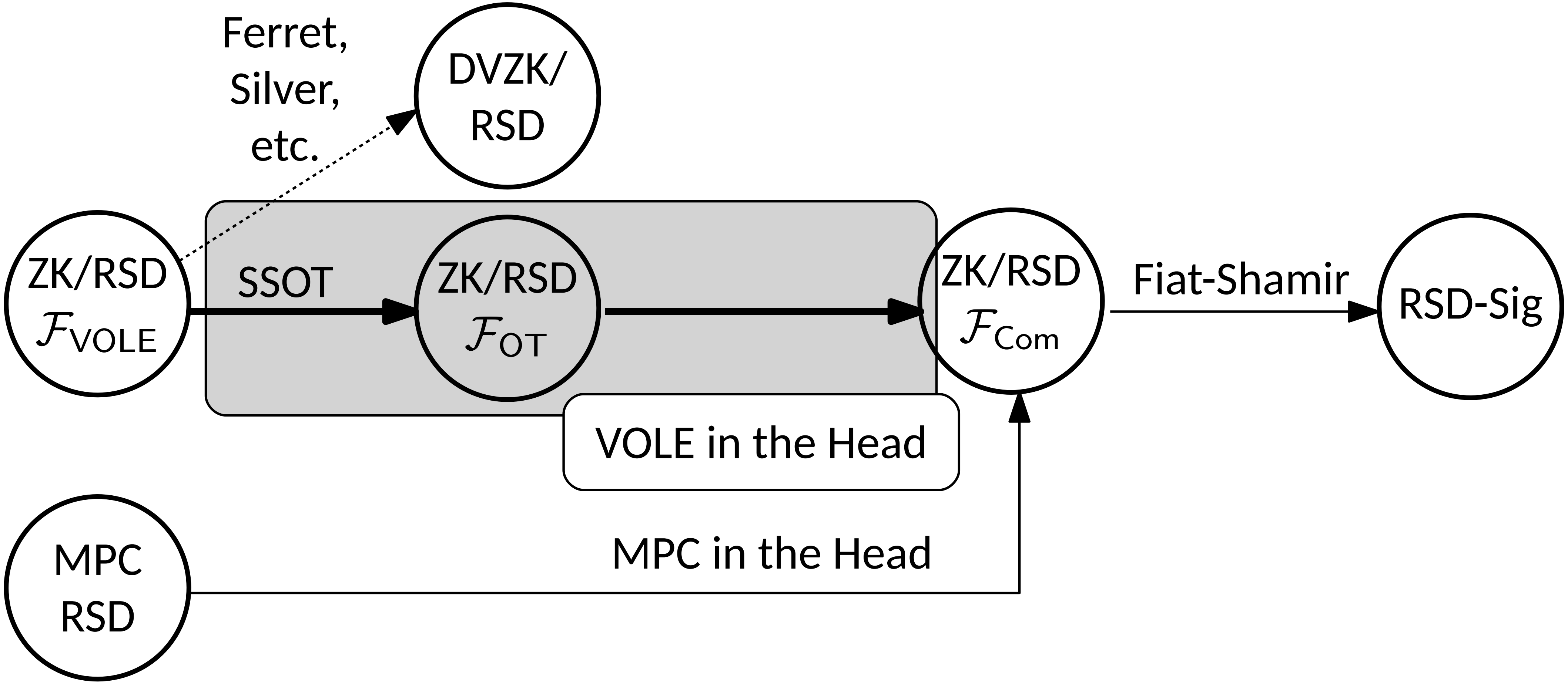
Contributions



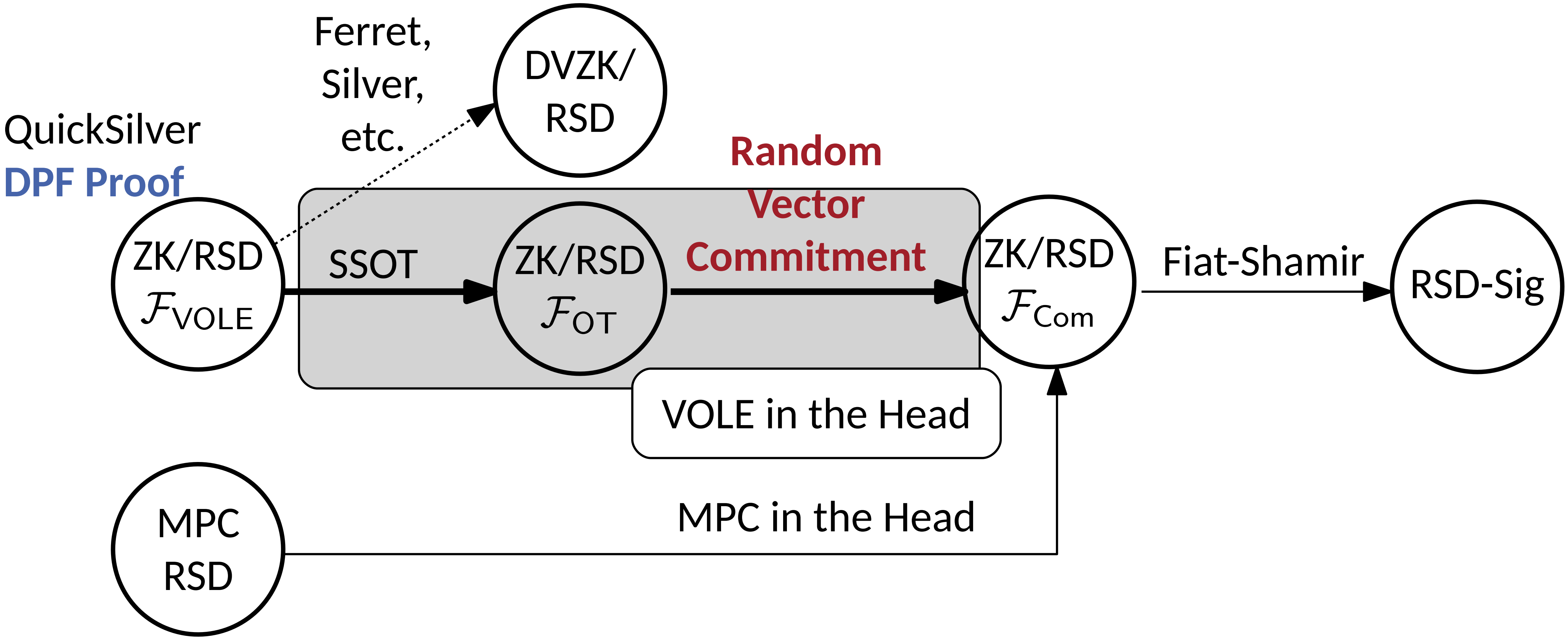
Contributions



Contributions



Contributions



Ferret, Silver, etc.

DVZK/ RSD

QuickSilver

DPF Proof

ZK/RSD $\mathcal{F}_{\text{VOLE}}$

SSOT

ZK/RSD $\mathcal{F}_{\text{OT}}$

Random Vector Commitment

ZK/RSD $\mathcal{F}_{\text{Com}}$

Fiat-Shamir

RSD-Sig

VOLE in the Head

MPC RSD

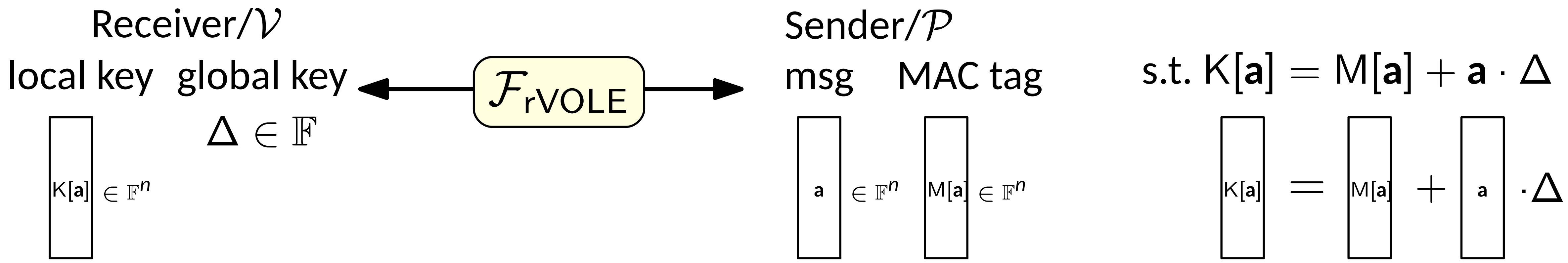
MPC in the Head

- Contribution 1: Combine **DPF sketch** with **VOLE-in-the-Head**
- Contribution 2: Use **half-tree** to optimize computational performance
- The resulting signature scheme demonstrates smaller signatures with comparable running time*

Synopsis

- Motivation
- **Vector-OLE in the Head**
- Proving RSD in VOLE-hybrid Model
- Results

VOLE-based DVZK



Receiver/$\mathcal{V}$

local key global key

$\mathsf{K}[\mathbf{a}] \in \mathbb{F}^n$

$\Delta \in \mathbb{F}$

$\mathcal{F}_{\text{rVOLE}}$

Sender/$\mathcal{P}$

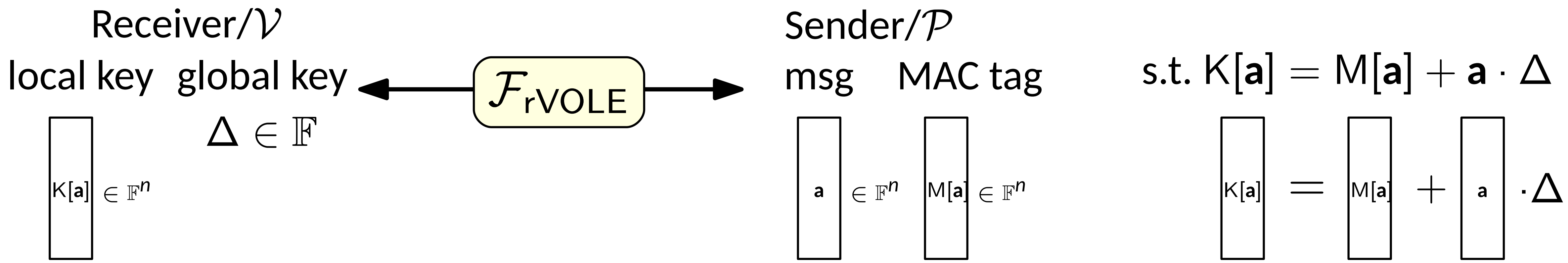
msg MAC tag

$\mathbf{a} \in \mathbb{F}^n$ $\mathsf{M}[\mathbf{a}] \in \mathbb{F}^n$

s.t. $\mathsf{K}[\mathbf{a}] = \mathsf{M}[\mathbf{a}] + \mathbf{a} \cdot \Delta$

$$\boxed{\mathsf{K}[\mathbf{a}]} = \boxed{\mathsf{M}[\mathbf{a}]} + \boxed{\mathbf{a}} \cdot \Delta$$

VOLE-based DVZK



Receiver/$\mathcal{V}$

local key global key

$\mathsf{K}[\mathbf{a}] \in \mathbb{F}^n$ $\Delta \in \mathbb{F}$

$\mathcal{F}_{\mathsf{rVOLE}}$

Sender/$\mathcal{P}$

msg MAC tag

$\mathbf{a} \in \mathbb{F}^n$ $\mathsf{M}[\mathbf{a}] \in \mathbb{F}^n$

s.t. $\mathsf{K}[\mathbf{a}] = \mathsf{M}[\mathbf{a}] + \mathbf{a} \cdot \Delta$

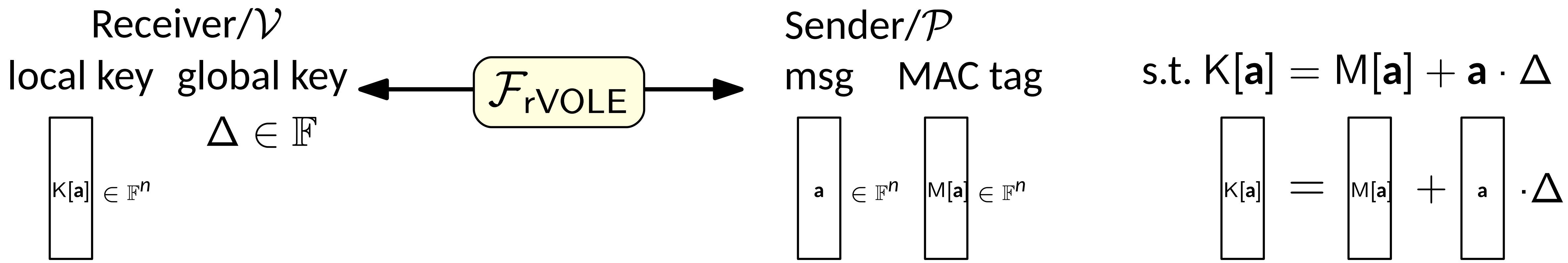
$\mathsf{K}[\mathbf{a}] = \mathsf{M}[\mathbf{a}] + \mathbf{a} \cdot \Delta$

IT-MAC $[\![\mathbf{a}]\!] := (\mathbf{a}, \mathsf{M}[\mathbf{a}], \mathsf{K}[\mathbf{a}])$ subject to $\mathsf{K}[\mathbf{a}] = \mathsf{M}[\mathbf{a}] + \mathbf{a} \cdot \Delta$

- Open($[\![a]\!]$): $\mathcal{P} \to \mathcal{V}$: $(a, \mathsf{M}[a])$, $\mathcal{V}$ checks $\mathsf{K}[a] = \mathsf{M}[a] + a \cdot \Delta$

- $\mathcal{P}$ opens a different value $\to$ $\mathcal{P}$ guesses Δ
- Soundness error $= \frac{1}{|\mathbb{F}|} = 2^{-\lambda}$

VOLE-based DVZK



Receiver/$\mathcal{V}$

local key global key

$\mathcal{F}_{\text{rVOLE}}$

Sender/$\mathcal{P}$

msg MAC tag

s.t. $\mathsf{K}[\mathbf{a}] = \mathsf{M}[\mathbf{a}] + \mathbf{a} \cdot \Delta$

$\mathsf{K}[\mathbf{a}] \in \mathbb{F}^n$ $\quad \Delta \in \mathbb{F}$

$\mathbf{a} \in \mathbb{F}^n$ $\quad \mathsf{M}[\mathbf{a}] \in \mathbb{F}^n$

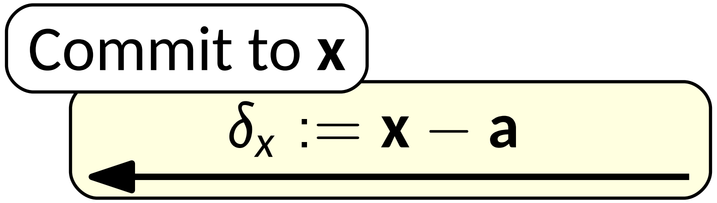
$\mathsf{K}[\mathbf{a}] = \mathsf{M}[\mathbf{a}] + \mathbf{a} \cdot \Delta$

IT-MAC $[\![\mathbf{a}]\!] := (\mathbf{a}, \mathsf{M}[\mathbf{a}], \mathsf{K}[\mathbf{a}])$ subject to $\mathsf{K}[\mathbf{a}] = \mathsf{M}[\mathbf{a}] + \mathbf{a} \cdot \Delta$

- Open($[\![a]\!]$): $\mathcal{P} \to \mathcal{V} : (a, \mathsf{M}[a])$, $\mathcal{V}$ checks $\mathsf{K}[a] = \mathsf{M}[a] + a \cdot \Delta$

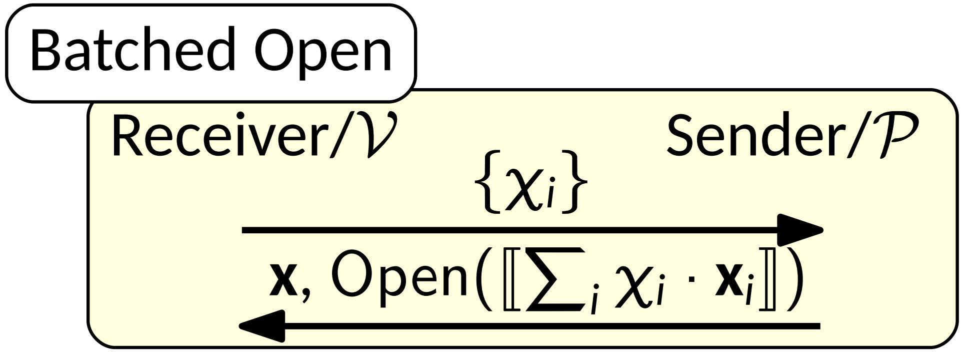
- $\mathcal{P}$ opens a different value $\to$ $\mathcal{P}$ guesses Δ
- Soundness error $= \frac{1}{|\mathbb{F}|} = 2^{-\lambda}$

- Linear Homomorphism: $[\![x]\!] + [\![y]\!] \mapsto [\![x + y]\!]$



Commit to $\mathbf{x}$

$\delta_x := \mathbf{x} - \mathbf{a}$



Batched Open

Receiver/$\mathcal{V}$ Sender/$\mathcal{P}$

$\{\chi_i\}$

$\mathbf{x}$, Open($[\![\sum_i \chi_i \cdot \mathbf{x}_i]\!]$)

Starting Point: DVZK for Quadratic Relations

Prove $a_1 \times a_2 = a_3$ $\underbrace{\mathsf{K}[\mathbf{a}] = \Delta}_{\mathcal{V}} \cdot \underbrace{\mathbf{a} + \mathsf{M}[\mathbf{a}]}_{\mathcal{P}}$

Starting Point: DVZK for Quadratic Relations

Prove $a_1 \times a_2 = a_3$

$$\underbrace{\mathsf{K}[\mathbf{a}] = \Delta}_{\mathcal{V}} \cdot \underbrace{\mathbf{a} + \mathsf{M}[\mathbf{a}]}_{\mathcal{P}}$$

$$\underbrace{\mathsf{K}[a_1] \cdot \mathsf{K}[a_2] - \Delta \cdot \mathsf{K}[a_3]}_{B} = (\mathsf{M}[a_1] + a_1 \cdot \Delta) \cdot (\mathsf{M}[a_2] + a_2 \cdot \Delta) - \Delta \cdot (\mathsf{M}[a_3] + a_3 \cdot \Delta)$$

$$= (a_1 \cdot a_2 - a_3)\Delta^2 + (\underbrace{a_1\mathsf{M}[a_2] + a_2\mathsf{M}[a_1] - \mathsf{M}[a_3]}_{A_1})\Delta + \underbrace{\mathsf{M}[a_1]\mathsf{M}[a_2]}_{A_0}$$

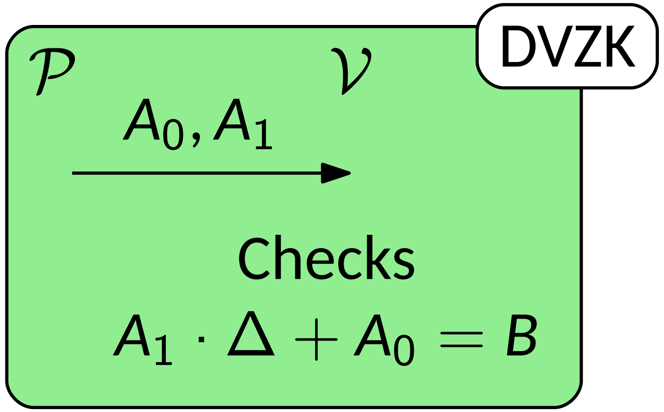
Starting Point: DVZK for Quadratic Relations

Prove $a_1 \times a_2 = a_3$ $\quad \underbrace{\mathsf{K}[\mathbf{a}] = \Delta}_{\mathcal{V}} \cdot \underbrace{\mathbf{a} + \mathsf{M}[\mathbf{a}]}_{\mathcal{P}}$

$$\underbrace{\mathsf{K}[a_1] \cdot \mathsf{K}[a_2] - \Delta \cdot \mathsf{K}[a_3]}_{B} = (\mathsf{M}[a_1] + a_1 \cdot \Delta) \cdot (\mathsf{M}[a_2] + a_2 \cdot \Delta) - \Delta \cdot (\mathsf{M}[a_3] + a_3 \cdot \Delta)$$

$$= (a_1 \cdot a_2 - a_3)\Delta^2 + (\underbrace{a_1\mathsf{M}[a_2] + a_2\mathsf{M}[a_1] - \mathsf{M}[a_3]}_{A_1})\Delta + \underbrace{\mathsf{M}[a_1]\mathsf{M}[a_2]}_{A_0}$$

- Assuming $\mathcal{P}$ and $\mathcal{V}$ has $[\![a_1]\!], [\![a_2]\!], [\![a_3]\!]$
- $\mathcal{P}$ sends A_0, A_1 to prove $a_1 \cdot a_2 = a_3$



Checks

$A_1 \cdot \Delta + A_0 = B$

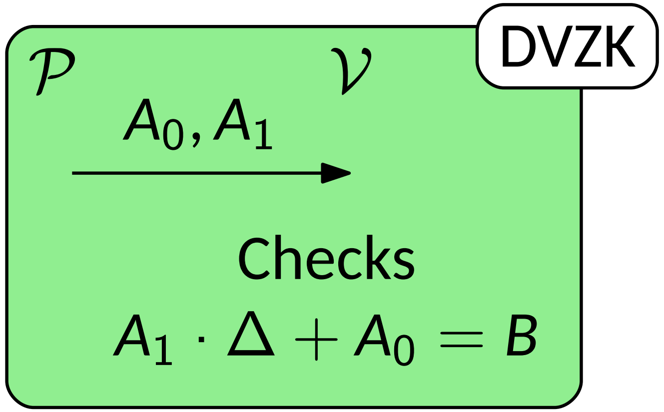
Starting Point: DVZK for Quadratic Relations

$\underline{\text{Prove } a_1 \times a_2 = a_3}$ $\quad \underbrace{\mathsf{K}[\mathbf{a}] = \Delta}_{\mathcal{V}} \cdot \underbrace{\mathbf{a} + \mathsf{M}[\mathbf{a}]}_{\mathcal{P}}$

$$\underbrace{\mathsf{K}[a_1] \cdot \mathsf{K}[a_2] - \Delta \cdot \mathsf{K}[a_3]}_{B} = (\mathsf{M}[a_1] + a_1 \cdot \Delta) \cdot (\mathsf{M}[a_2] + a_2 \cdot \Delta) - \Delta \cdot (\mathsf{M}[a_3] + a_3 \cdot \Delta)$$

$$= (a_1 \cdot a_2 - a_3)\Delta^2 + (\underbrace{a_1\mathsf{M}[a_2] + a_2\mathsf{M}[a_1] - \mathsf{M}[a_3])}_{A_1}\Delta + \underbrace{\mathsf{M}[a_1]\mathsf{M}[a_2]}_{A_0}$$

- Assuming $\mathcal{P}$ and $\mathcal{V}$ has $[\![a_1]\!], [\![a_2]\!], [\![a_3]\!]$
- $\mathcal{P}$ sends A_0, A_1 to prove $a_1 \cdot a_2 = a_3$



DVZK

$\mathcal{P}$ $\qquad$ $\mathcal{V}$

$$\xrightarrow{A_0, A_1}$$

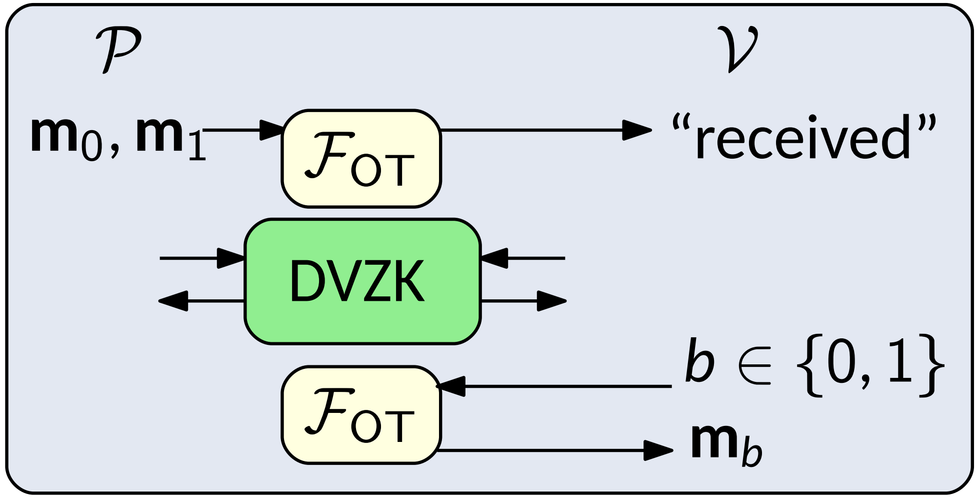
Checks

$A_1 \cdot \Delta + A_0 = B$

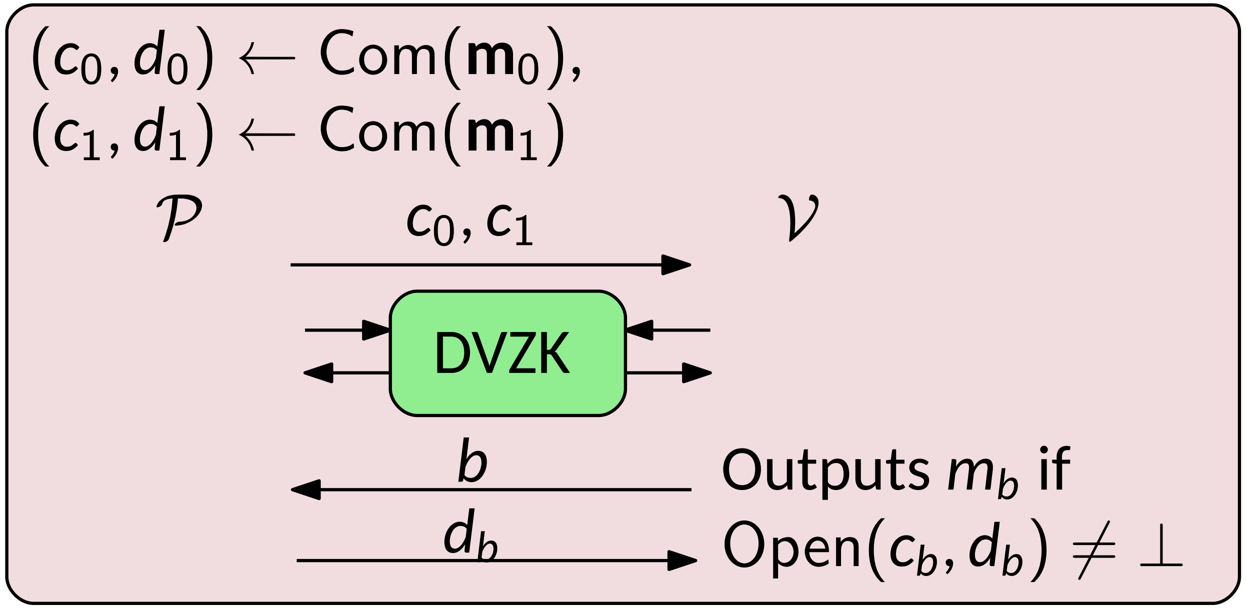
- We can prove multiple quadratic relations using random linear combination
- Sample $\boldsymbol{\chi} = (\chi^{(1)}, \ldots, \chi^{(\ell)})$
- Compute $A_1 = \sum_i \chi^{(i)} A_1^{(i)}, A_0 = \sum_i \chi^{(i)} A_0^{(i)}, B = \sum_i \chi^{(i)} B^{(i)}$
- Soundness loss $= \frac{1}{|\mathbb{F}|} = 2^{-\lambda}$

VOLEitH Step 1: Replace $\mathcal{F}_{\mathrm{OT}}$ by Com&Open

- For public-coin DVZK, we can replace $\binom{2}{1}$-OT with commitment



$\equiv$

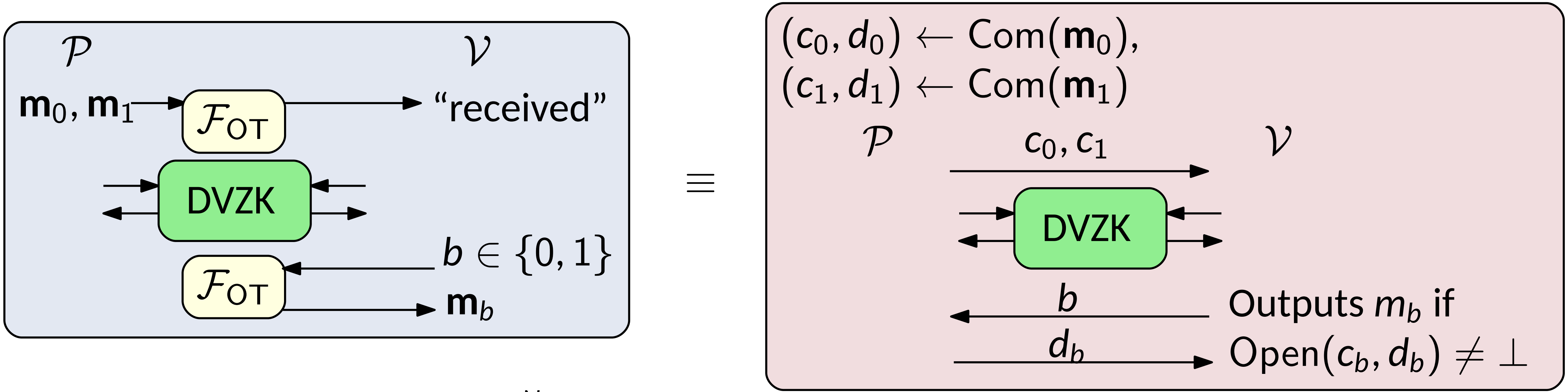


$(c_0, d_0) \leftarrow \mathrm{Com}(\mathbf{m}_0)$,
$(c_1, d_1) \leftarrow \mathrm{Com}(\mathbf{m}_1)$

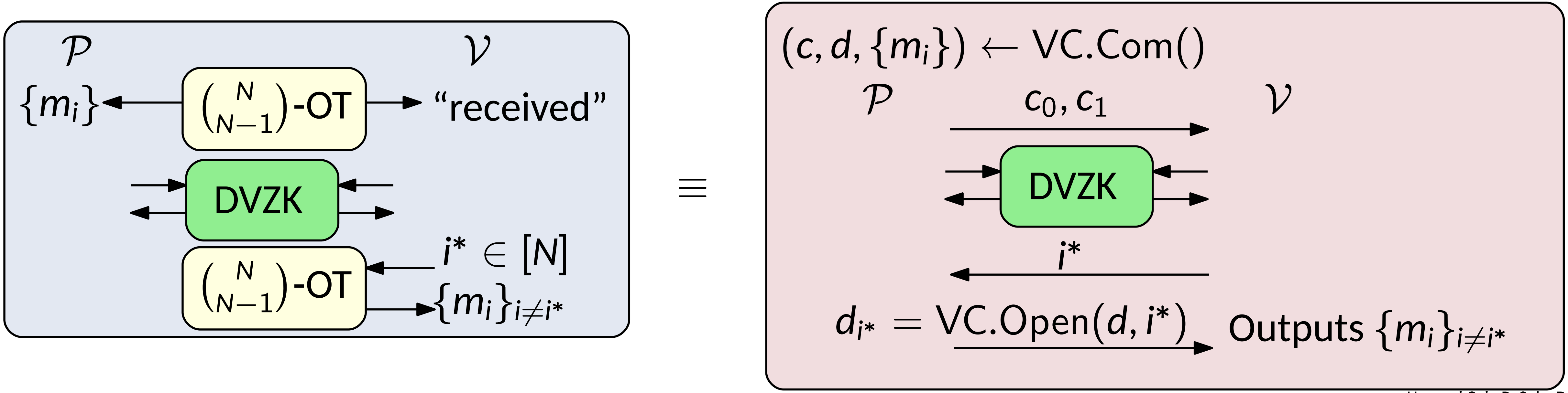
Outputs m_b if
$\mathrm{Open}(c_b, d_b) \neq \bot$

VOLEitH Step 1: Replace $\mathcal{F}_{\mathsf{OT}}$ by Com&Open

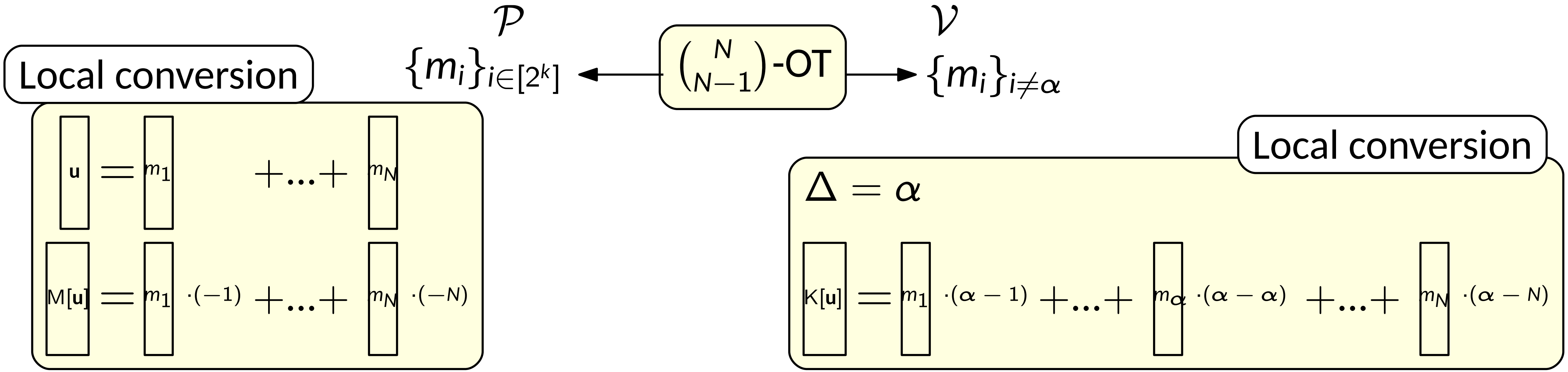
- For public-coin DVZK, we can replace $\binom{2}{1}$-OT with commitment



- Moreover, we can replace $\binom{N}{N-1}$-OT with vector commitment.



VOLEitH Step 2: Small Field VOLE from VC



$\mathcal{P}$

$\{m_i\}_{i\in[2^k]}$ $\longleftarrow$ $\binom{N}{N-1}$-OT $\longrightarrow$ $\{m_i\}_{i\neq\alpha}$

$\mathcal{V}$

Local conversion

$$\mathbf{u} = m_1 + \ldots + m_N$$

$$\mathsf{M}[\mathbf{u}] = m_1 \cdot(-1) + \ldots + m_N \cdot(-N)$$

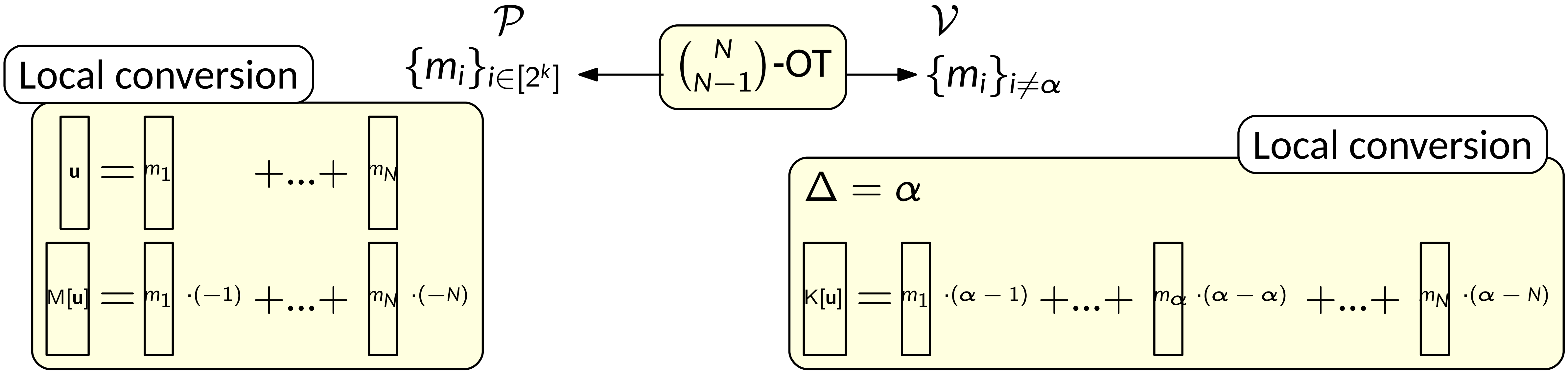
Local conversion

$$\Delta = \alpha$$

$$\mathsf{K}[\mathbf{u}] = m_1 \cdot(\alpha - 1) + \ldots + m_\alpha \cdot(\alpha - \alpha) + \ldots + m_N \cdot(\alpha - N)$$

- The $k = 1$ case underlies the classical [IKNP03] OT extension.
- To achieve λ-bit security, one need $\frac{\lambda}{k}$ instances of depth k GGM trees

VOLEitH Step 2: Small Field VOLE from VC



$\mathcal{P}$

$\{m_i\}_{i\in[2^k]} \longleftarrow \binom{N}{N-1}\text{-OT} \longrightarrow \{m_i\}_{i\neq\alpha}$

$\mathcal{V}$

Local conversion

$$\mathbf{u} = m_1 + \ldots + m_N$$

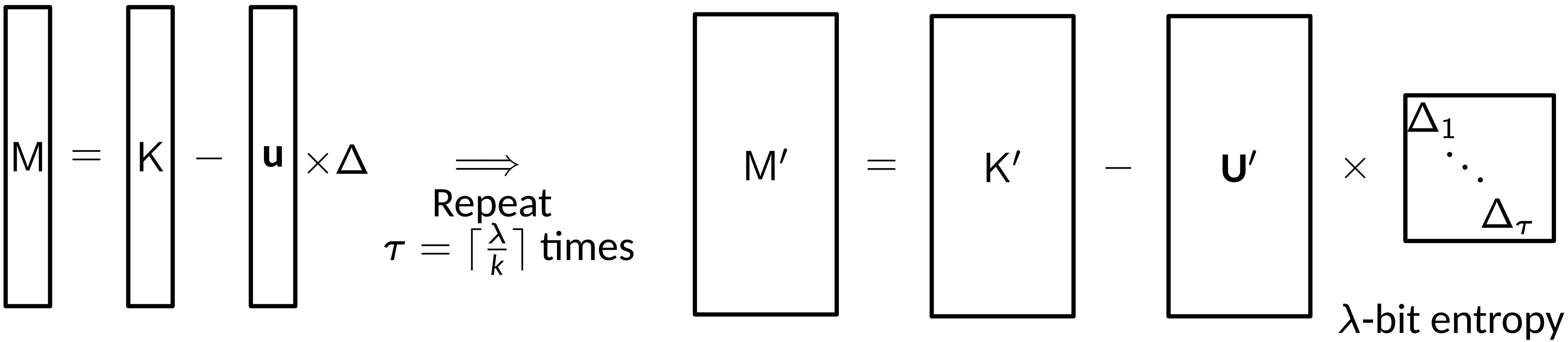
$$\mathsf{M}[\mathbf{u}] = m_1 \cdot (-1) + \ldots + m_N \cdot (-N)$$

Local conversion

$$\Delta = \alpha$$

$$\mathsf{K}[\mathbf{u}] = m_1 \cdot (\alpha - 1) + \ldots + m_\alpha \cdot (\alpha - \alpha) + \ldots + m_N \cdot (\alpha - N)$$

- The $k = 1$ case underlies the classical [IKNP03] OT extension.
- To achieve λ-bit security, one need $\frac{\lambda}{k}$ instances of depth k GGM trees

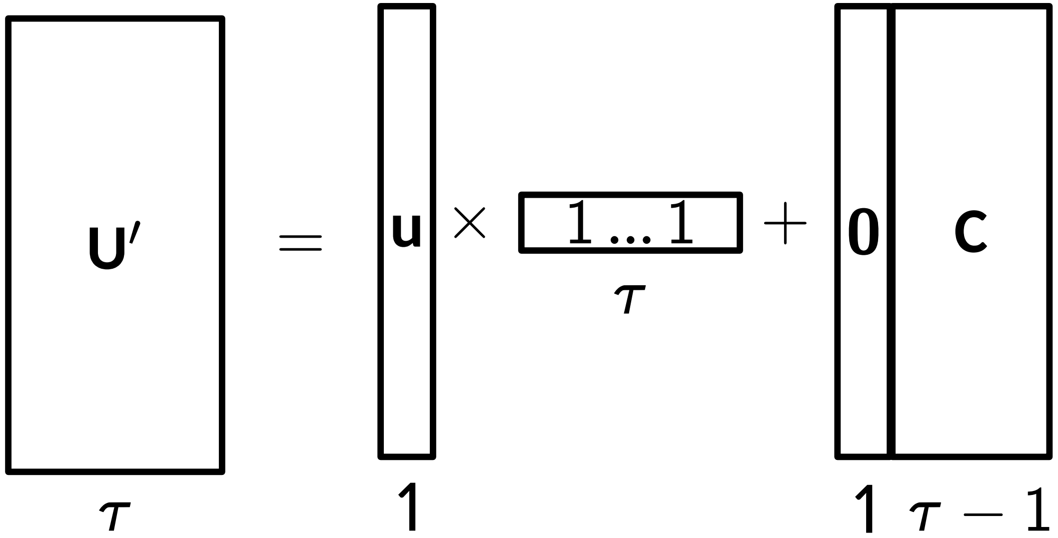


$$\mathsf{M} = \mathsf{K} - \mathbf{u} \times \Delta \quad \underset{\tau = \lceil \frac{\lambda}{k} \rceil \text{ times}}{\overset{\Longrightarrow}{\text{Repeat}}} \quad \mathsf{M}' = \mathsf{K}' - \mathbf{U}' \times \begin{pmatrix} \Delta_1 & & \\ & \ddots & \\ & & \Delta_\tau \end{pmatrix}$$

λ-bit entropy

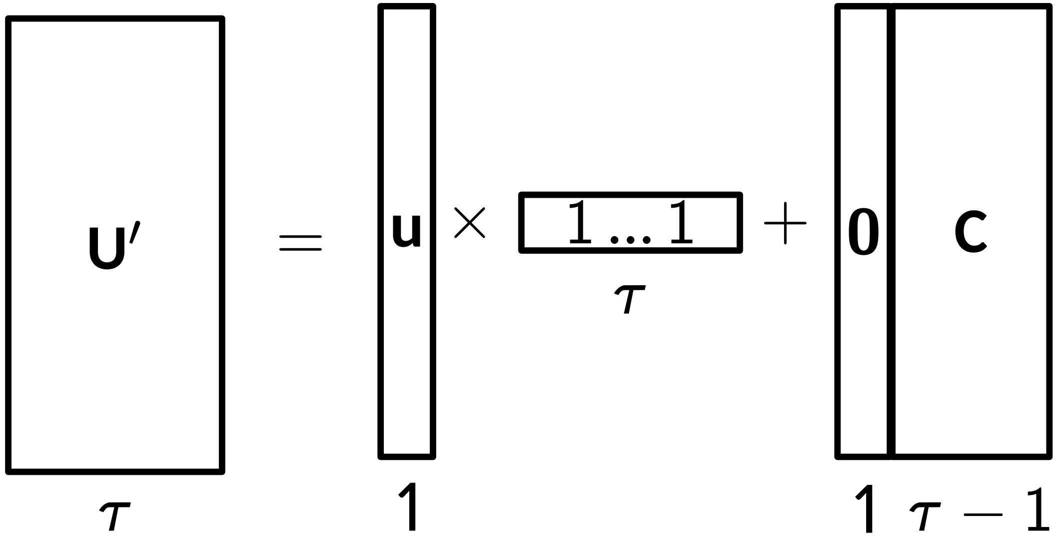
VOLEitH Step 3: Merge Small Field VOLE into Large Field VOLE

- $\mathcal{P}$ sends syndrome **C** to $\mathcal{V}$
- $\mathcal{V}$ locally sets $\mathsf{K} = \mathsf{K}' - [0 \| \mathbf{C}] \cdot \text{diag}(\boldsymbol{\Delta})$

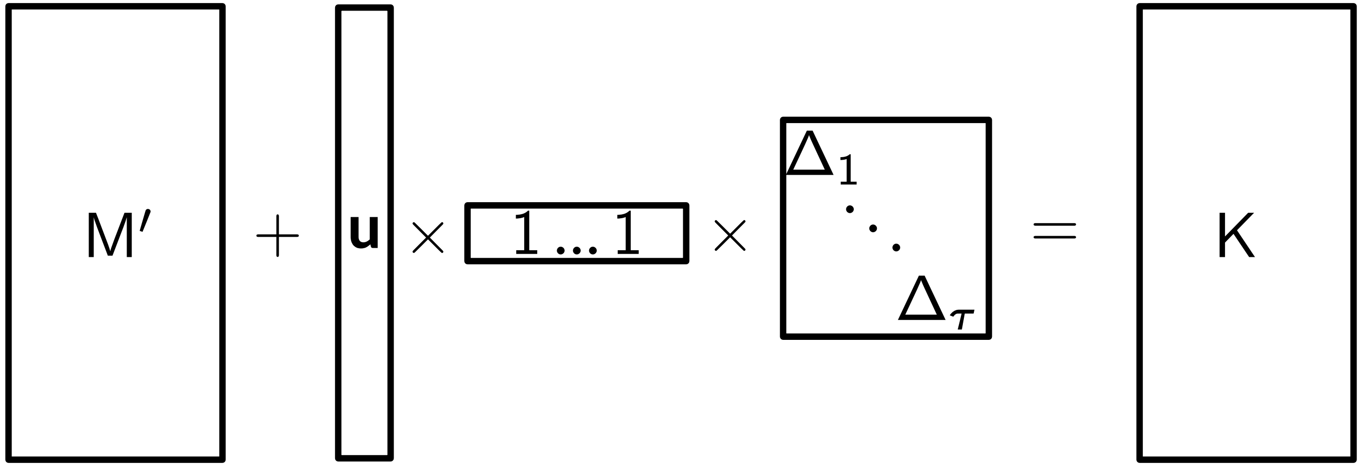


VOLEitH Step 3: Merge Small Field VOLE into Large Field VOLE

- $\mathcal{P}$ sends syndrome $\mathbf{C}$ to $\mathcal{V}$
- $\mathcal{V}$ locally sets $\mathsf{K} = \mathsf{K}' - [0 \| \mathbf{C}] \cdot \mathrm{diag}(\boldsymbol{\Delta})$



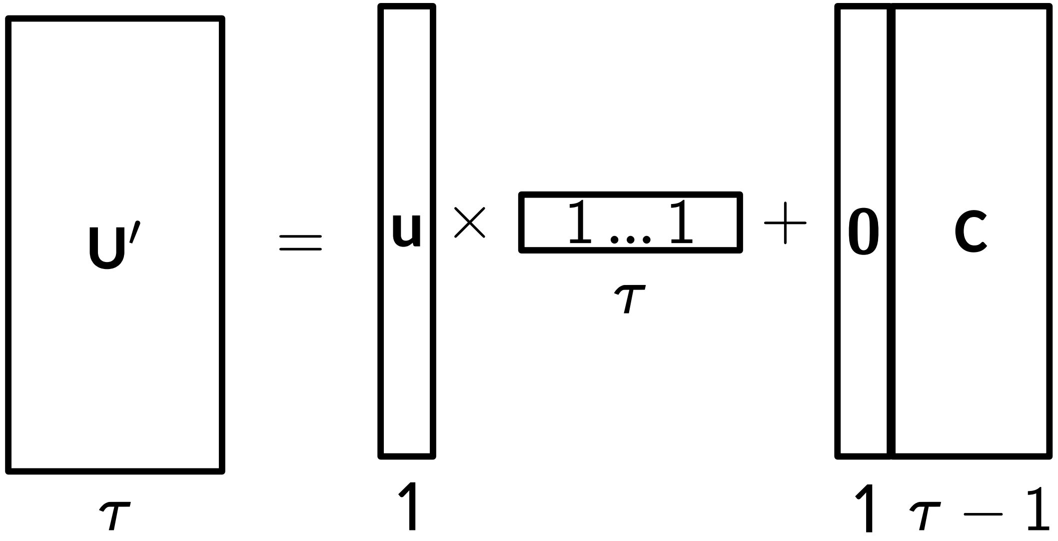
$$
\begin{aligned}
\mathsf{K} &= \mathsf{K}' - [0 \| \mathbf{C}] \cdot \mathrm{diag}(\boldsymbol{\Delta}) \\
&= \mathsf{M}' + (\mathbf{u} \cdot \mathbf{1} + [0 \| \mathbf{C}]) \cdot \mathrm{diag}(\boldsymbol{\Delta}) - [0 \| \mathbf{C}] \cdot \mathrm{diag}(\boldsymbol{\Delta}) \\
&= \mathsf{M}' + \mathbf{u} \cdot \mathbf{1} \cdot \mathrm{diag}(\boldsymbol{\Delta})
\end{aligned}
$$



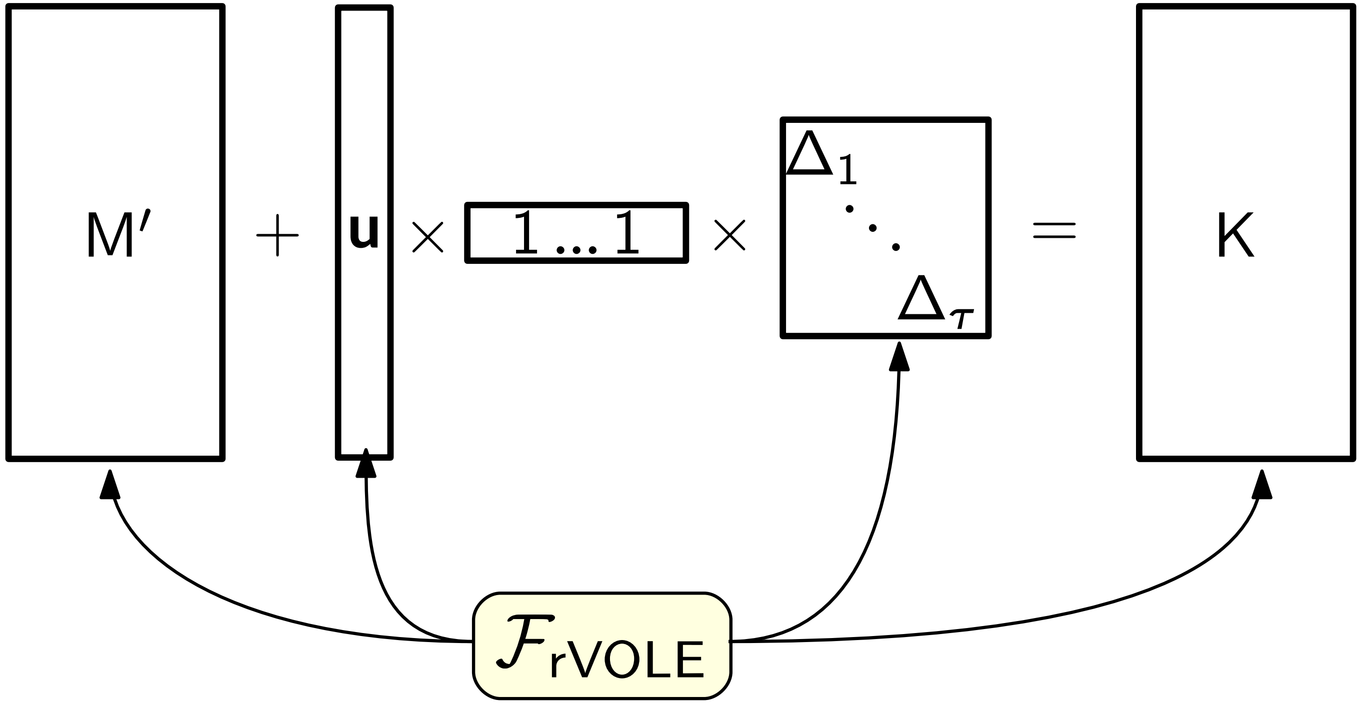
$\mathcal{F}_{\mathsf{rVOLE}}$

VOLEitH Step 3: Merge Small Field VOLE into Large Field VOLE

- $\mathcal{P}$ sends syndrome $\mathbf{C}$ to $\mathcal{V}$
- $\mathcal{V}$ locally sets $\mathsf{K} = \mathsf{K}' - [0 \| \mathbf{C}] \cdot \mathrm{diag}(\boldsymbol{\Delta})$



$$
\begin{aligned}
\mathsf{K} &= \mathsf{K}' - [0 \| \mathbf{C}] \cdot \mathrm{diag}(\boldsymbol{\Delta}) \\
&= \mathsf{M}' + (\mathbf{u} \cdot \mathbf{1} + [0 \| \mathbf{C}]) \cdot \mathrm{diag}(\boldsymbol{\Delta}) - [0 \| \mathbf{C}] \cdot \mathrm{diag}(\boldsymbol{\Delta}) \\
&= \mathsf{M}' + \mathbf{u} \cdot \mathbf{1} \cdot \mathrm{diag}(\boldsymbol{\Delta})
\end{aligned}
$$



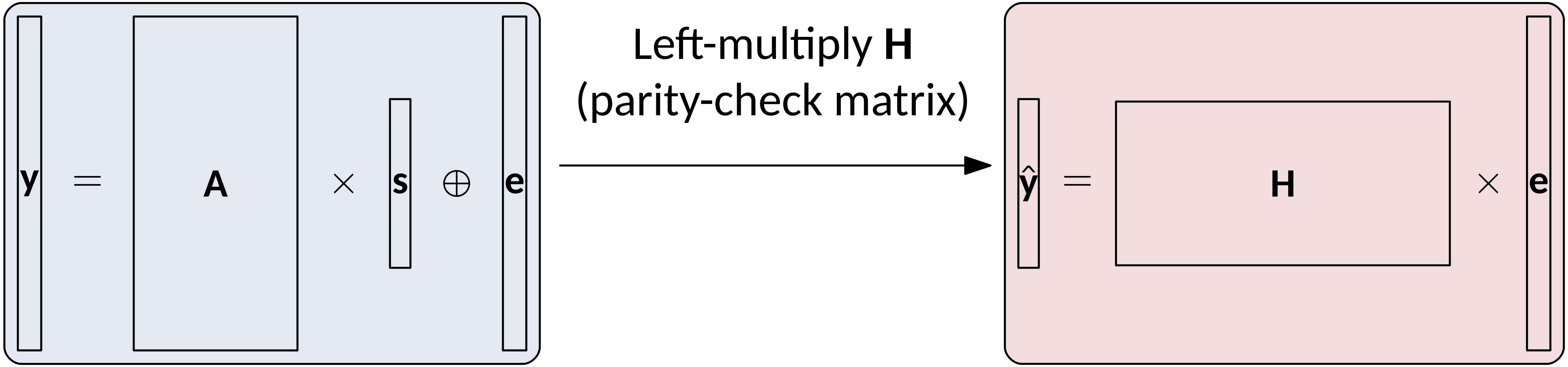
- SSOT: Check correlation on a random linear combination for consistency
- $\mathcal{A}$ can gain 1-bit information about Δ via selective failure attack

Synopsis

- Motivation
- Vector-OLE in the Head
- **Proving RSD in VOLE-hybrid Model**
- Results

Proving LPN/SD

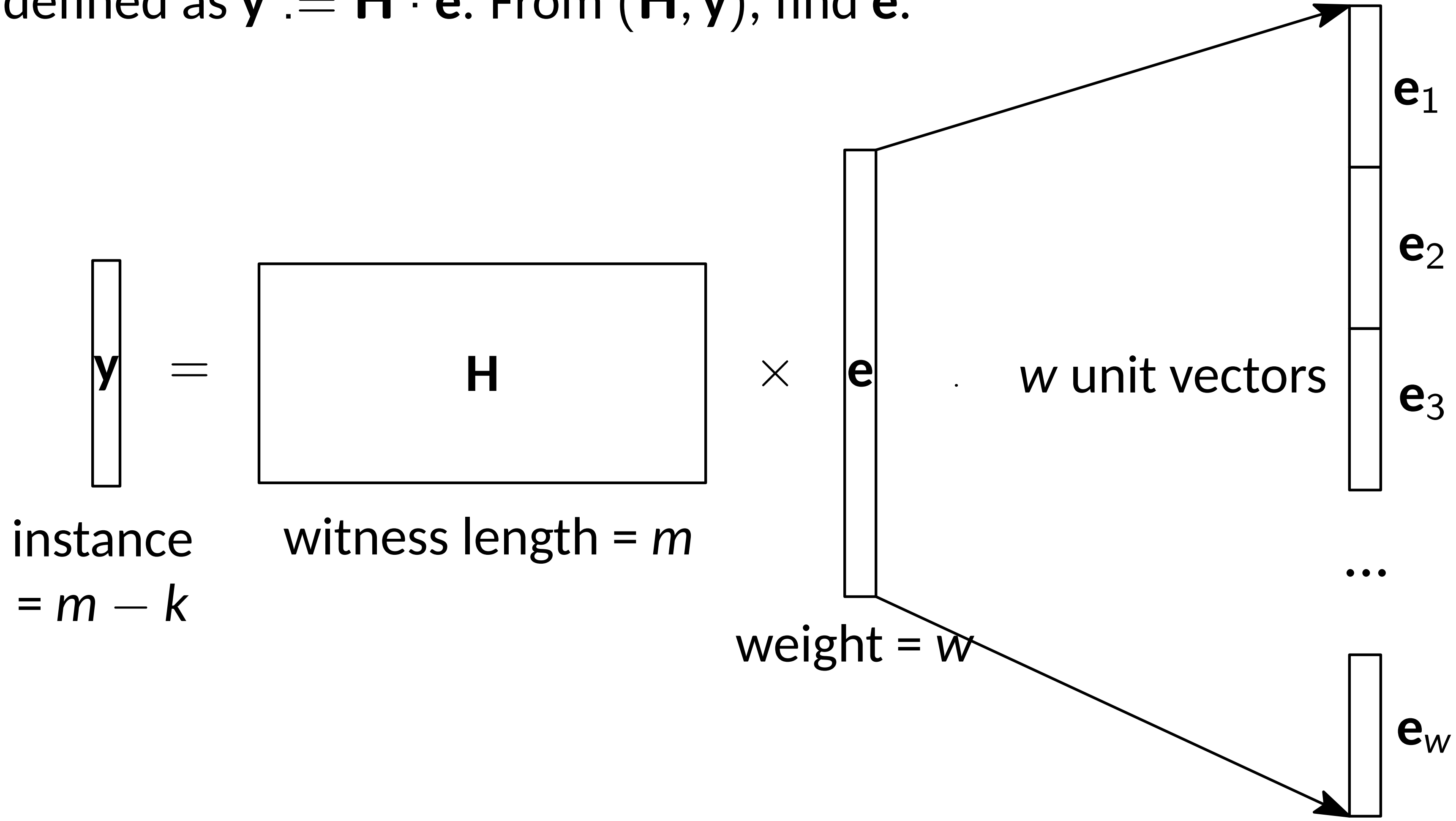
- First step: Consider the **dual** form of LPN
- Proving knowledge of **s**, **e** with respect to **A**, **y** is equivalent to proving knowledge of **e** alone



Regular Syndrome Decoding (Learning Parity with Regular Noise)

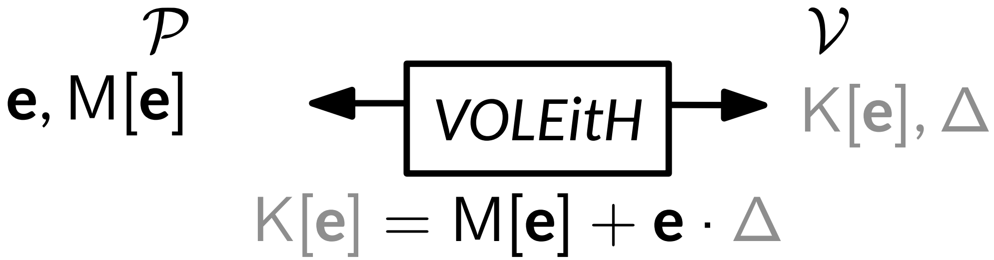
Let m, k, w, d be positive integers such that $m > k$, $m > w$ and $d = w$. The regular noise syndrome decoding problem with parameters (m, k, w, d) is the following problem: Let $\mathbf{H}$, $\mathbf{e}$ and $\mathbf{y}$ be such that:

1. $\mathbf{H}$ is uniformly sampled from $\mathbb{F}_2^{(m-k)\times m}$,
2. $\mathbf{e}$ is uniformly sampled from $\{[\mathbf{e}_1 \| ... \| \mathbf{e}_w] : \forall i \in [1, w], \mathbf{e}_i \in \mathbb{F}_2^{\frac{m}{w}}, \|\mathbf{e}_i\|_0 = 1\}$,
3. $\mathbf{y}$ is defined as $\mathbf{y} := \mathbf{H} \cdot \mathbf{e}$. From $(\mathbf{H}, \mathbf{y})$, find $\mathbf{e}$.



Proving Regularity in DVZK

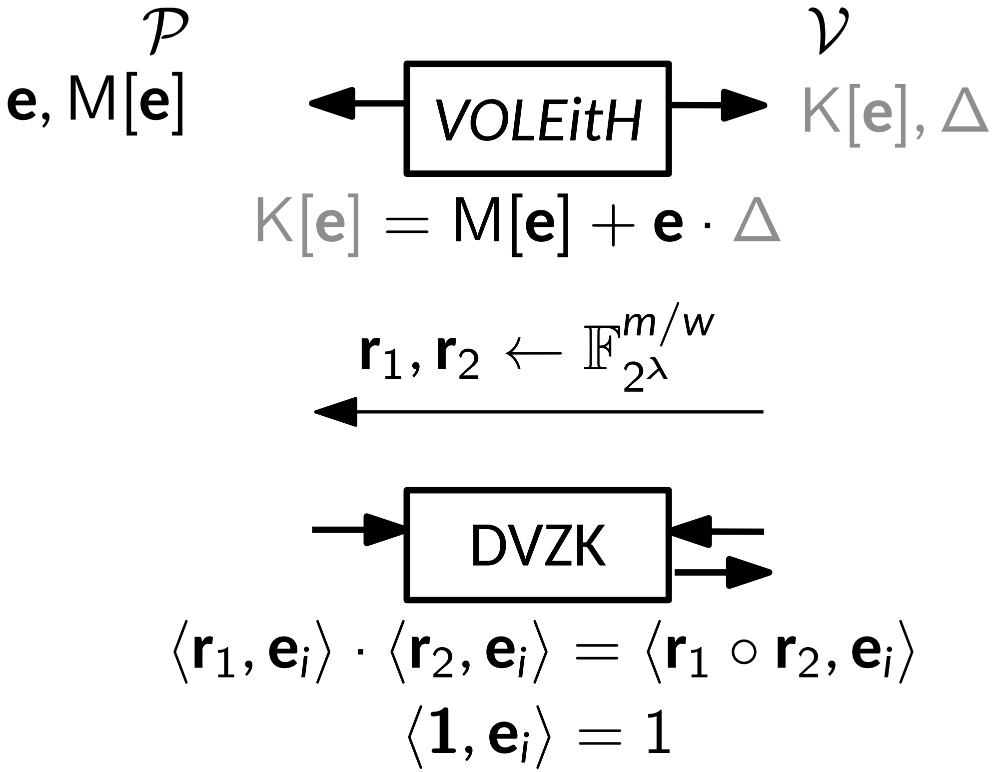
- Using VOLEitH we can get $[\![\mathbf{e}]\!]$
- $\mathbf{e} = \mathbf{e}_1 \| \ldots \| \mathbf{e}_w$
- Prove that $\mathbf{e}_i$ is a unit vector



$$\mathsf{K}[\mathbf{e}] = \mathsf{M}[\mathbf{e}] + \mathbf{e} \cdot \Delta$$

Proving Regularity in DVZK

- Using VOLEitH we can get $[\![\mathbf{e}]\!]$
- $\mathbf{e} = \mathbf{e}_1 \| ... \| \mathbf{e}_w$
- Prove that $\mathbf{e}_i$ is a unit vector
- Solution: linear sketch functions [BGI16]



$$\mathsf{K}[\mathbf{e}] = \mathsf{M}[\mathbf{e}] + \mathbf{e} \cdot \Delta$$

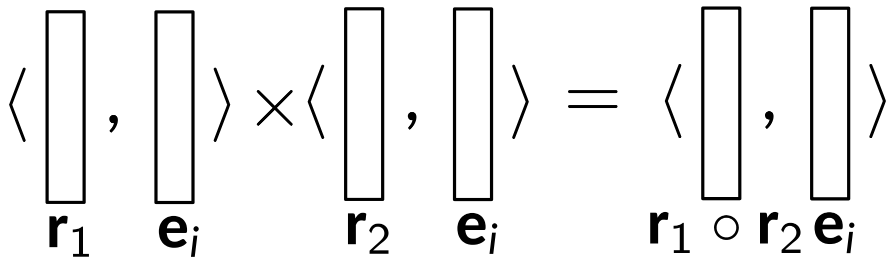
$$\mathbf{r}_1, \mathbf{r}_2 \leftarrow \mathbb{F}_{2^\lambda}^{m/w}$$

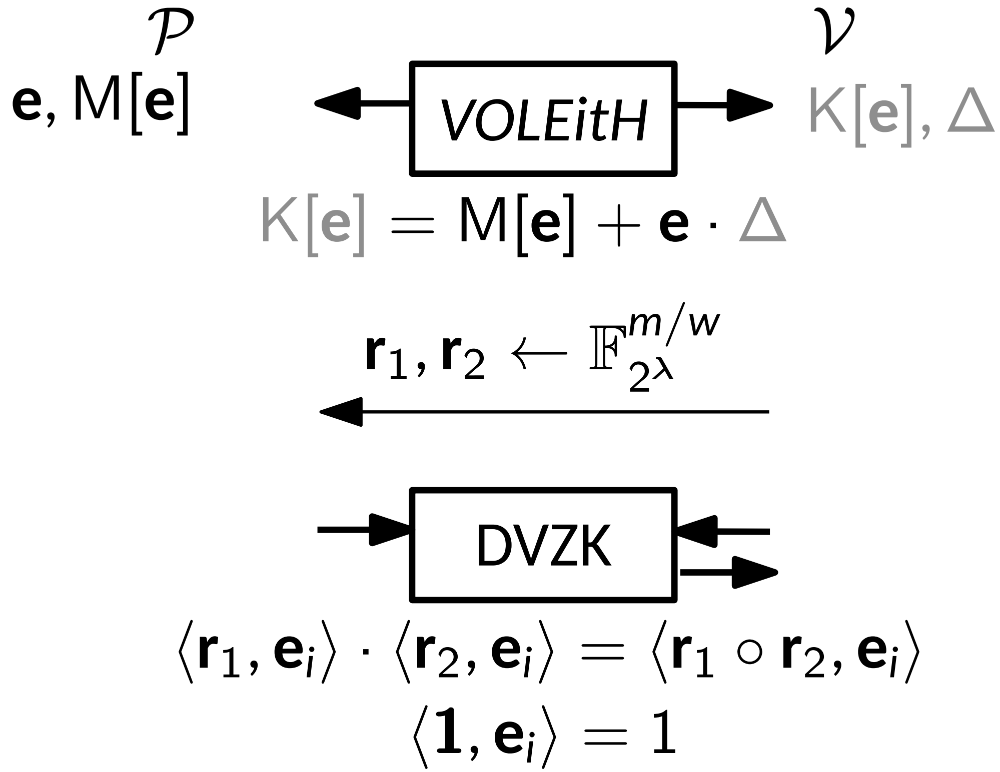
$$\langle \mathbf{r}_1, \mathbf{e}_i \rangle \cdot \langle \mathbf{r}_2, \mathbf{e}_i \rangle = \langle \mathbf{r}_1 \circ \mathbf{r}_2, \mathbf{e}_i \rangle$$

$$\langle \mathbf{1}, \mathbf{e}_i \rangle = 1$$

Proving Regularity in DVZK

- Using VOLEitH we can get $[\![\mathbf{e}]\!]$
- $\mathbf{e} = \mathbf{e}_1 \| \ldots \| \mathbf{e}_w$
- Prove that $\mathbf{e}_i$ is a unit vector
- Solution: linear sketch functions [BGI16]
- **Completeness.** If $\mathbf{e}_i = \mathrm{unit}(j)$





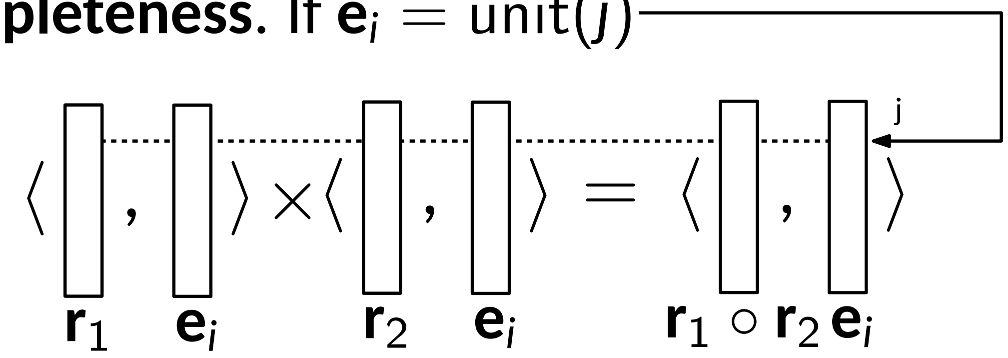
$$\mathsf{K}[\mathbf{e}] = \mathsf{M}[\mathbf{e}] + \mathbf{e} \cdot \Delta$$

$$\langle \mathbf{r}_1, \mathbf{e}_i \rangle \cdot \langle \mathbf{r}_2, \mathbf{e}_i \rangle = \langle \mathbf{r}_1 \circ \mathbf{r}_2, \mathbf{e}_i \rangle$$

$$\langle \mathbf{1}, \mathbf{e}_i \rangle = 1$$

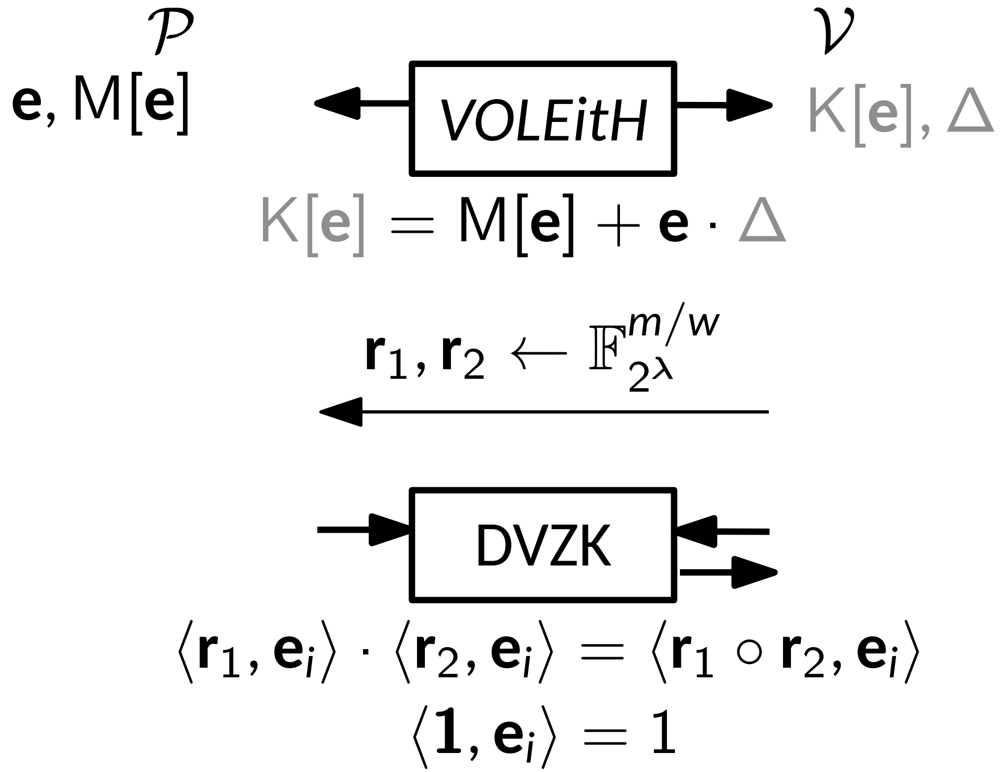
Proving Regularity in DVZK

- Using VOLEitH we can get $[\![\mathbf{e}]\!]$
- $\mathbf{e} = \mathbf{e}_1 \| \ldots \| \mathbf{e}_w$
- Prove that $\mathbf{e}_i$ is a unit vector
- Solution: linear sketch functions [BGI16]
- **Completeness.** If $\mathbf{e}_i = \mathrm{unit}(j)$



$$\mathbf{r}_{1,j} \times \mathbf{r}_{2,j} = \mathbf{r}_{1,j} \cdot \mathbf{r}_{2,j}$$

$$\langle \mathbf{1}, \mathbf{e}_i \rangle = \mathbf{e}_{i,1} + \ldots + \mathbf{e}_{i,m/w} = \mathbf{e}_{i,j} = 1$$



$$\mathsf{K}[\mathbf{e}] = \mathsf{M}[\mathbf{e}] + \mathbf{e} \cdot \Delta$$

$$\mathbf{r}_1, \mathbf{r}_2 \leftarrow \mathbb{F}_{2^\lambda}^{m/w}$$

$$\langle \mathbf{r}_1, \mathbf{e}_i \rangle \cdot \langle \mathbf{r}_2, \mathbf{e}_i \rangle = \langle \mathbf{r}_1 \circ \mathbf{r}_2, \mathbf{e}_i \rangle$$

$$\langle \mathbf{1}, \mathbf{e}_i \rangle = 1$$

Proving Regularity in DVZK

- **Soundness.** For every $j, k \in [m/w]$ s.t. $j \neq k \wedge \mathbf{e}_{i,j} = 1 \wedge \mathbf{e}_{i,k} = 1$

$$\left\langle \underset{\mathbf{r}_1}{\boxed{}}, \underset{\mathbf{e}_i}{\boxed{}} \right\rangle \times \left\langle \underset{\mathbf{r}_2}{\boxed{}}, \underset{\mathbf{e}_i}{\boxed{}} \right\rangle - \left\langle \underset{\mathbf{r}_1 \circ \mathbf{r}_2}{\boxed{}}, \underset{\mathbf{e}_i}{\boxed{}} \right\rangle = \sum_{j,k} \mathbf{r}_{1,j} \cdot \mathbf{r}_{2,k} + \mathbf{r}_{1,k} \cdot \mathbf{r}_{2,j}$$

Proving Regularity in DVZK

- **Soundness**. For every $j, k \in [m/w]$ s.t. $j \neq k \wedge \mathbf{e}_{i,j} = 1 \wedge \mathbf{e}_{i,k} = 1$

$$\langle \underset{\mathbf{r}_1}{\boxed{}}, \underset{\mathbf{e}_i}{\boxed{}} \rangle \times \langle \underset{\mathbf{r}_2}{\boxed{}}, \underset{\mathbf{e}_i}{\boxed{}} \rangle - \langle \underset{\mathbf{r}_1 \circ \mathbf{r}_2}{\boxed{}}, \underset{\mathbf{e}_i}{\boxed{}} \rangle = \sum_{j,k} \mathbf{r}_{1,j} \cdot \mathbf{r}_{2,k} + \mathbf{r}_{1,k} \cdot \mathbf{r}_{2,j}$$

Quadratic equation in $\mathbb{F}_{2^\lambda}[X_1, ..., X_{2m/w}]$

- If $\mathrm{wt}(\mathbf{e}_i) > 1$, there will be cross terms
- SZ-Lemma: except with probability $\frac{2}{2^\lambda}$, we have $\mathrm{wt}(\mathbf{e}_i) \leq 1$

Proving Regularity in DVZK

- **Soundness**. For every $j, k \in [m/w]$ s.t. $j \neq k \wedge \mathbf{e}_{i,j} = 1 \wedge \mathbf{e}_{i,k} = 1$

$$\left\langle \underset{\mathbf{r}_1}{\boxed{}}, \underset{\mathbf{e}_i}{\boxed{}} \right\rangle \times \left\langle \underset{\mathbf{r}_2}{\boxed{}}, \underset{\mathbf{e}_i}{\boxed{}} \right\rangle - \left\langle \underset{\mathbf{r}_1 \circ \mathbf{r}_2}{\boxed{}}, \underset{\mathbf{e}_i}{\boxed{}} \right\rangle = \sum_{j,k} \mathbf{r}_{1,j} \cdot \mathbf{r}_{2,k} + \mathbf{r}_{1,k} \cdot \mathbf{r}_{2,j}$$

Quadratic equation in $\mathbb{F}_{2^\lambda}[X_1, ..., X_{2m/w}]$

- If $\mathrm{wt}(\mathbf{e}_i) > 1$, there will be cross terms
- SZ-Lemma: except with probability $\frac{2}{2^\lambda}$, we have $\mathrm{wt}(\mathbf{e}_i) \leq 1$

$$\left\langle \underset{\mathbf{1}}{\boxed{}}, \underset{\mathbf{e}_i}{\boxed{}} \right\rangle = 1$$

- Use IT-MAC opening to check that $\langle \mathbf{1}, \mathbf{e}_i \rangle = 1$

Synopsis

- Motivation
- Vector-OLE in the Head
- Proving RSD in VOLE-hybrid Model
- **Results**

ReSolveD Signature

Systematic Form

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

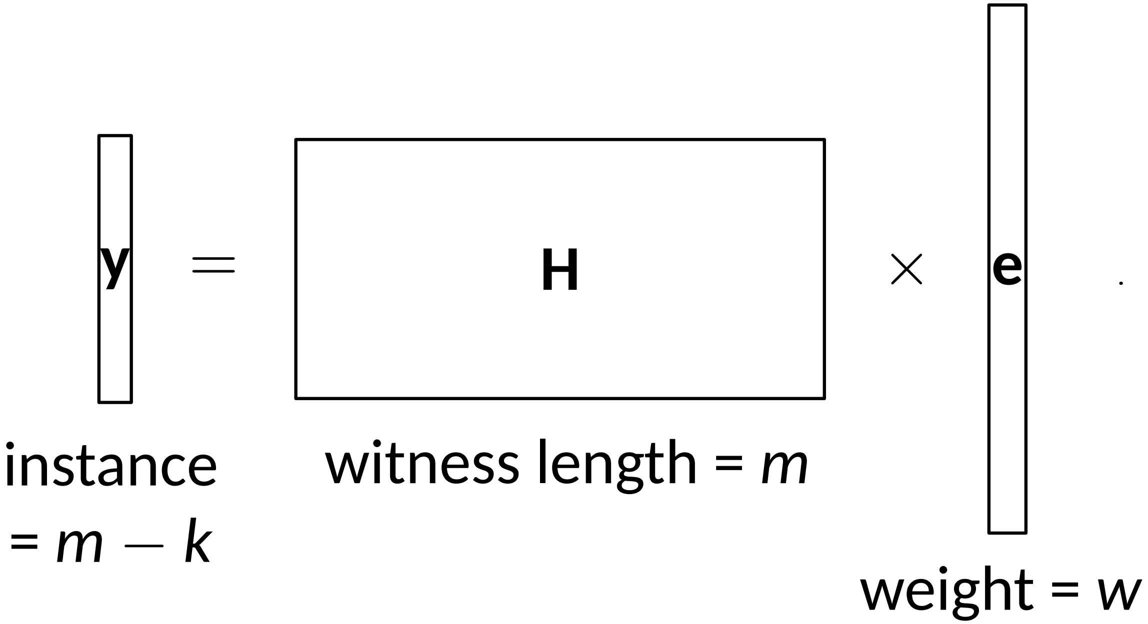
Half-Tree

- Replace $(r_{2i} \| r_{2i+1}) \leftarrow G(r_i)$ with $r_{2i} \leftarrow H(r_i)$, $r_{2i+1} \leftarrow H(r_i) \oplus r_1$
- Saves half of the AES calls
- Provable security in RPM

Parameters

- m: witness length, τ: repetition count
- Security estimation according to the formulas in [CCJ23]

Parameter Set	m	k	w	τ	Estimated Bit Security
ReSolveD-128-Var1	1302	738	217	14	128.20
ReSolveD-128-Var2	1302	738	217	10	128.20
ReSolveD-L1	1470	834	245	11	143.20
ReSolveD-L3	2196	1248	366	17	207.48
ReSolveD-L5	2934	1668	489	22	272.29



$$\mathbf{y} = \mathbf{H} \times \mathbf{e} .$$

instance
= $m - k$

witness length = m

weight = w

Performance

Compared with NIST Alternative PQ Signature

Scheme	Sizes in Bytes				Runtimes in ms			Assumption
	$\|\text{sig}\|$	$\|\text{sk}\|$	$\|\text{pk}\|$	$\|\text{sig}\| + \|\text{pk}\|$	t_{keygen}	t_{sign}	t_{verify}	
ReSolveD-L1	3916	32	96	**4012**	4.36	97.51	80.21	RSD over $\mathbb{F}_2$
ReSolveD-L3	8532	48	143	**8675**	9.97	257.37	226.71	RSD over $\mathbb{F}_2$
ReSolveD-L5	14944	64	191	**15135**	17.66	537.54	469.72	RSD over $\mathbb{F}_2$
FAEST-L1-S	5006	32	32	5038	0.19	129.14	124.89	AES
FAEST-L3-S	12744	56	64	12808	1.01	401.76	371.87	AES
FAEST-L5-S	22100	64	64	22164	1.47	624.62	586.12	AES
FAEST_EM-L1-S	4566	32	32	4598	0.18	112.06	108.85	EM-AES
FAEST_EM-L3-S	10824	48	48	10872	0.46	297.66	288.40	EM-AES
FAEST_EM-L5-S	20956	64	64	21020	1.41	540.35	540.04	EM-AES
SDitH-L1-gf256	8224	404	120	8344	6.08	33.23	28.62	SD over $\mathbb{F}_{256}$
SDitH-L1-gf251	8224	404	120	8344	4.41	14.76	12.32	SD over $\mathbb{F}_{251}$
SDitH-L3-gf256	19544	616	183	19727	7.31	113.98	98.82	SD over $\mathbb{F}_{256}$
SDitH-L3-gf251	19544	616	183	19727	5.30	34.46	28.32	SD over $\mathbb{F}_{251}$
SDitH-L5-gf256	33992	812	234	34226	10.59	209.67	186.77	SD over $\mathbb{F}_{256}$
SDitH-L5-gf251	33992	812	234	34226	8.74	59.33	54.85	SD over $\mathbb{F}_{251}$

More Performace

- Compared with previous PQC submissions

Scheme	Sizes in KB			Runtimes in ms		Assumption
	$\|sig\|$	$\|pk\|$	$\|sig\| + \|pk\|$	t_{sign}	t_{verify}	
Dilithium2	2.36	1.28	**3.64**	0.128	0.046	MLWE
Falcon-512	0.65	0.88	1.53	0.168	0.036	NTRU
SPHINCS$^+$-SHAKE-L1-F	16.69	0.03	16.72	18.37	1.08	Hash
SPHINCS$^+$-SHAKE-L1-S	7.67	0.03	7.70	355.64	0.38	Hash
SPHINCS$^+$-SHA2-L1-F	16.69	0.03	16.72	10.86	0.69	Hash
SPHINCS$^+$-SHA2-L1-S	7.67	0.03	7.70	207.98	0.28	Hash
SPHINCS-α-SHAKE-L1-F	16.33	0.03	16.36	15.85	0.99	Hash
SPHINCS-α-SHAKE-L1-S	6.72	0.03	6.75	316.60	1.36	Hash
SPHINCS-α-SHA2-L1-F	16.33	0.03	16.36	7.40	0.56	Hash
SPHINCS-α-SHA2-L1-S	6.72	0.03	6.75	149.18	0.75	Hash
Picnic1-L1-FS	32.09	0.03	32.12	1.37	1.10	LowMC
Picnic2-L1-FS	12.05	0.03	12.08	40.95	18.20	LowMC
Picnic3-L1	12.30	0.03	12.33	5.17	3.96	LowMC
Picnic3-L1-K12	12.30	0.03	12.33	3.98	2.87	LowMC
Picnic3-L1-64	11.14	0.03	11.17	23.25	17.21	LowMC
Picnic3-5-L1	13.38	0.03	13.41	5.59	4.63	LowMC
ReSolveD-L1	3.82	0.09	**3.91**	95.51	80.21	RSD

Thanks for your listening