VOLE-in-the-Head and the FAEST Post-Quantum Signature Scheme

Peter Scholl

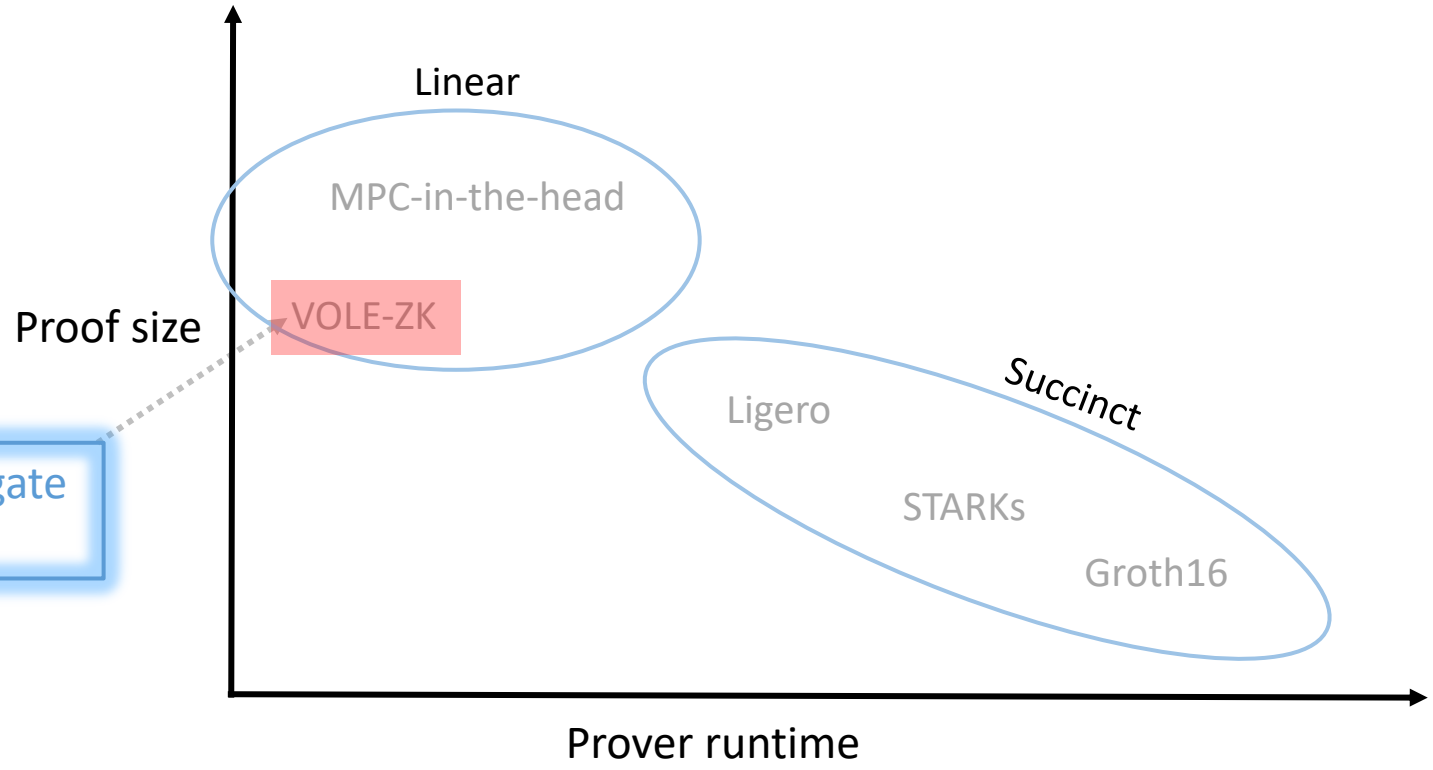
ZKProof 5.5, 2 August 2023

Based on

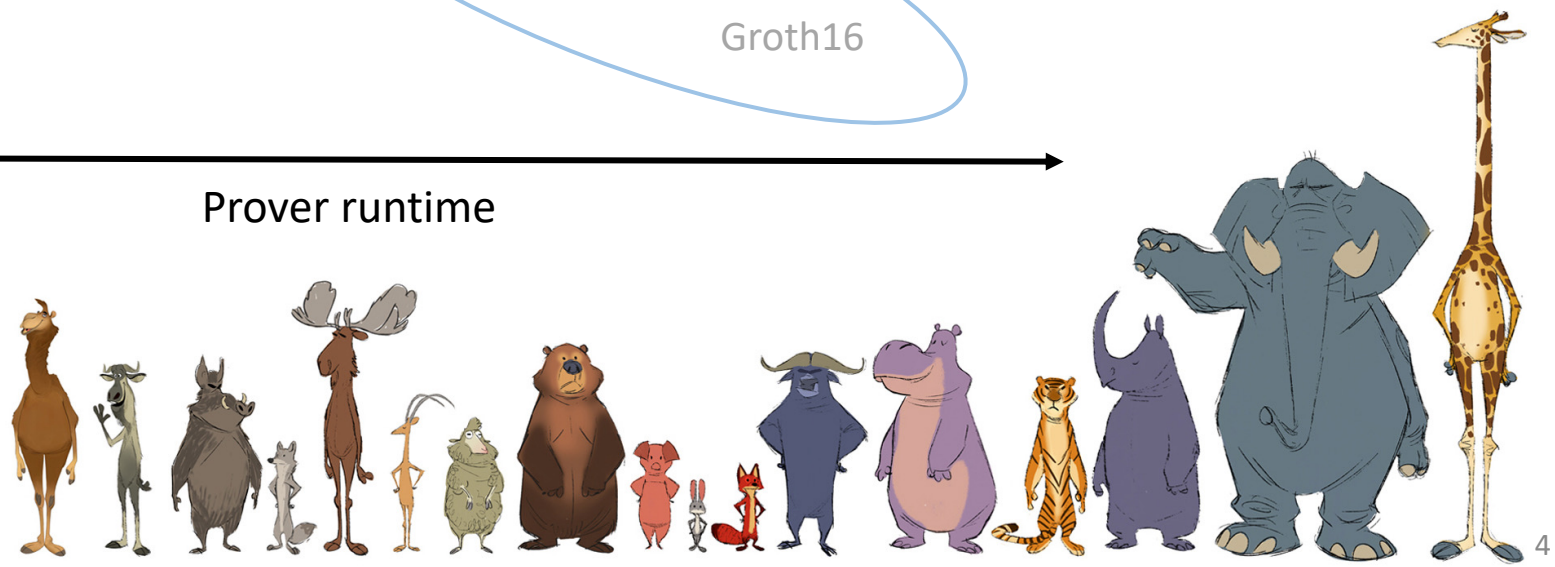
Publicly Verifiable Zero-Knowledge and Post-Quantum Signatures From VOLE-in-the-Head
with *Carsten Baum, Lennart Braun, Cyprien Delpech de Saint Guilhem, Michael Klooß, Emmanuela Orsini, Lawrence Roy*
CRYPTO 2023

FAEST Digital Signature Scheme
+ Christian Majenz, Shibam Mukherjee, Sebastian Ramacher, Christian Rechberger
Submission to NIST PQC Standardization process

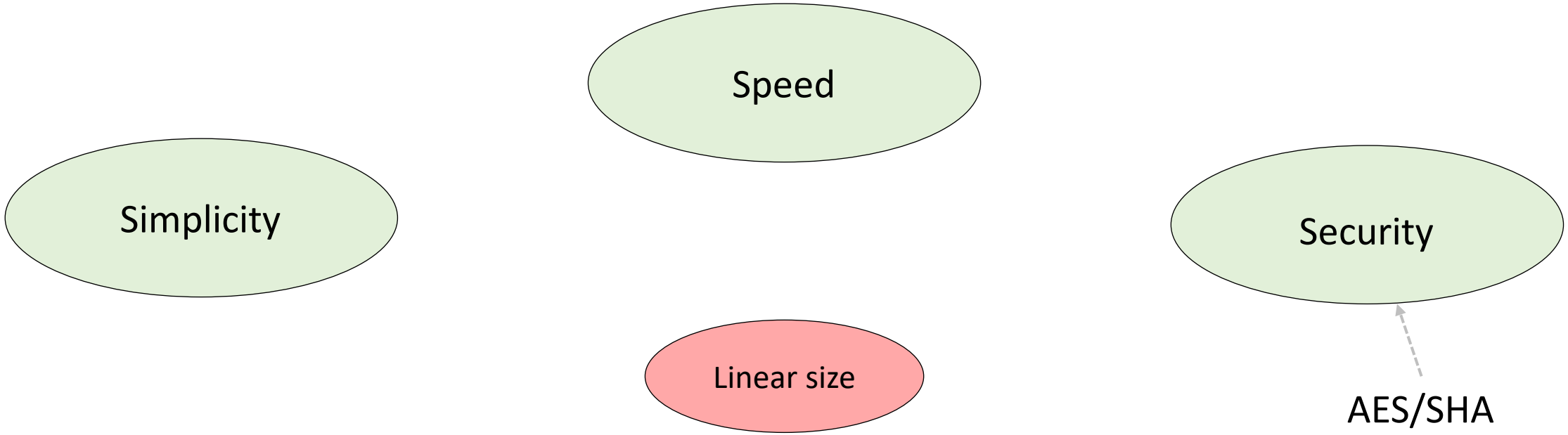
Families of ZK Proofs



Size: ≈ 1× bit per AND gate
designated verifier



VOLE-in-the-Head: a general tool for making VOLE-ZK proofs publicly verifiable



Application: FAEST post-quantum signature scheme

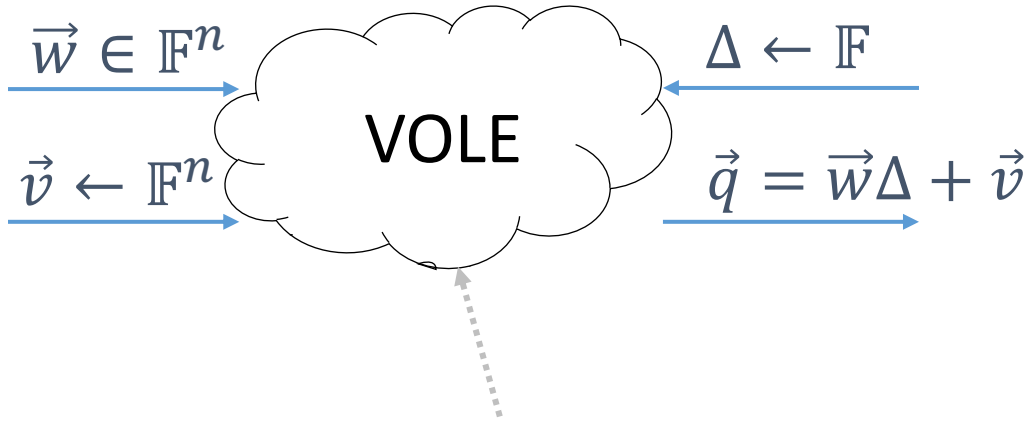
VOLE-ZK

in the designated verifier setting

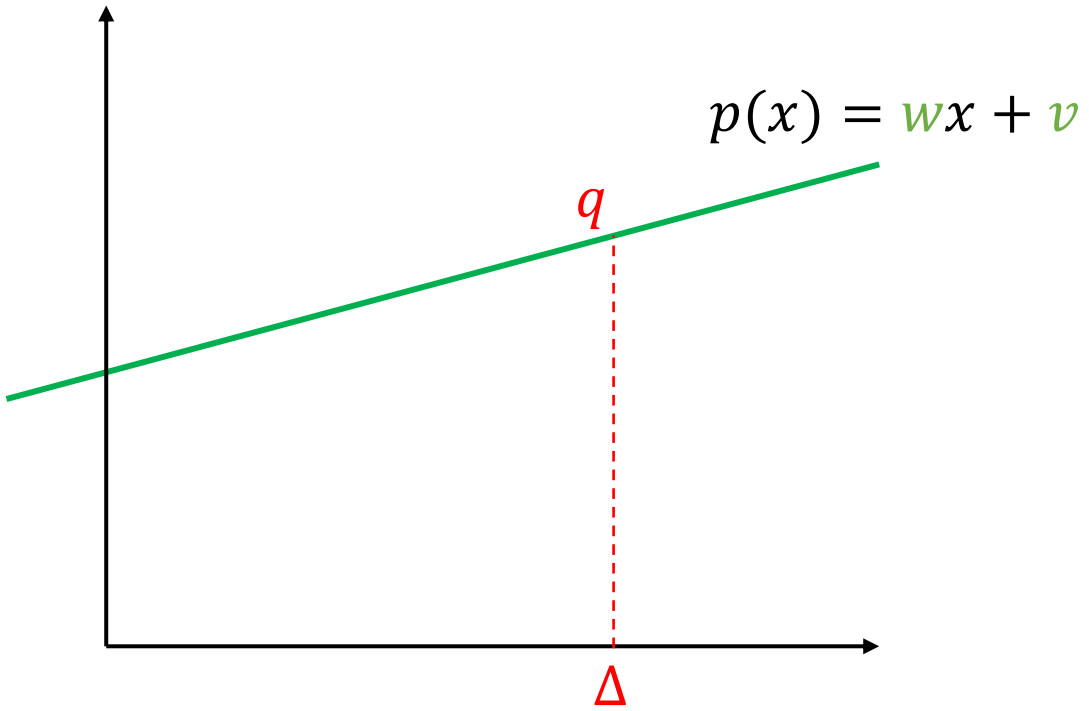
Background: VOLE (vector oblivious linear evaluation)

Prover

Verifier



Can be instantiated with OT, HE, LPN…



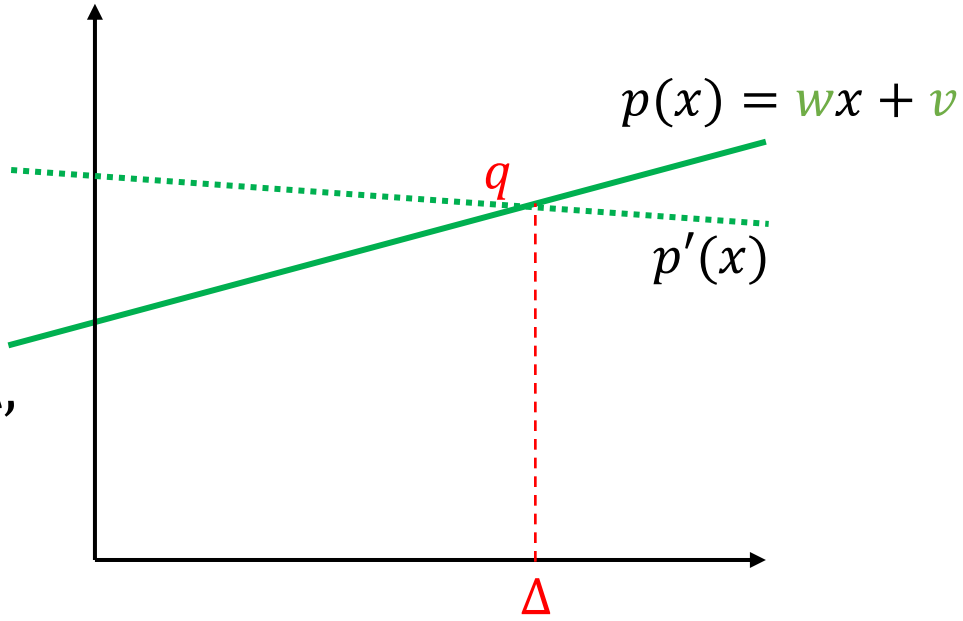
ZK from VOLE (designated verifier)

[BMRS 21, WYKW 21]

Use VOLE as a linear commitment to $\vec{w}$

To open

- Alice sends (w, v), Bob checks if $q = w\Delta + v$
- Hiding: since v is random
- Binding: opening to $w' \neq w$ requires guessing Δ, prob. $1/|\mathbb{F}|$

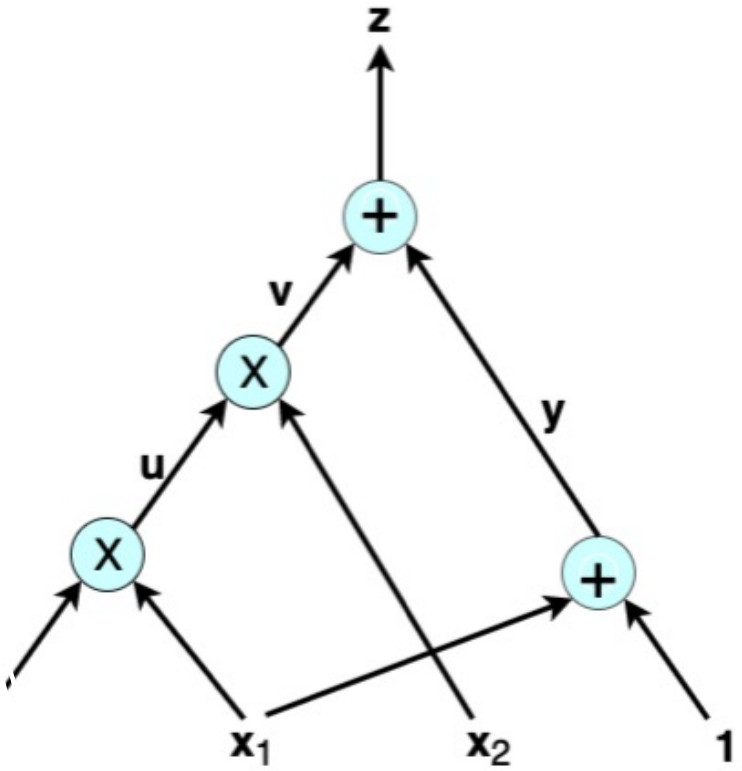


Commitments are linearly homomorphic

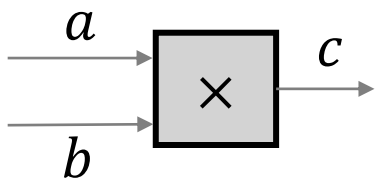
ZK from VOLE via Commit-and-Prove

[BMRS 21, WYKW 21]

- Commit to witness $\vec{w}$
- Evaluate C gate-by-gate:
  - Linear gates: easy
  - Multiplication: ???

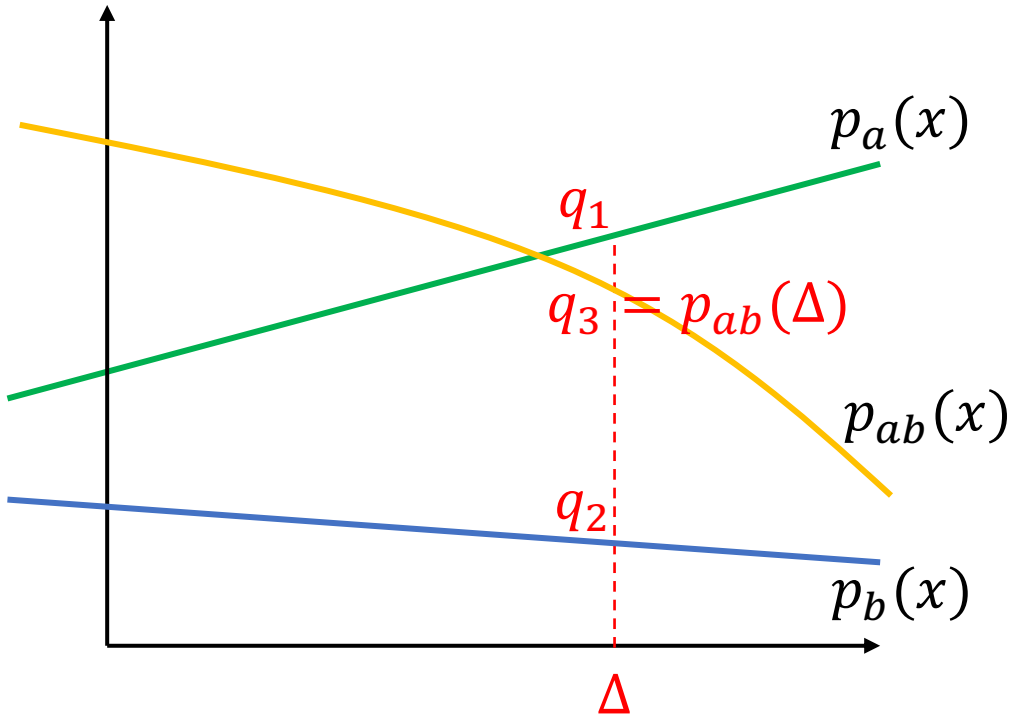


Multiplication gates in VOLE-ZK



[DIO 21, YSWW 21]

- Multiply two lines ⇒ quadratic polynomial
  - $p_{ab}(x) = d_0 + d_1 x + abx^2$
- Commit to output $c \Rightarrow p_c(x) = v + cx$
- $p_{ab}(x) - xp_c(x)$ should be degree-1
  - Open and check
  - First, mask with random deg-1 commitment



Cost analysis for VOLE-ZK

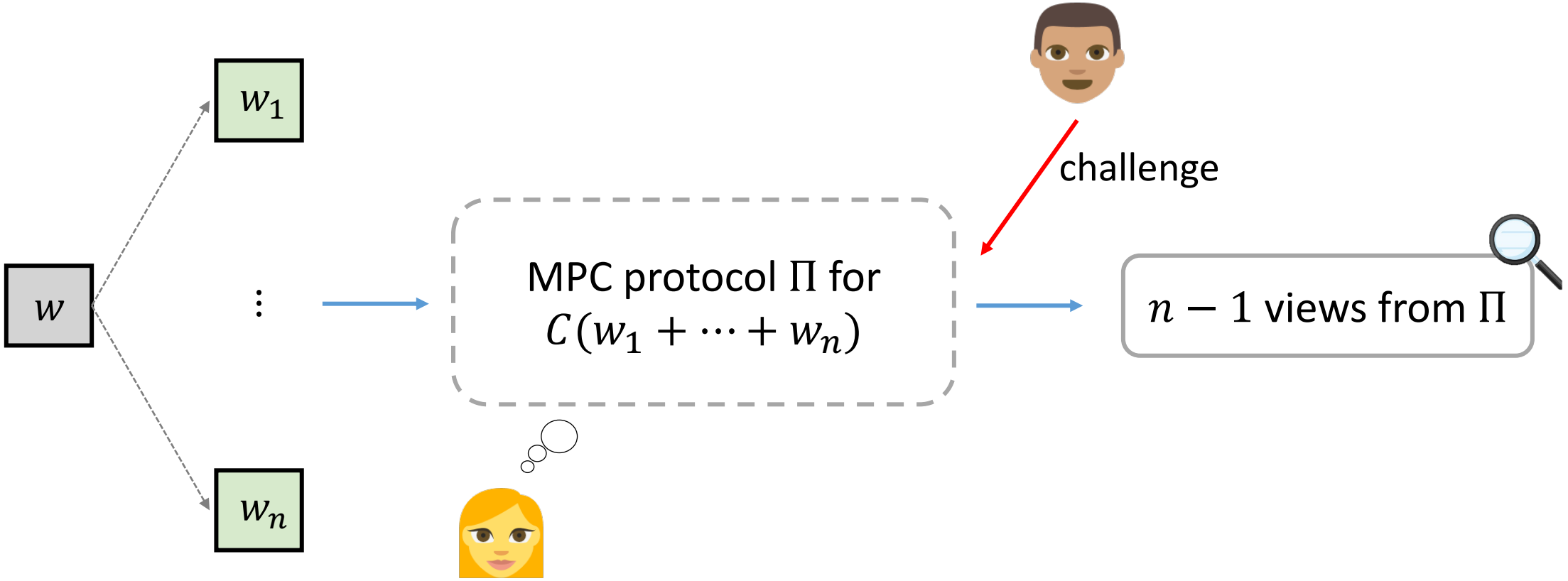
- Per multiplication gate:
  - Commit to c
    - $1\times$ VOLE element
  - Open masked commitment
    - Can be amortized (check random combination of gates)

- For circuit:
  - n field elements for circuit with n mult. gates (assuming cheap VOLE)
  - Improvements:
    - General deg-2 and higher degree gates; branching; field switching…

VOLE-in-the-Head

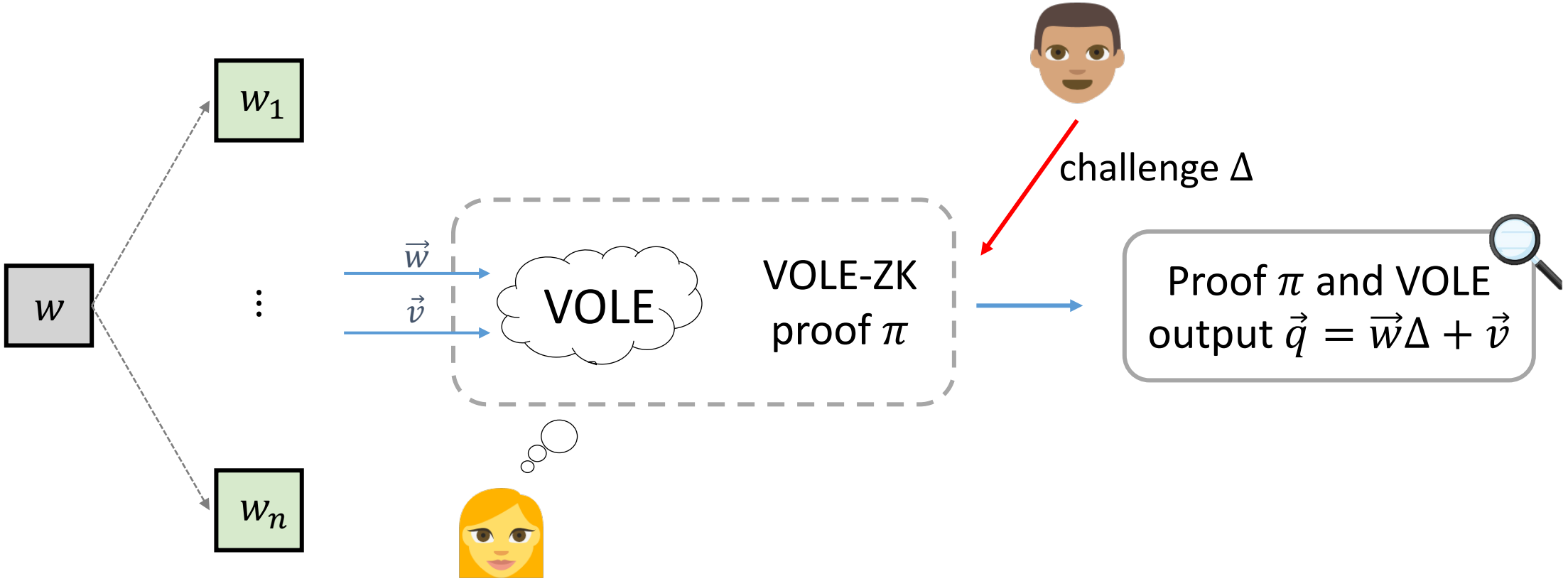
Adding public verifiability

MPC-in-the-Head vs VOLE-in-the-head: high-level differences



$w = w_1 + \cdots + w_n$

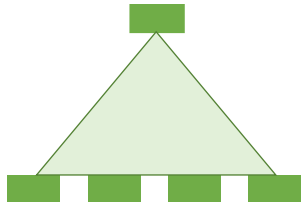
MPC-in-the-Head vs VOLE-in-the-head: high-level differences



$$w = w_1 + \cdots + w_n$$

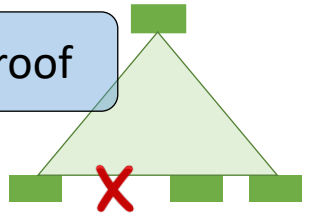
How to do VOLE-in-the-head?

All-but-one
vector commitment



Commit to n random strings

Run VOLE-ZK proof



Challenge Δ

Open $n-1$

Convert to VOLE

$\vec{u}, \vec{v}$

$\vec{q} = \vec{u}\Delta + \vec{v}$

VOLE-in-the-head: some details

- $(n-1)$-out-of-n vector commit ⇒ VOLE in $\mathbb{F}_n$
  - Commitments have soundness error $\frac{1}{n}$ ☹
  - What about $\mathbb{F}_m$ for large m?

- For extension fields, $m = n^\tau$:
  - Repeat τ times, with same $w \in \mathbb{F}_n$
  - Cost e.g. over $\mathbb{F}_2$, 10-16 bits per AND

- For large prime fields:
  - Encode w with linear code
  - Cost: 1-2 field elements per MULT

Needs consistency check

Application to Post-Quantum Signatures

Call for Additional Digital Signature Schemes

Paradigm for ZK-based signatures

- Signature:
  - NIZK proof of knowledge of sk, such that $pk = \mathrm{Enc}_{sk}(x)$

- Challenge: finding a ZK-friendly Enc
  - Custom ciphers: e.g. LowMC, MiMC
  - Other assumptions: code-based, multivariate…

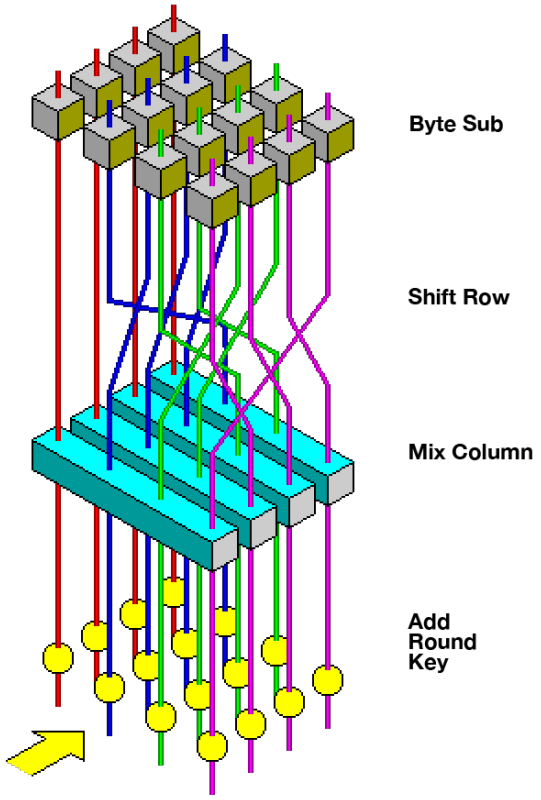
AES: a ZK-friendly OWF?

ShiftRows, MixColumns, AddRoundKey:

- All linear over $\mathbb{F}_2$

S-Box:

- Inversion in $\mathbb{F}_{2^8}$
- Prove in ZK as 1 multiplication constraint



Proving AES-128 in FAEST

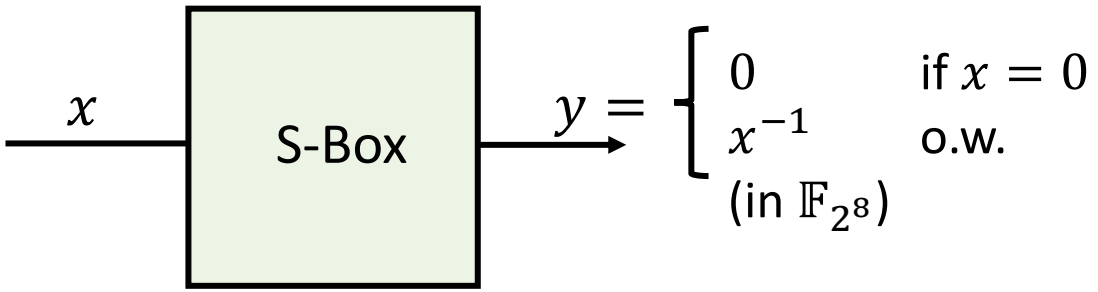
Witness: key + internal state of each round

- 1600 bits (in $\mathbb{F}_2$)

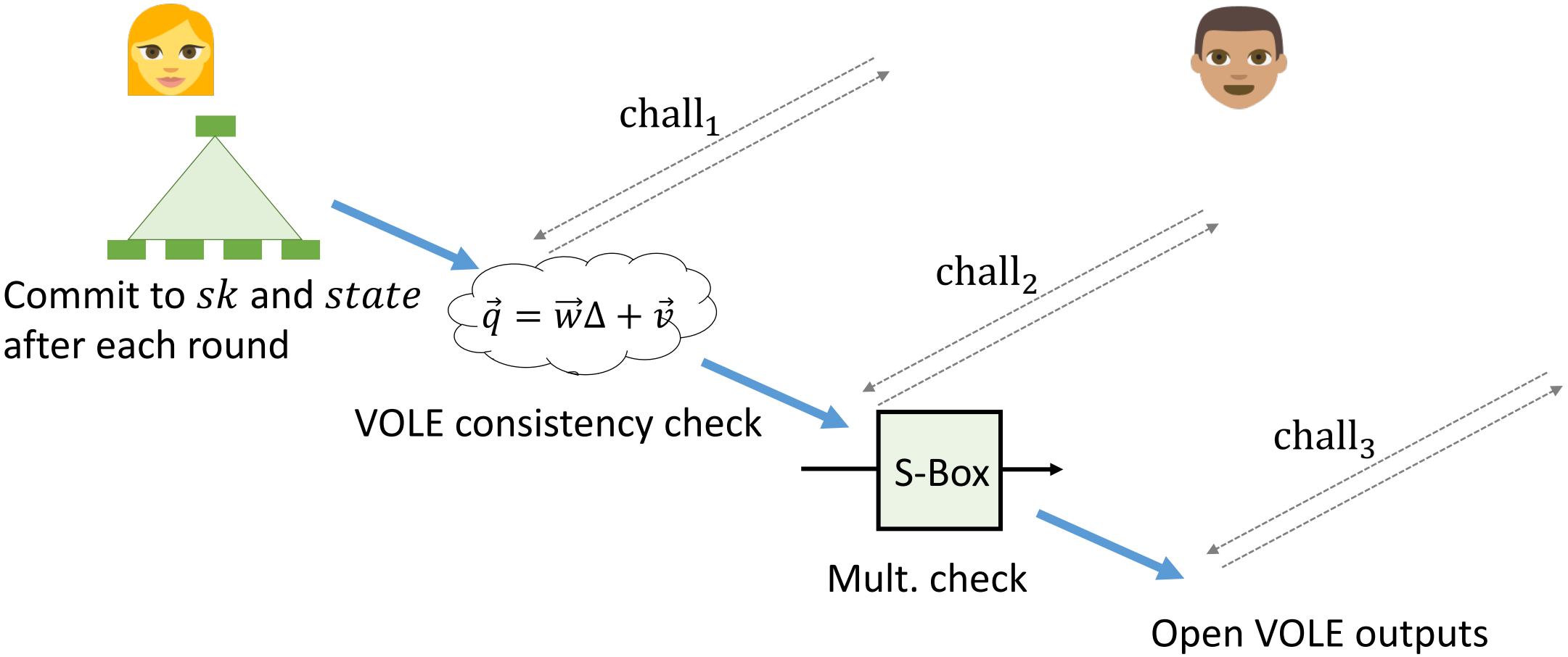
200 constraints over $\mathbb{F}_{2^8}$:

- 1 per S-box: degree-2 polynomial

  $xy = 1$



FAEST overview: proving $pk = \mathrm{AES}_{sk}(x)$



FAEST: example performance

	Sign/Verify	Size
FAEST-128s	≈ 8ms	5 006 B
FAEST-128f	≈ 1ms	6 336 B
FAEST-256s	≈ 27ms	22 100 B
FAEST-256f	≈ 3ms	28 400 B

- Signature sizes:
  - Smaller than SPHINCS+ and most code-based candidates
  - Faster signing, slower verification

- Possible variants:
  - MQ instead of AES: size ≈ 3 kB

Conclusion

VOLE-ZK proofs:

- Lightweight and fast with linear size
- VOLE-in-the-head: publicly verifiable

FAEST signature:

- Conservative security
- Reasonable performance

Resources:

Paper: https://ia.cr/2023/996

PQ signature: https://faest.info