FAEST round 2 update

Carsten Baum (Technical University of Denmark)
Ward Beullens (IBM Research Europe)
Lennart Braun (Université Paris Cité, CNRS, IRIF)
Cyprien Delpech de Saint Guilhem (3MI Labs, KU Leuven)
Michael Klooß (ETH Zurich)
Christian Majenz (Technical University of Denmark)
Shibam Mukherjee (Graz University of Technology, Know Center)
Emmanuela Orsini (Bocconi University)
Sebastian Ramacher (Austrian Institute of Technology)
Christian Rechberger (Graz University of Technology)
Lawrence Roy (Aarhus University)
Peter Scholl (Aarhus University)

9/26/2025

Credit to Carsten, Lance, and Lennart for some of the slides

Talk outline

High level overview of FAEST

Round 2 changes:

1. Optimized vector commitments
2. Optimized AES proof strategy
3. Change keyspace for improved security proof

FAEST in one slide:

KeyGen: Sample a random AES/Rijndael key K,
Sample a random message x,
Encrypt $y = Enc_K(x)$, (ECB or Evan-Mansour)
Output s$k = K,\ pk = (x, y)$.

Sign: Generate a "VOLE-in-the-head" zero-knowledge proof of knowledge of K such that $Enc_K(x) = y$.

Verify: Check the zero-knowledge proof.

Security follows from the security of AES + security of ZK-proof.

Only standard symmetric-crypto security assumptions!

Round 2 sizes and performance

Scheme	Runtimes in ms, Mcyc.						Sizes in B		
	KeyGen		Sign		Verify		sk	pk	Signature
FAEST-EM-128s	0.002	0.005	2.766	9.403	2.176	7.398	32	32	3 906
FAEST-EM-128f	0.002	0.005	0.413	1.404	0.327	1.113	32	32	5 060
FAEST-EM-192s	0.003	0.009	11.553	39.282	10.659	36.239	48	48	9 340
FAEST-EM-192f	0.003	0.009	1.523	5.177	1.372	4.665	48	48	12 380
FAEST-EM-256s	0.004	0.013	18.372	62.465	17.570	59.738	64	64	17 984
FAEST-EM-256f	0.004	0.013	2.775	9.436	2.566	8.725	64	64	23 476

Reasonable performance and sizes (faster signing and smaller signatures than SLH-DSA), despite the very conservative security assumptions!

*Timings performed on a AMD Zen 3 Ryzen 9 5950X processor at 3.4 GHz

Talk outline

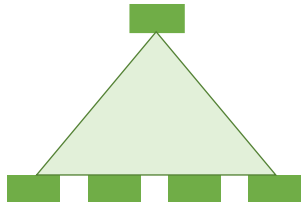
High level overview of FAEST

Round 2 changes:

1. Optimized vector commitments
2. Optimized AES proof strategy
3. Change keyspace for improved security proof

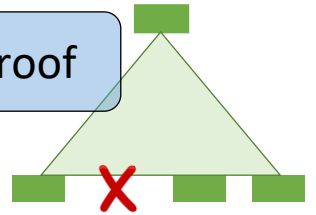
How to do VOLE-in-the-head?

All-but-one
vector commitment



Commit to n random strings

Run VOLE-ZK proof



Challenge Δ

Open $n-1$

Convert to VOLE

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

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

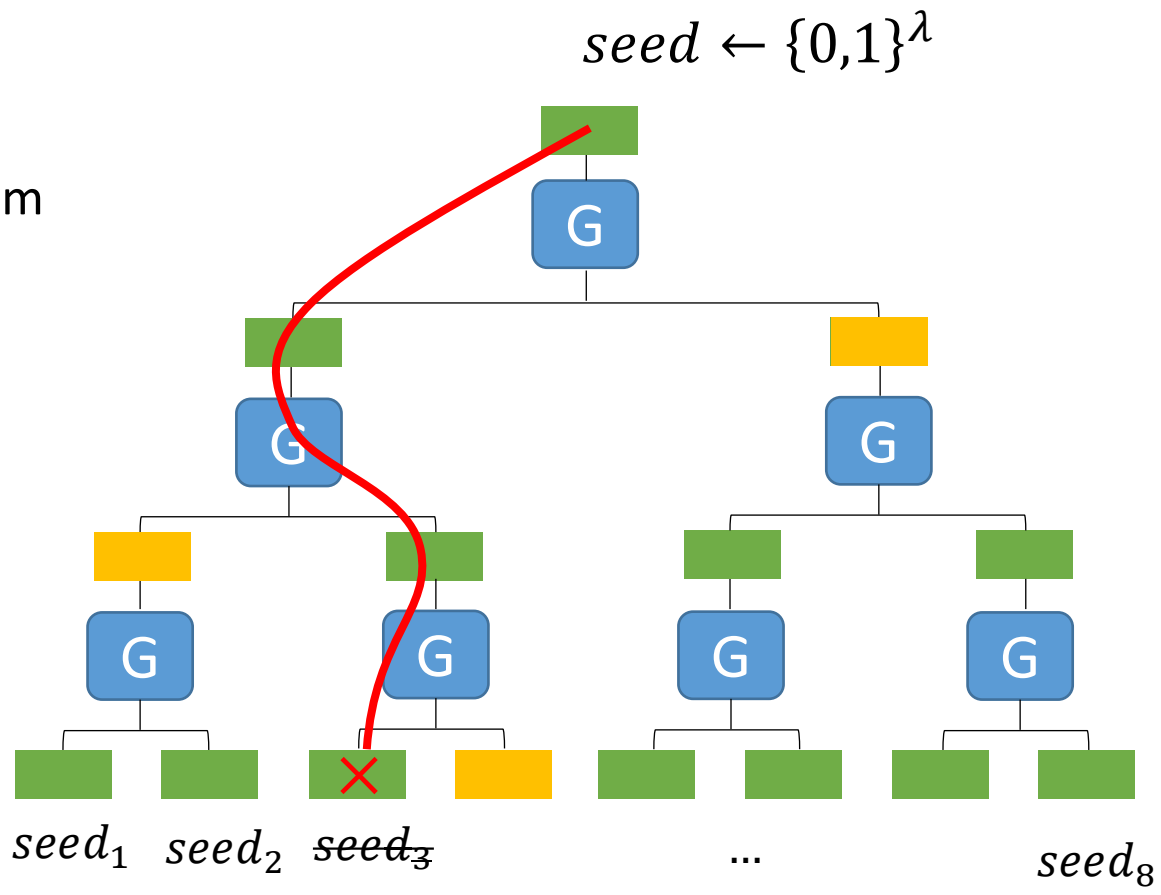
All-but-one commitments

Let G be a length-doubling PRG

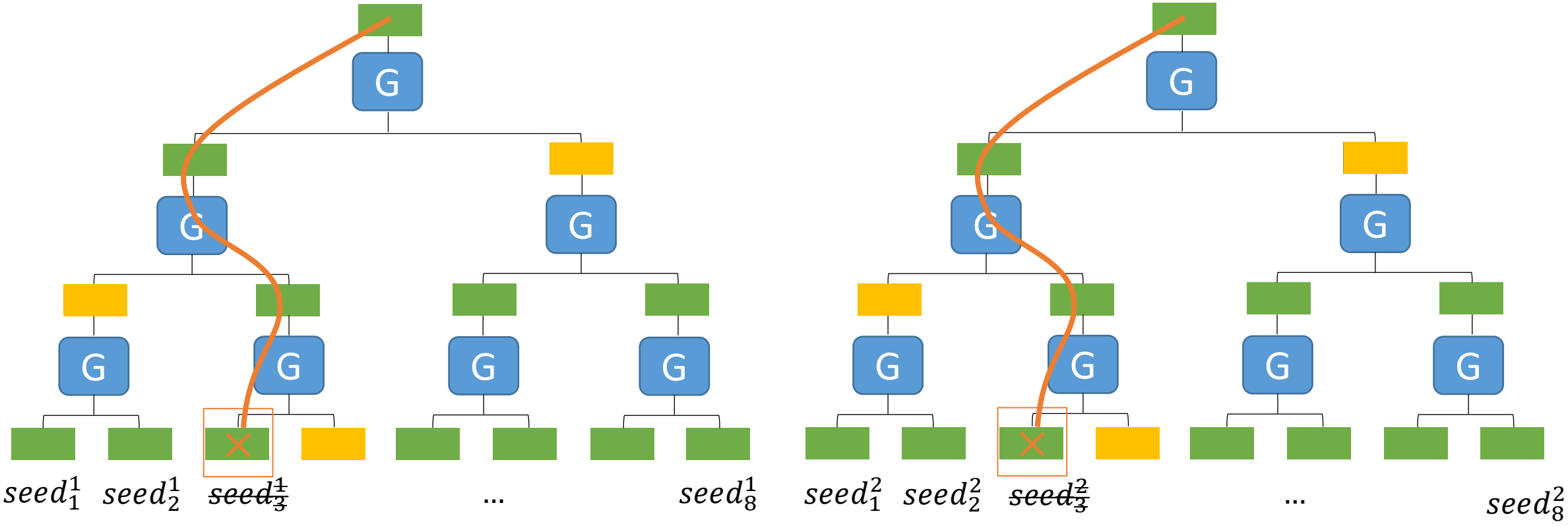
Derive all nodes and leaves recursively from root via G

Open $n-1$ leaves (seeds):

- Send $O(\log n)$ PRG seeds

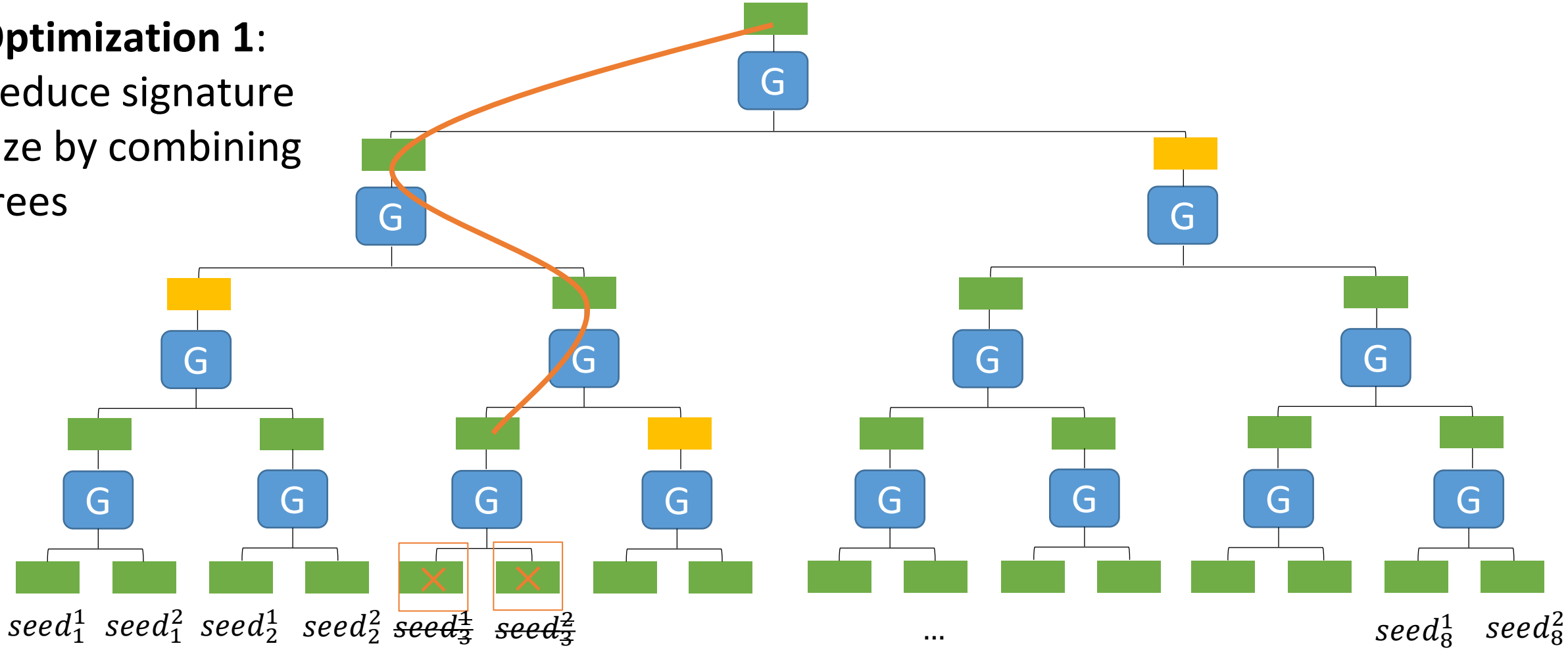


FAESTv1: Multiple GGM trees in parallel



FAEST version 2: One-tree optimization [BBM+24]

Optimization 1:
Reduce signature size by combining trees



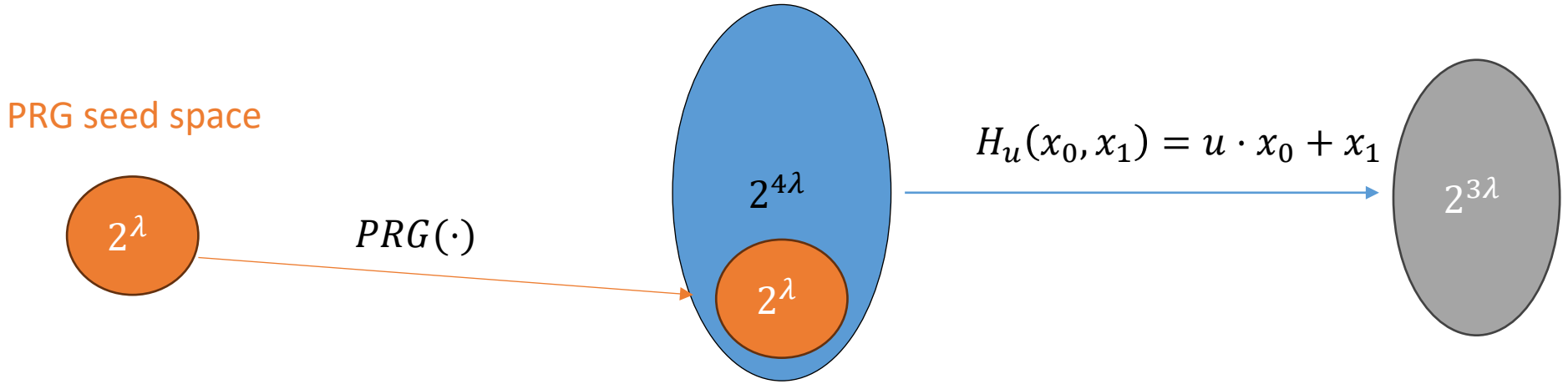
More optimizations!

Computing these is expensive!

Current state

Prover sends $\mathrm{h} = H(com(seed_1)| \cdots |com(seed_n))$

New idea: compute $com(seed_i) = H'(PRG(seed_i))$ where H' is UHF



More optimizations!

Computing these is expensive!

Current state

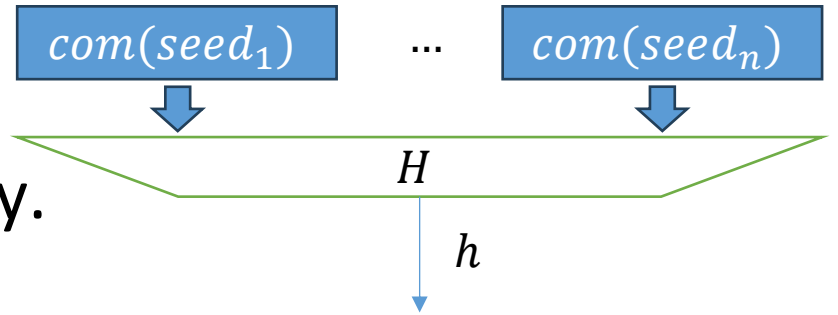
Prover sends $\mathrm{h} = H(com(seed_1)| \cdots |com(seed_n))$

New idea: compute $com(seed_i) = H'(PRG(seed_i))$ where H' is UHF

Problem: Breaks security proof.

Solution: Painful new security proof.

Result: Up to 2x speedup for sign and verify.



Talk outline

High level overview of FAEST

Round 2 changes:

1. Optimized vector commitments
2. Optimized AES proof strategy
3. Change keyspace for improved security proof

How to prove an AES encryption using VOLE-in-the-Head

VOLE-in-the-Head allows to prove any low-degree polynomial constraints of the witness. Cost of the proof is $O(\ |witness|\ + deg\ )$

Problem: $Enc_K(x) - y$ has a huge degree
(as a polynomial in bits of witness K)

Solution: Extend the witness with state after every AES round R

$w\ = (K, x_1, x_2, \dots, x_9\ )$. Prove $R(x_i) - x_{i+1}\ = 0$ for $i \in \{0, \dots, 9\}$

$$x = x_0 \ \xrightarrow{R}\ x_1 \ \xrightarrow{R}\ x_2 \ \xrightarrow{R}\ \dots \ \xrightarrow{R}\ x_9 \ \xrightarrow{R}\ x_{10} = y$$

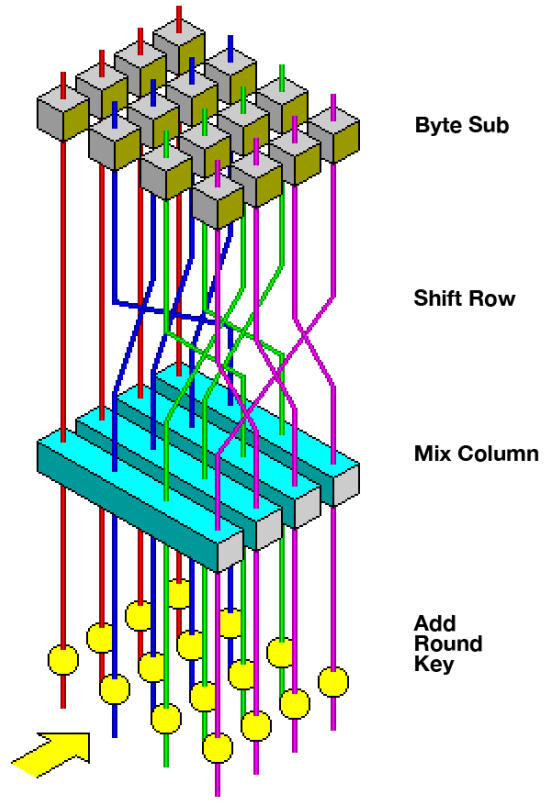
Proving a single AES round (Round 1 version)

Naively $R(x)$ has degree 7. But we did better.

The only nonlinear operation is the S-box

AES S-box is $\mathrm{a} \mapsto \begin{cases} \frac{1}{a} & a \neq 0 \\ 0 & a = 0 \end{cases}$

Instead of proving that $b = S(a)$, (degree 7)
we just prove $ab = 1$ (degree 2)



We make sure that no s-box has a zero input during KeyGen!

Proving two consecutive AES rounds together

Witness $= (K, x_2, \ldots, x_8)$. Prove $R(x_i) = R^{-1}(x_{i+2})$ for $i \in \{0, \ldots, 8\}$

$$x = x_0 \xrightarrow{R^2} x_2 \xrightarrow{R^2} \ldots \xrightarrow{R^2} x_8 \xrightarrow{R^2} x_{10} = y$$

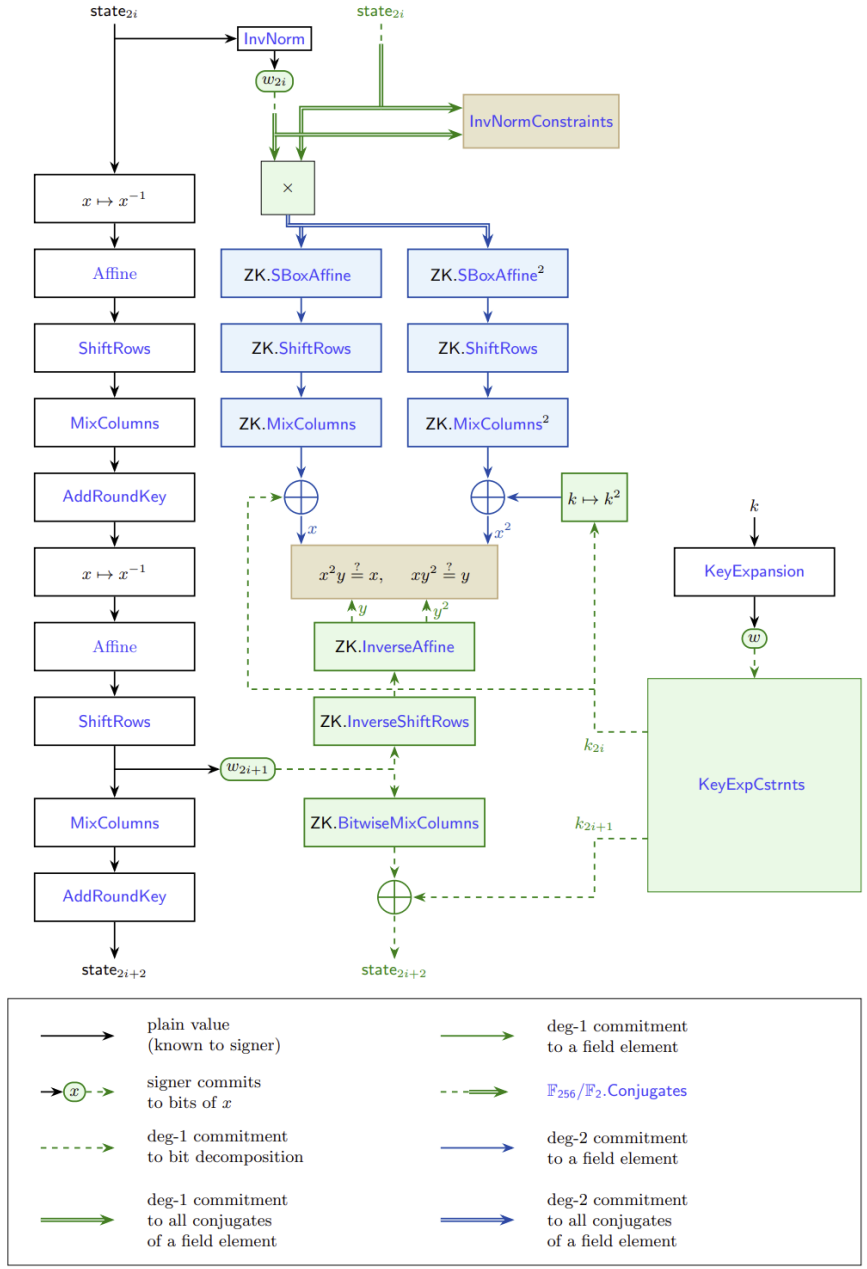
Reduce witness by 50%, but degree 7. Good, but we can do better!

Proving two consecutive rounds together. (Round 2)

We use a trick using the Field norm $N_{GF(256)/GF(16)}$ to have a witness size reduction of 25% and only use degree 3.

This gives roughly a 5% reduction in signature size.

Also, removes restriction that S-box inputs have to be non-zero.



Talk outline

High level overview of FAEST

Round 2 changes:

1. Optimized vector commitments
2. Optimized AES proof strategy
3. Change keyspace for improved security proof

Security proof in the QROM

One key idea is to make the keys “lossy” i.e. make it so that many public keys don’t have a corresponding secret key.

Extra constraint: The first two bits of the key are not both 1.
This is a quadratic constraint $K_1 K_2 = 0$,
so we can prove it for free.

Proof of EUF-KO security: Replace public key $(x, y = Enc_K(x))$ by a random pair. With probability $\sim 1/4$ there does not exist a secret key. So we only need soundness, not knowledge soundness.

Conclusion

FAEST is a signature scheme with **reasonably good performance** and very **conservative security assumptions**

The Round 2 version is **faster and has smaller signatures** due to various optimizations, and has a **security proof in the QROM**

https://faest.info