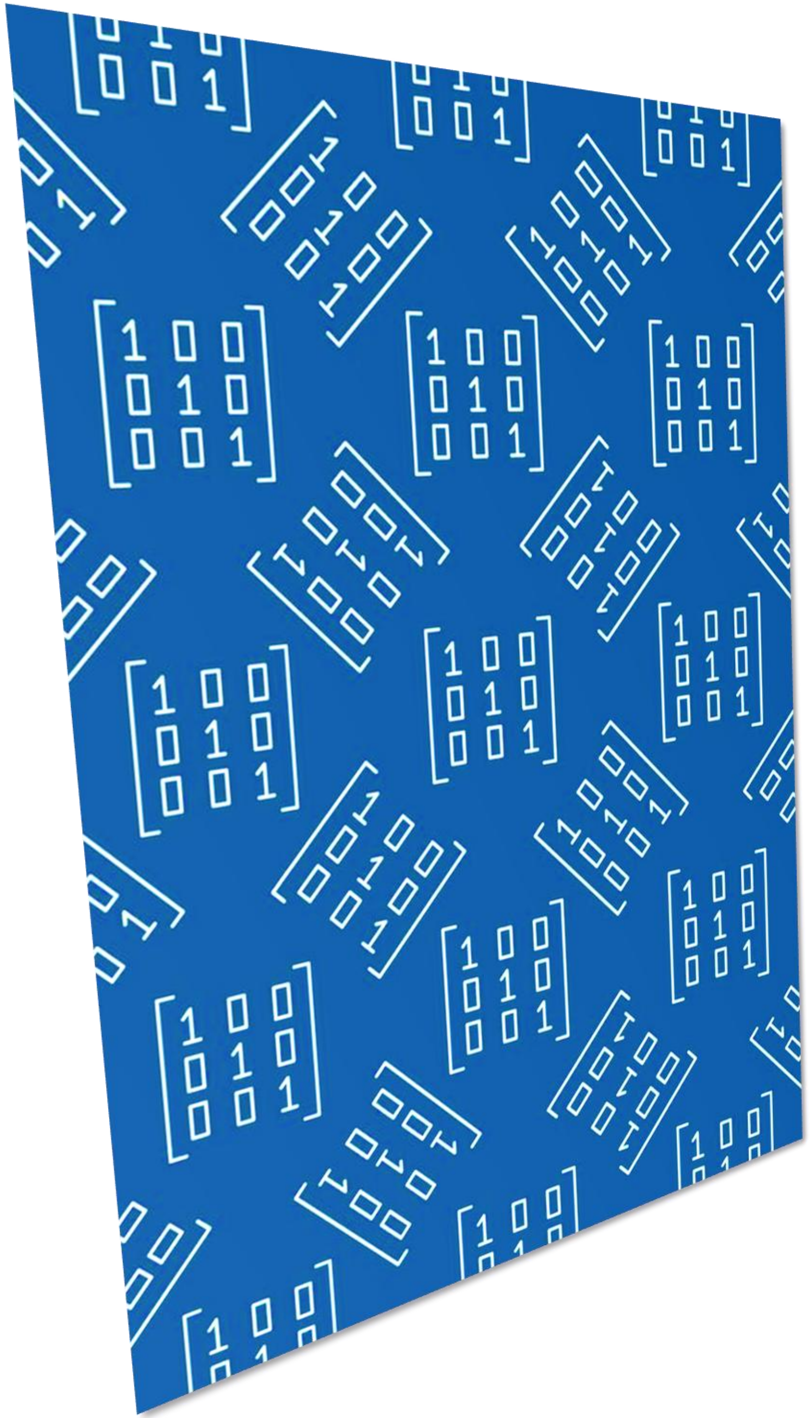


LESS

LINEAR EQUIVALENCE SIGNATURE SCHEME

SAPIENZA
UNIVERSITÀ DI ROMA

Politecnico di Torino
+CrypTO

Leonardo Errati

2025-06-20

LESSon 0:

LESS:
THE ORIGINS

2017 - CALL FOR PROPOSALS

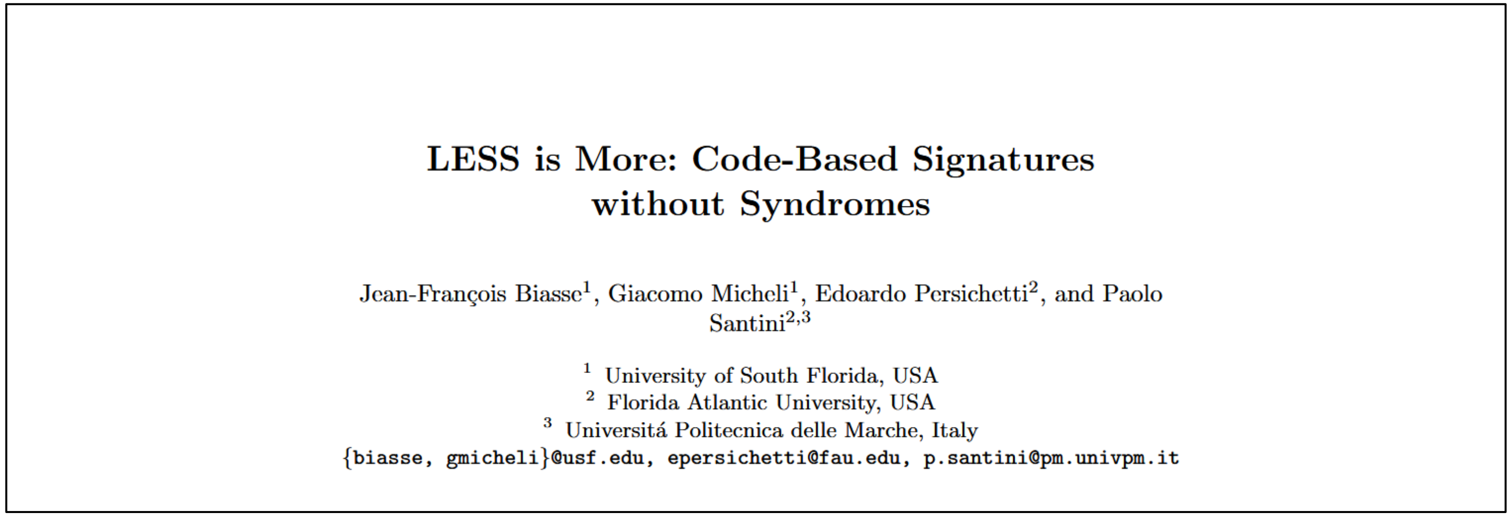
> *"NIST is soliciting proposals for post-quantum cryptosystems [...]. The goal of this process is to select a number of acceptable candidate cryptosystems for standardization."*

2024: standardisation of

- **CRYSTALS-Dilithium**
- **CRYSTALS-KYBER**
- **SPHINCS+**

NIST, *Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process*, 2022

2020 - LESS!



LESS is More: Code-Based Signatures without Syndromes

Jean-François Biasse[1], Giacomo Micheli[1], Edoardo Persichetti[2], and Paolo Santini[2,3]

[1] University of South Florida, USA
[2] Florida Atlantic University, USA
[3] Universitá Politecnica delle Marche, Italy
{biasse, gmicheli}@usf.edu, epersichetti@fau.edu, p.santini@pm.univpm.it

«[…] we construct a signature scheme by exploring a new approach to the area. […] We show that practical instances of our protocol have the potential to outperform the state of the art on code-based signatures […].»

Biasse, **Micheli**, **Persichetti**, **Santini**, LESS is More: Code-Based Signatures Without Syndromes, 2020

2022 - CALL FOR SIGNATURES

> «NIST is calling for additional digital signature proposals to be considered in the PQC standardization process.»

Requirements:

1. not based on structured lattices
2. performance advantage over **SPHINCS+**
3. if lattice-based, performance advantage over **CRYSTALS**

Dear Santa

My name is NIST

I am 124 years old.

I live in a place called USA

This year I have been

☐ Naughty ☐ Good ☐ Very Good ☒ A bit naughty

Could you please bring me

post-quantum

Thank you Santa!

Love from NIST

NIST, *Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process*, 2022

- WHAT IS **LINEAR EQUIVALENCE**?
- WHAT IS **LESS**?
- IS **LESS** SECURE?

*…WHAT IS A **CODE**?*

- WHAT IS **LINEAR EQUIVALENCE**?
- WHAT IS **LESS**?
- IS **LESS** SECURE?

*…WHAT IS A **CODE**?*

1. WHAT IS **LINEAR EQUIVALENCE**?
2. WHAT IS **LESS**?
3. IS **LESS** SECURE?

LESSon 1:

LINEAR CODE EQUIVALENCE

LINEAR CODES

LINEAR CODE

An (n, k)- **linear code** C is a k-dimensional subspace of F_q^n.
The matrix G whose rows are a basis of C is its **generator matrix.**

All generator matrices are connected by some change of basis $S \in GL_k(q)$.
For some S, $SG = (I_k \mid A)$. This is the **systematic form.**

LINEAR CODES

LINEAR CODE

An (n, k)- **linear code** C is a k-dimensional subspace of F_q^n.
The matrix G whose rows are a basis of C is its **generator matrix.**

All generator matrices are connected by some change of basis $S \in GL_k(q)$.
For some S, $SG = (I_k \mid A)$. This is the **systematic form.**

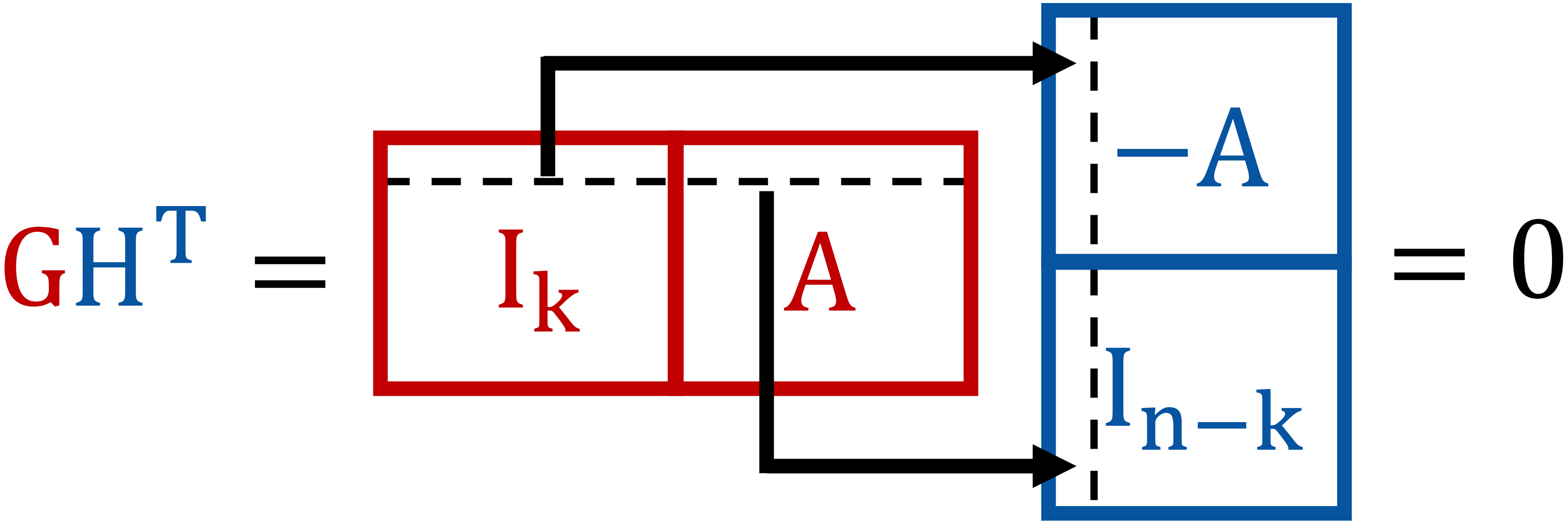
DUAL CODE

The dual of an (n, k)-linear code C is the $(n, n-k)$-linear code

$$C^{\perp} = \{y \in F_q^n : \forall x \in C, yx^T = 0\}$$

Its generator matrix is the **parity check matrix** of C.
If $G = (I_k \mid A)$, then $H = (-A^{\mathrm{T}} \mid I_{\mathrm{n-k}})$.

LINEAR CODES



$$\mathrm{GH^T} = \begin{pmatrix} \mathrm{I_k} & \mathrm{A} \end{pmatrix} \begin{pmatrix} -\mathrm{A} \\ \mathrm{I_{n-k}} \end{pmatrix} = 0$$

Its generator matrix is the **parity check matrix** of C.

If $G = (I_k \mid A)$, then $H = (-A^{\mathrm{T}} \mid I_{\mathrm{n-k}})$.

MEET: MONOMIAL MATRICES

Permutation

$\pi \in S_n$

$$\begin{bmatrix} & 1 & \\ & & 1 \\ 1 & & \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_3 & x_2 & x_1 \end{bmatrix}$$

Linear isometry

$\mu = (v; \pi) \in \underbrace{F_q^{*n} \rtimes S_n}_{M_n}$

$$\begin{bmatrix} & v_1 & \\ & & v_2 \\ v_3 & & \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} v_3x_3 & v_2x_2 & v_1x_1 \end{bmatrix}$$

MEET: MONOMIAL MATRICES

Permutation Equivalence Problem (search)

given C, C'
find $\pi \in S_n$ such that $C' = \pi(C)$

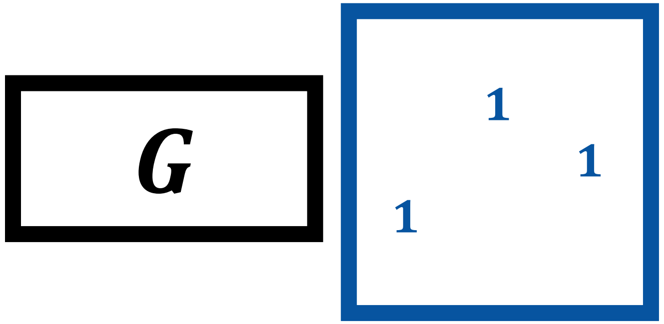
Linear Equivalence Problem (search)

given C, C'
find $\mu \in M_n$ such that $C' = \mu(C)$

MEET: MONOMIAL MATRICES

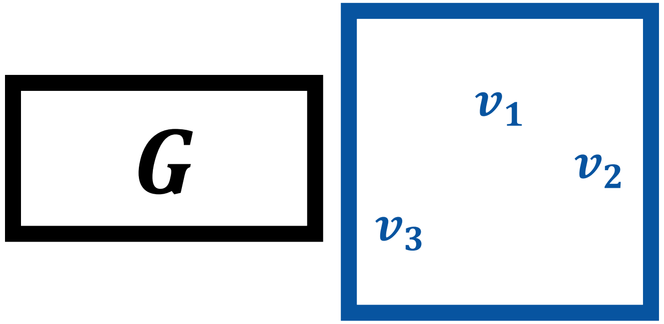
Permutation Equivalence Problem (search)

given G, G'
find $P \in S_n$ such that $G' = GP$



Linear Equivalence Problem (search)

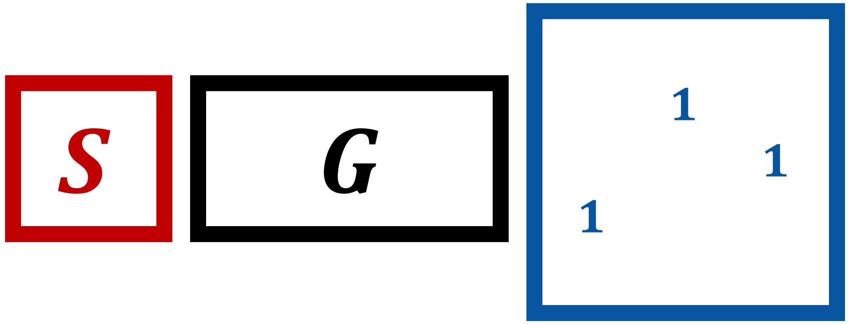
given G, G'
find $Q \in M_n$ such that $G' = GQ$



MEET: MONOMIAL MATRICES

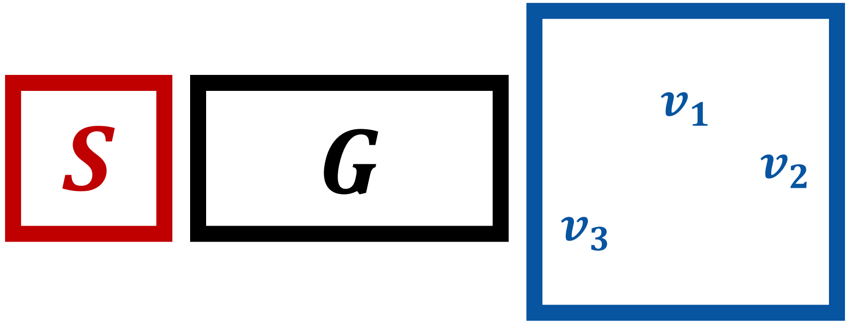
Permutation Equivalence Problem (search)

given G, G'
find $P \in S_n$ and $S \in GL_k(q)$ such that $G' = SGP$



Linear Equivalence Problem (search)

given G, G'
find $Q \in M_n$ and $S \in GL_k(q)$ such that $G' = SGQ$



COMLEXITY OF LEP & PEP

$$\begin{tikzcd}
\textbf{GIP} \arrow[r] & \textbf{PEP-search} \arrow[r, shift left] \arrow[d] & \textbf{PEP-decision} \arrow[l, shift left] \\
 & \textbf{LEP-search} \arrow[r, shift left] & \textbf{LEP-decision} \arrow[l, shift left]
\end{tikzcd}$$

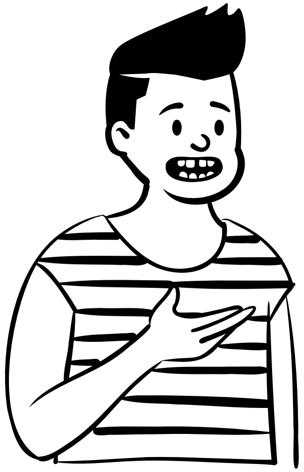
$\mathbf{A} \longrightarrow \mathbf{B}$ A reduces to B

Barenghi, **Biasse**, **Micheli**, **Persichetti**, **Santini**, *On The Computational Hardness Of The Code Equivalence Problem*, 2022
Battagliola, **Mora**, **Santini**, *Using the Schur Product to Solve the Code Equivalence Problem*, 2025

LESSon 2:

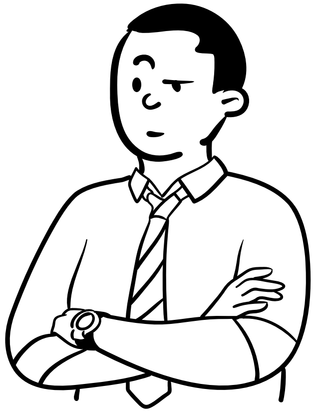
DESIGNING THE SCHEME

LESS: THE SIGMA PROTOCOL (ZKPoK)



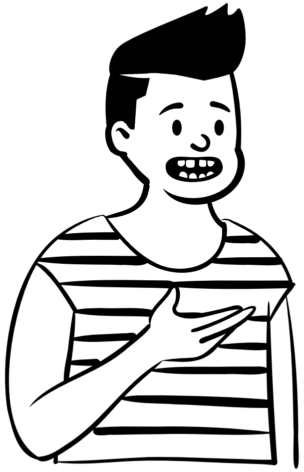
I know Q and S such that $G' = SGQ$!

Prove it.



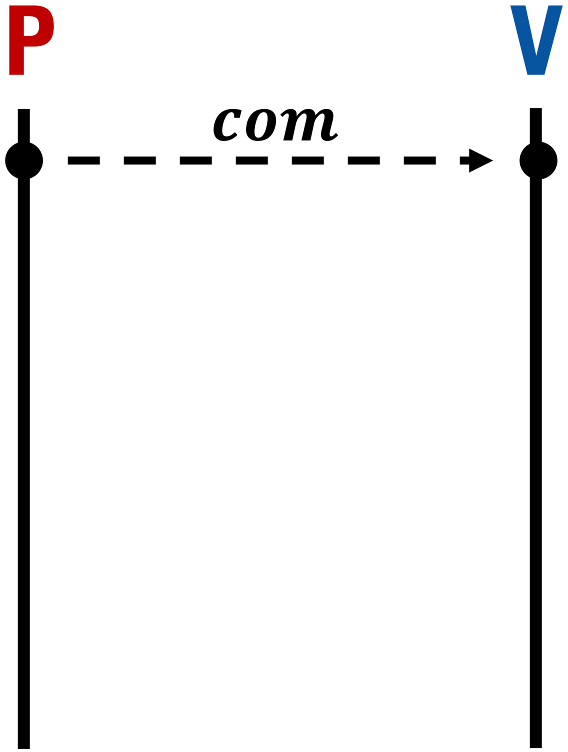
Biasse, **Micheli**, **Persichetti**, **Santini**, *LESS is More: Code-Based Signatures without Syndrome*, 2020

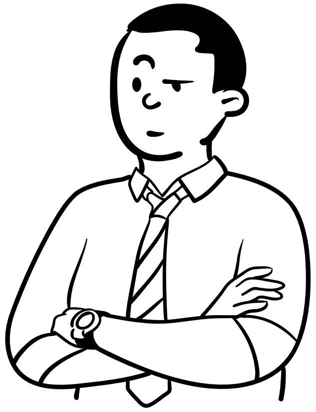
LESS: THE SIGMA PROTOCOL (ZKPoK)



random $\bar{Q} \in M_n$

$com = SF(G\bar{Q})$

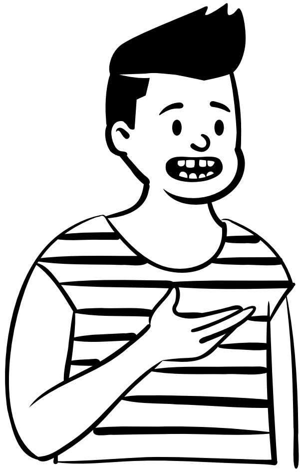




$Q, S: \ G' = SGQ$

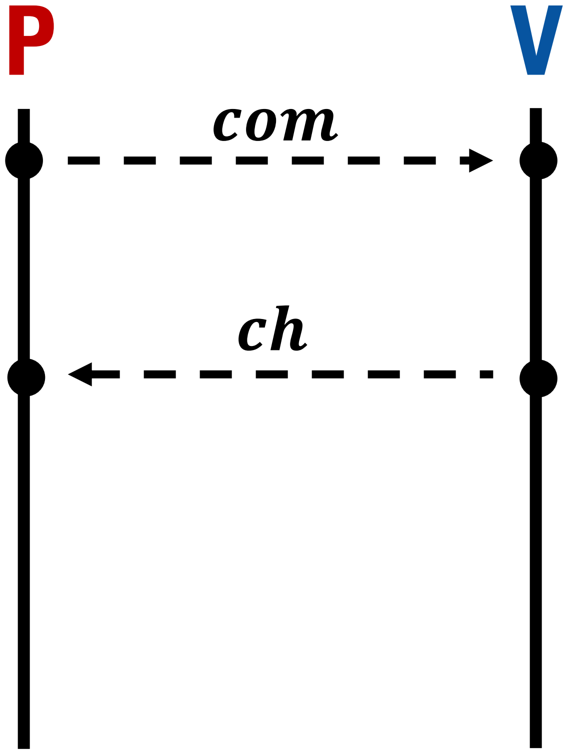
Biasse, **Micheli**, **Persichetti**, **Santini**, *LESS is More: Code-Based Signatures without Syndrome*, 2020

LESS: THE SIGMA PROTOCOL (ZKPoK)

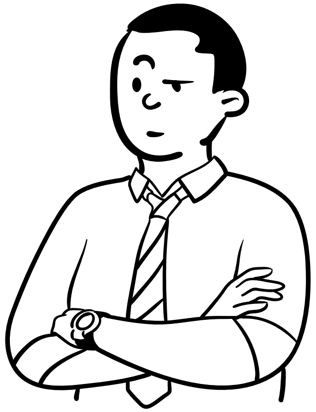


random $\bar{Q} \in M_n$

$com = SF(G\bar{Q})$



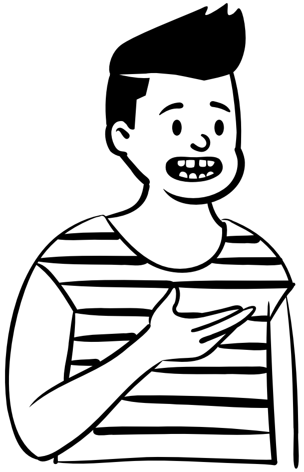
random $ch \in \{0,1\}$

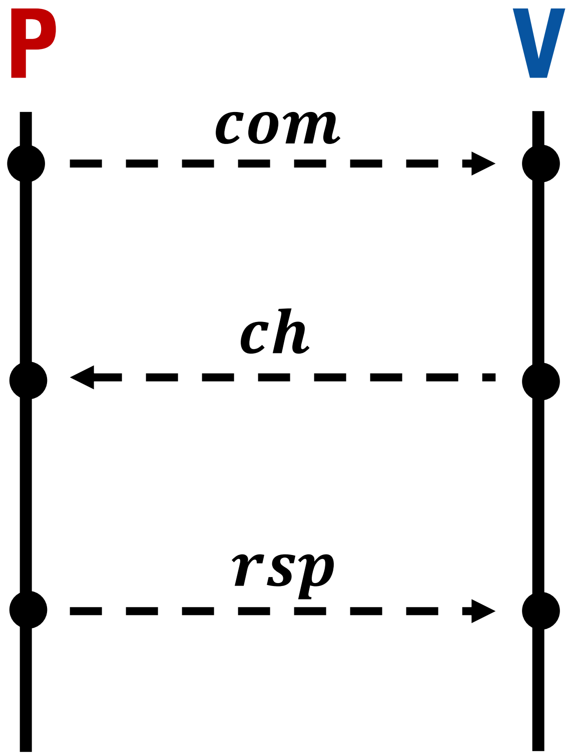


$Q, S: \; G' = SGQ$

Biasse, **Micheli**, **Persichetti**, **Santini**, *LESS is More: Code-Based Signatures without Syndrome*, 2020

LESS: THE SIGMA PROTOCOL (ZKPoK)





random $\bar{Q} \in M_n$

$com = SF(G\bar{Q})$

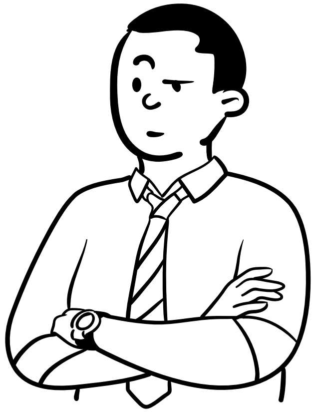
random $ch \in \{0, 1\}$

if $ch = 0\,, rsp = \bar{Q}$

if $ch = 1, rsp = Q^{-1}\bar{Q}$

$SF(G \cdot rsp) = com$

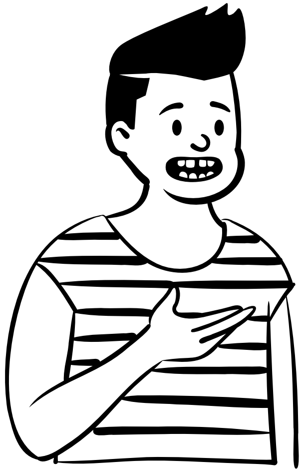
$SF(G' \cdot rsp) = com$

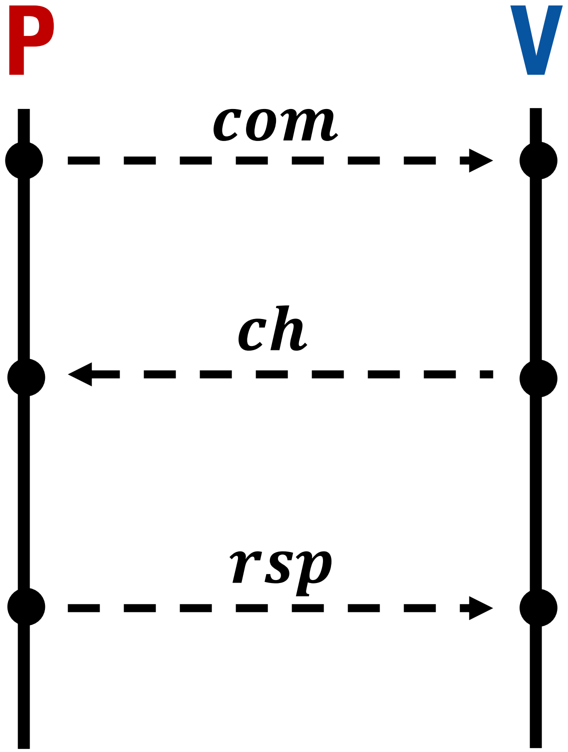


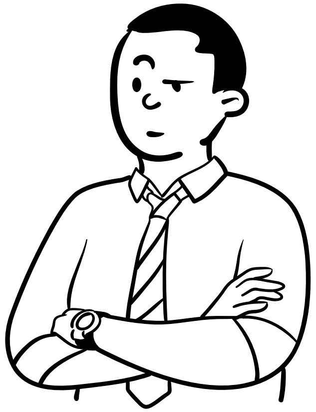
$Q, S:\ G' = SGQ$

Biasse, **Micheli**, **Persichetti**, **Santini**, *LESS is More: Code-Based Signatures without Syndrome*, 2020

LESS: THE SIGMA PROTOCOL (ZKPoK)







random $\bar{Q} \in M_n$

$com = h(SF(G\bar{Q}))$

random $ch \in \{0,1\}$

if $ch = 0\,, rsp = \bar{Q}$

if $ch = 1, rsp = Q^{-1}\bar{Q}$

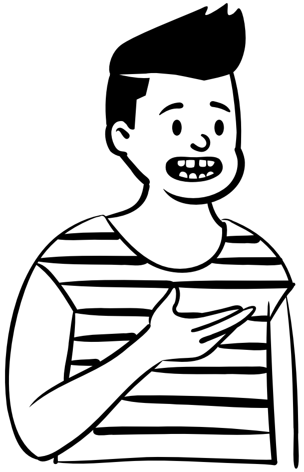
$h(SF(G \cdot rsp)) = com$

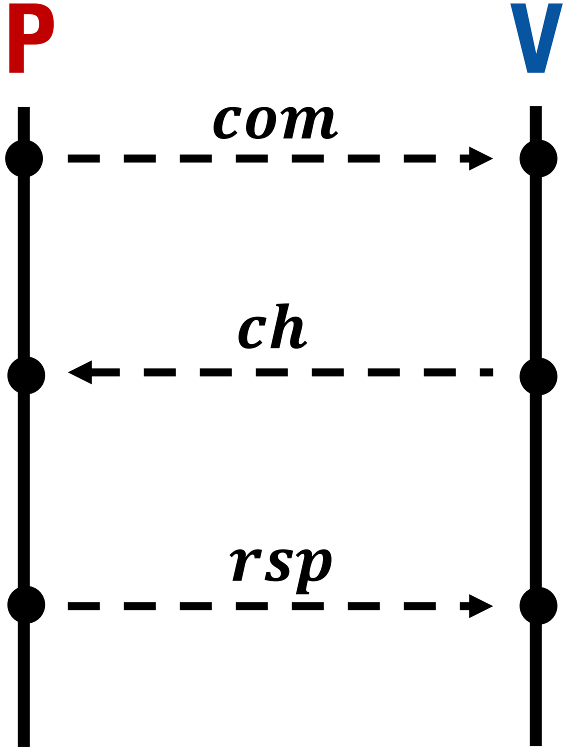
$h(SF(G' \cdot rsp)) = com$

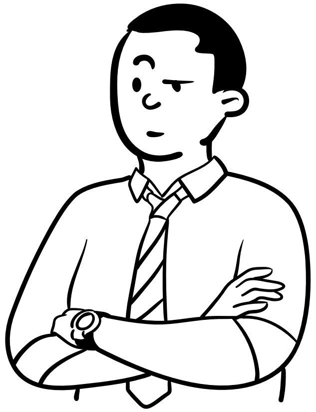
$Q, S: \; G' = SGQ$

Biasse, Micheli, Persichetti, Santini, *LESS is More: Code-Based Signatures without Syndrome*, 2020

LESS: THE SIGMA PROTOCOL (ZKPoK)







random $\overline{Q} \in M_n$

$com = h(RREF(G\overline{Q}))$

random $ch \in \{0,1\}$

if $ch = 0$, $rsp = \overline{Q}$

if $ch = 1$, $rsp = Q^{-1}\overline{Q}$

$h(RREF(G \cdot rsp)) = com$

$h(RREF(G' \cdot rsp)) = com$

$Q\colon\ G' = RREF(SQ)$

Biasse, Micheli, Persichetti, Santini, *LESS is More: Code-Based Signatures without Syndrome*, 2020

LESS: THE SIGMA PROTOCOL (ZKPoK)

$$\begin{tikzcd}
\boldsymbol{G} \arrow[rr, dashed, "\textbf{witness}"] \arrow[dr, "\overline{\boldsymbol{Q}}"'] & & \boldsymbol{G'} \arrow[dl, "\boldsymbol{Q}^{-1}\overline{\boldsymbol{Q}}"] \\
& \boldsymbol{RREF}(\boldsymbol{G}\overline{\boldsymbol{Q}}) &
\end{tikzcd}$$

Biasse, **Micheli**, **Persichetti**, **Santini**, *LESS is More: Code-Based Signatures without Syndrome*, 2020

LESS: THE SIGNATURE

```
**random** $\bar{Q} \in M_n$
$com_i = h(RREF(G\bar{Q}))$        $i = 1, \dots, t$

$ch = h(m, com)$
$ch_i = ch[i]$                     $i = 1, \dots, t$

for $i = 1, \dots, t$
    if $ch_i = 0$, $rsp_i = \bar{Q}$
    if $ch_i = 1$, $rsp_i = Q^{-1}\bar{Q}$

$\sigma \leftarrow (com_1, \dots, com_t, rsp_1, \dots, rsp_t)$
```

$$\begin{tikzcd}
G \arrow[rr, dashed, "\text{witness}"] \arrow[dr, "\bar{Q}_i"'] & & G' \arrow[dl, "Q^{-1}\bar{Q}_i"] \\
& RREF(G\bar{Q}_i) &
\end{tikzcd}$$

soundness of Σ is ½,
iterate $t = \lambda$ times

Biasse, **Micheli**, **Persichetti**, **Santini**, *LESS is More: Code-Based Signatures without Syndrome*, 2020

LESSon 3:

SECURITY & ATTACKS

SECURITY PROOF

FACT

If Σ is a non-trivial canonical identification protocol secure against passive impersonation attacks, the signature scheme FS(Σ) is UF-CMA secure,

$$“\ Adv_{FS(\Sigma),A}^{uf-cma}(\lambda) \leq f(\lambda) \cdot Adv_{\Sigma,B}^{pa-imp}(\lambda) + g(\lambda)\ ”$$

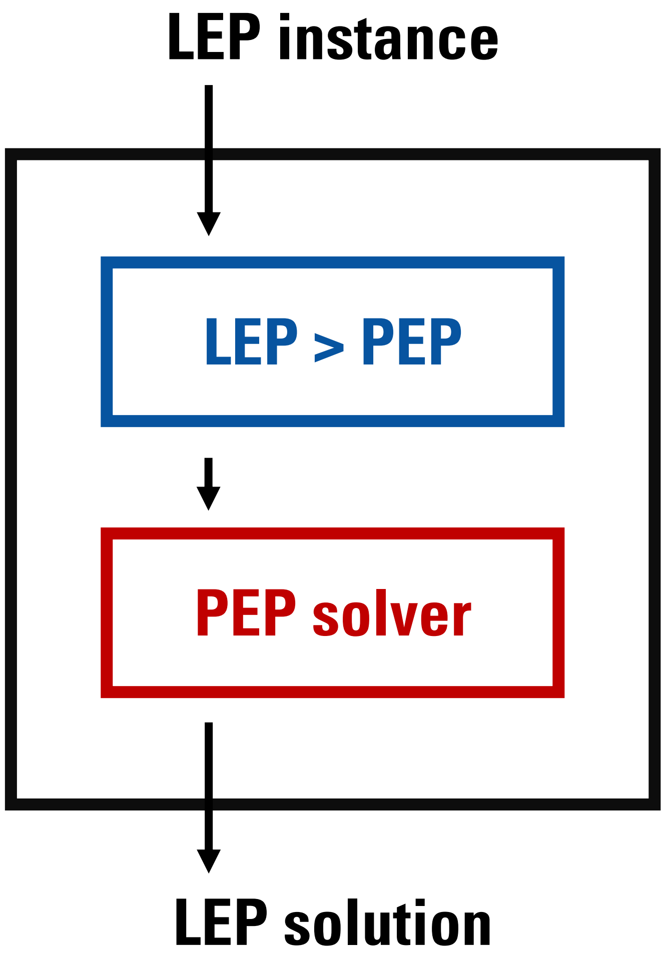
This holds in **ROM** and is believed to hold for the **QROM**.
The security of LESS is based on that of LEP.

uf-cma sec. of $FS(\Sigma)$ ⟶ **pa-imp sec. of Σ** ⟶ **LEP-search**

Abdalla, **An**, **Bellare**, **Namprempre**, *From Identification to Signatures via the Fiat-Shamir Transform*, 2002
Don, **Fehr**, **Majenz**, **Schaffner**, *Security of the Fiat-Shamir transformation in the quantum random-oracle model*, 2019

ATTACKS

Type 1: solving PEP (e.g. SSA)



LEP instance

LEP > PEP

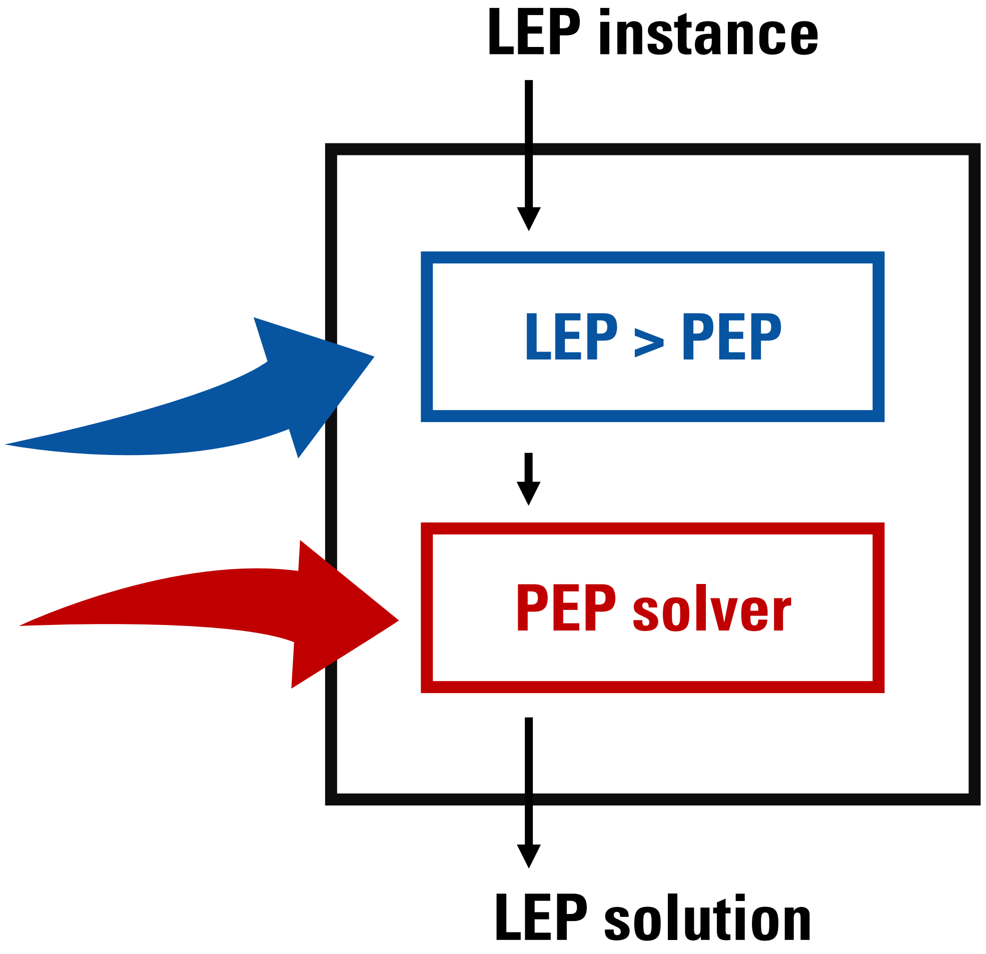
PEP solver

LEP solution

ATTACKS

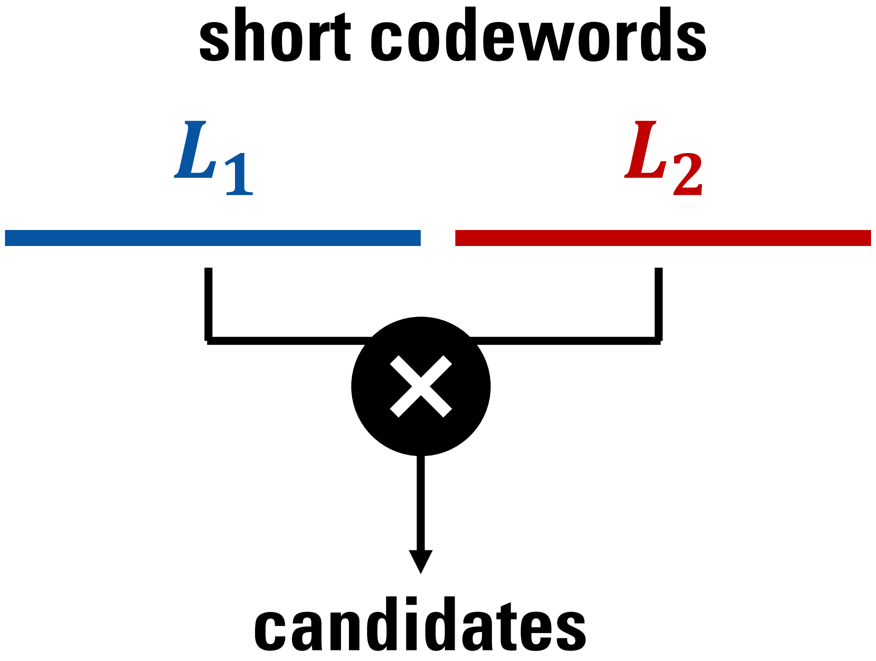
Type 1: solving PEP (e.g. SSA)

- if two codes are linearly equivalent, their **closures** are permutationally equivalent $cl(C)_a = \{c \otimes a : c \in C\}$ (a ordering of F_q^*)
- deteriorates with dimension of the **hull** of the code, but closures have maximal hull…



LESS team, *LESS: Linear Equivalence Signature Scheme (v2)*, 2025

ATTACKS



short codewords

L_1 L_2

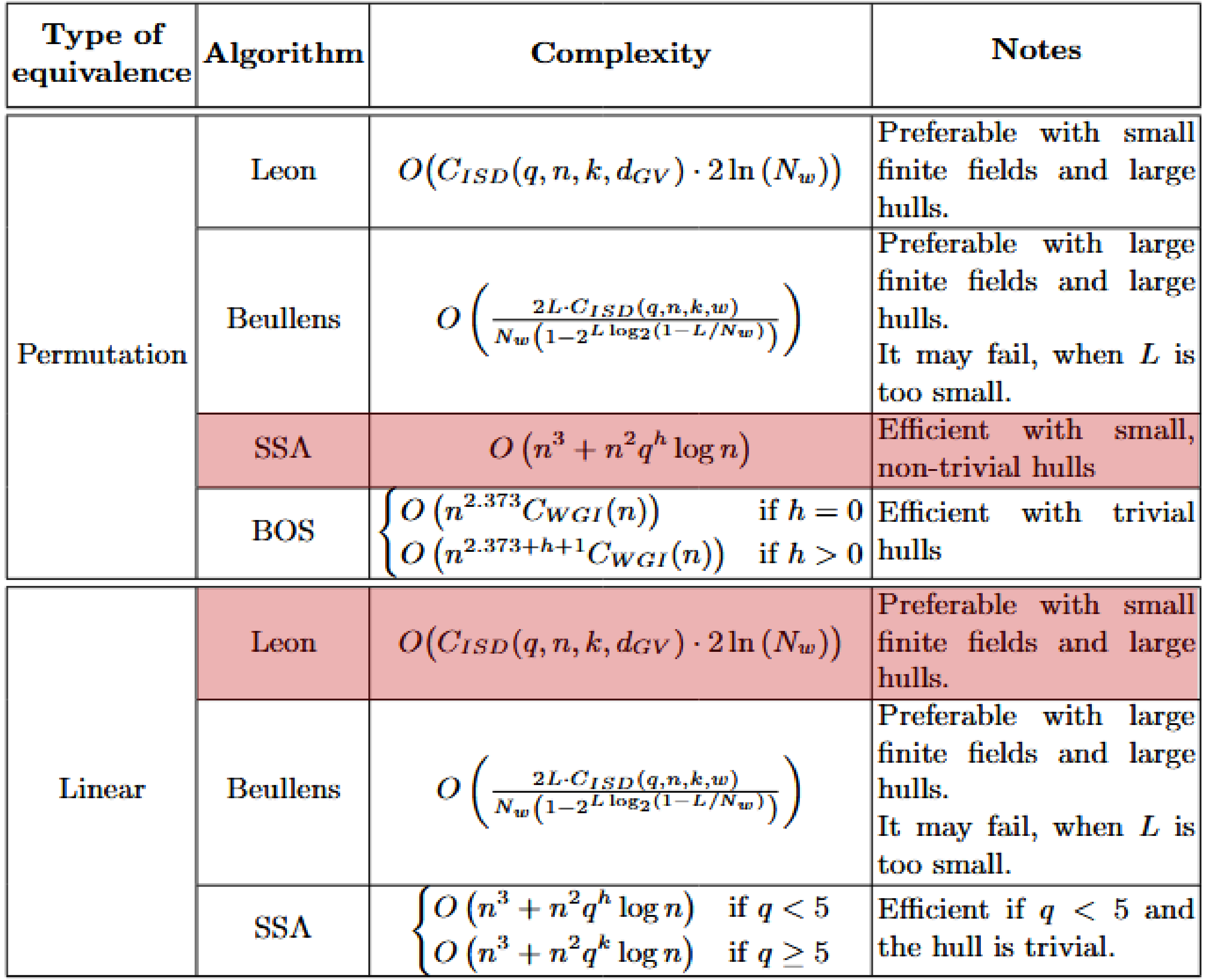
candidates

Type 2: low-weight codeword finding (e.g. Prange)

- in general of exponential complexity
- structured variants deteriorate with increasing q
- Leon’s algorithm: generate relations with L_1, L_2 of weight-w codewords such that $L_1 = QL_2$
- NIST constraints the depth of quantum circuits, rendering quantum attacks (e.g. Prange + Grover) impractical

LESS team, *LESS: Linear Equivalence Signature Scheme (v2)*, 2025

ATTACKS



Type of equivalence	Algorithm	Complexity	Notes
Permutation	Leon	$O(C_{ISD}(q,n,k,d_{GV})\cdot 2\ln(N_w))$	Preferable with small finite fields and large hulls.
	Beullens	$O\left(\frac{2L\cdot C_{ISD}(q,n,k,w)}{N_w\left(1-2^{L\log_2(1-L/N_w))}\right)}\right)$	Preferable with large finite fields and large hulls. It may fail, when L is too small.
	SSA	$O\left(n^3+n^2q^h\log n\right)$	Efficient with small, non-trivial hulls
	BOS	$\begin{cases} O\left(n^{2.373}C_{WGI}(n)\right) & \text{if } h=0 \\ O\left(n^{2.373+h+1}C_{WGI}(n)\right) & \text{if } h>0 \end{cases}$	Efficient with trivial hulls
Linear	Leon	$O(C_{ISD}(q,n,k,d_{GV})\cdot 2\ln(N_w))$	Preferable with small finite fields and large hulls.
	Beullens	$O\left(\frac{2L\cdot C_{ISD}(q,n,k,w)}{N_w\left(1-2^{L\log_2(1-L/N_w))}\right)}\right)$	Preferable with large finite fields and large hulls. It may fail, when L is too small.
	SSA	$\begin{cases} O\left(n^3+n^2q^h\log n\right) & \text{if } q<5 \\ O\left(n^3+n^2q^k\log n\right) & \text{if } q\geq 5 \end{cases}$	Efficient if $q<5$ and the hull is trivial.

Table 2: Summary of techniques to solve the code equivalence problem

LESS team, *LESS: Linear Equivalence Signature Scheme (v2)*, 2025

PARAMETERS

$$
\begin{aligned}
Adv_{FS(\Sigma),A}^{uf-cma}(\lambda) &\leq f(\lambda) \cdot Adv_{\Sigma,B}^{pa-imp}(\lambda) + g(\lambda) \\
&\leq f'(\lambda) \cdot Adv_{C}^{LEP}(\lambda) + g'(\lambda)
\end{aligned}
$$

PARAMETERS

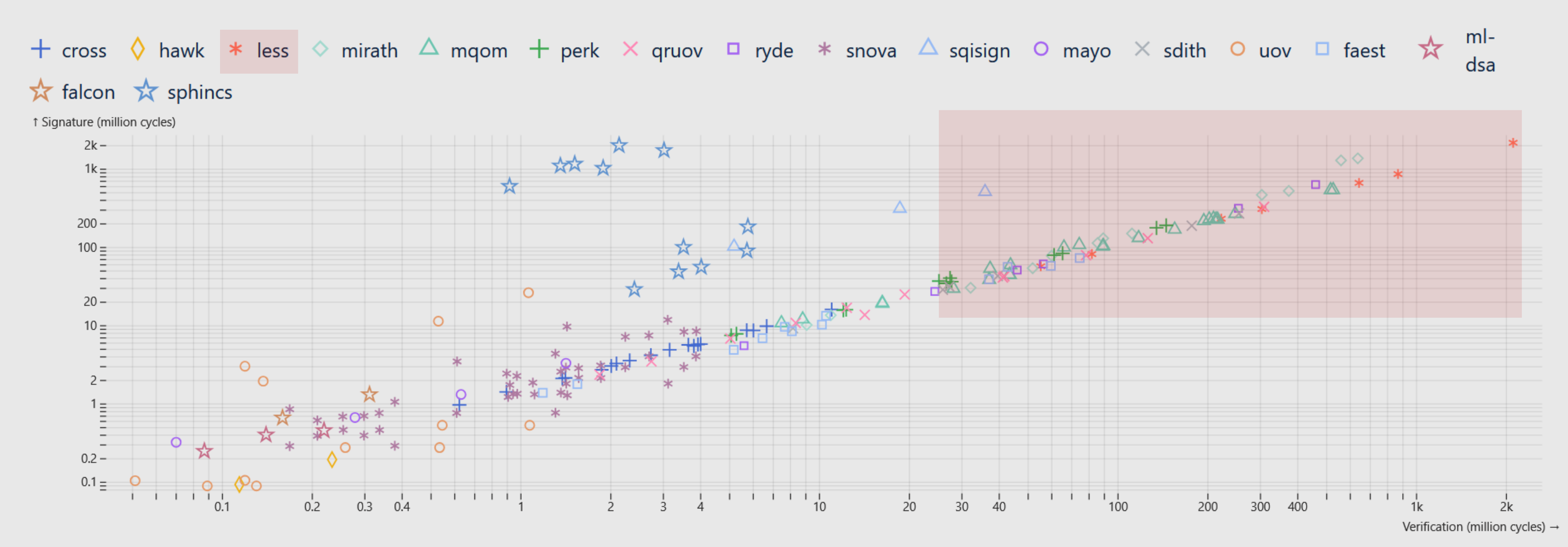
$$Adv^{uf-cma}_{FS(\Sigma),A}(\lambda) \leq f(\lambda) \cdot Adv^{pa-imp}_{\Sigma,B}(\lambda) + g(\lambda)$$
$$\leq f'(\lambda) \cdot Adv^{LEP}_{C}(\lambda) + g'(\lambda)$$

INSTANTIATION

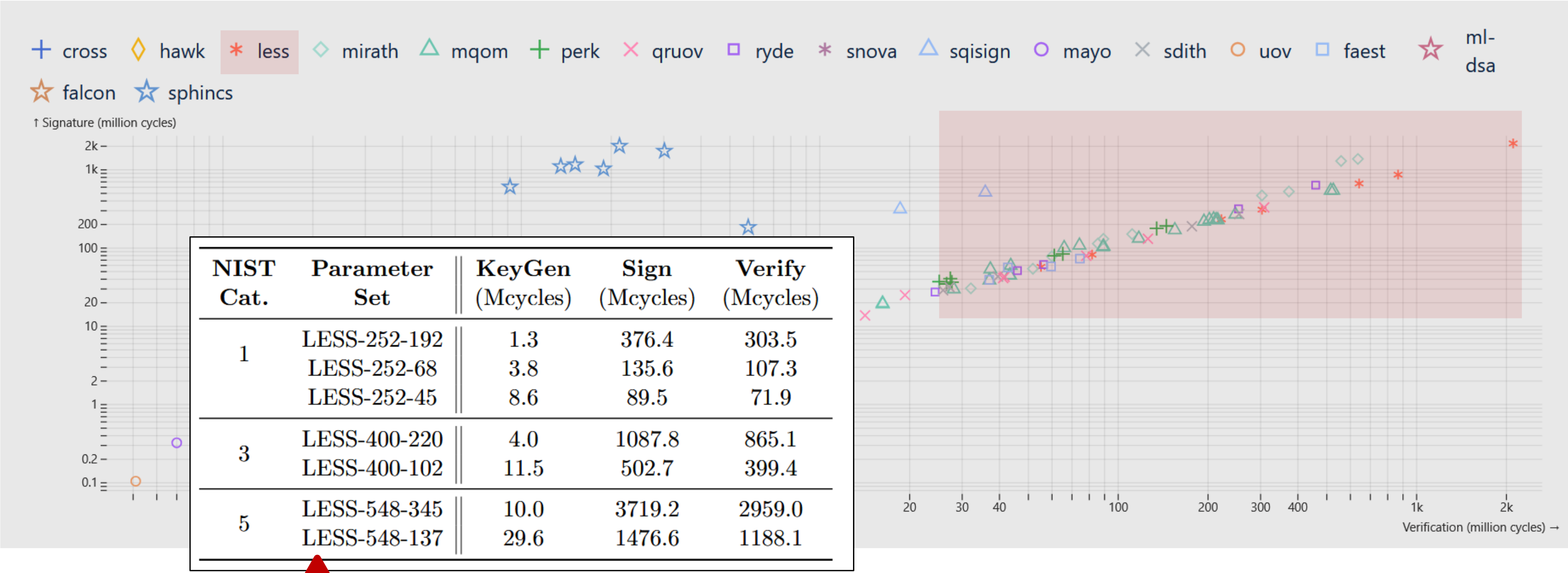
Consider $q \geq 5$ and random codes. We select n, k, q such that for any weight $w = 1, \ldots, n$ finding lists of weight- w codewords L_1 and L_2 having non-empty $L_1 \cap L_2 Q$ takes at least time 2^{λ}.

$$\frac{C_{ISD}(w)}{\sqrt{N(w)}} < 2^{\lambda}$$

FOR AN OLD VERSION OF LESS!



TII, *PQsort*



NIST Cat.	Parameter Set	KeyGen (Mcycles)	Sign (Mcycles)	Verify (Mcycles)
1	LESS-252-192	1.3	376.4	303.5
	LESS-252-68	3.8	135.6	107.3
	LESS-252-45	8.6	89.5	71.9
3	LESS-400-220	4.0	1087.8	865.1
	LESS-400-102	11.5	502.7	399.4
5	LESS-548-345	10.0	3719.2	2959.0
	LESS-548-137	29.6	1476.6	1188.1

NEW VERSION OF LESS!

TII, *PQsort*

LESS team, *LESS: Linear Equivalence Signature Scheme (v2)*, 2025

…WHAT IS A ***CODE****?*

1. WHAT IS **LINEAR EQUIVALENCE**?
2. WHAT IS **LESS**?
3. IS **LESS** SECURE?

LESSon 4:

UPGRADES!

LESSon 4:

UPGRADES!

… an overview

LESS-F

```
random $\bar{Q} \in M_n$
$com_i = h(RREF(G\bar{Q}))$        $i = 1, \dots, t$

$ch = h(m, com)$
$ch_i = ch[i]$                     $i = 1, \dots, t$

for $i = 1, \dots, t$
    if $ch_i = 0$ , $rsp_i = \bar{Q}$
    if $ch_i = 1, rsp_i = Q^{-1}\bar{Q}$

$\sigma \leftarrow (com_1, \dots, com_t, rsp_1, \dots, rsp_t)$
```

idea: challenge is lighter for $b = 0$, just send the seed used to generate $\bar{Q}$

Use a weight-restricted hash h.

- ☹ need more rounds t
- ☺ more efficient broadcasts

Barenghi, **Biasse**, **Persichetti**, **Santini**, *LESS-FM: Fine-tuning Signatures from the Code Equivalence Problem*, 2021

LESS-M

random $\overline{Q} \in M_n$
$com_i = h(RREF(G\overline{Q}))$ $\quad i = 1, \dots, t$

$ch = h(m, com)$
$\boldsymbol{ch_i = ch[(i-1)\ell, i\ell]}$ $\quad \boldsymbol{i = 1, \dots, t}$

for $i = 1, \dots, t$
    if $ch_i = 1, rsp_i = \boldsymbol{Q_{ch_i}^{-1}}\overline{Q}$

$\sigma \leftarrow (com_1, \dots, com_t, rsp_1, \dots, rsp_t)$

idea: increasing the challenge space reduces repetitions t

The ch_i become ℓ- bit challenges, interpreted as integers in $[0, 2^{\ell} - 1]$.

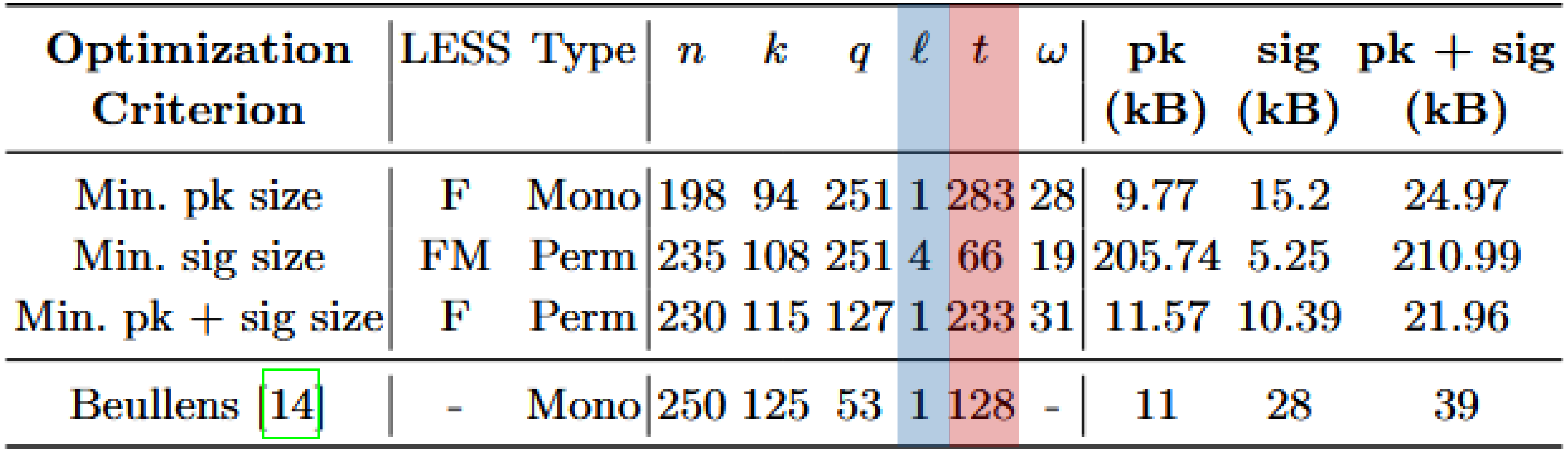
☹ 2^{ℓ} public keys Q_i (note: $Q_1 = I_n$)

☺ reduced rounds t

Barenghi, **Biasse**, **Persichetti**, **Santini**, *LESS-FM: Fine-tuning Signatures from the Code Equivalence Problem*, 2021

LESS-FM

LESS-F + LESS-M



Optimization Criterion	LESS Type		n	k	q	ℓ	t	ω	pk (kB)	sig (kB)	pk + sig (kB)
Min. pk size	F	Mono	198	94	251	1	283	28	9.77	15.2	24.97
Min. sig size	FM	Perm	235	108	251	4	66	19	205.74	5.25	210.99
Min. pk + sig size	F	Perm	230	115	127	1	233	31	11.57	10.39	21.96
Beullens [14]	-	Mono	250	125	53	1	128	-	11	28	39

Table 7: Parameter sets for LESS-FM, for a security level of $\lambda = 128$ classical bits.

Barenghi, Biasse, Persichetti, Santini, *LESS-FM: Fine-tuning Signatures from the Code Equivalence Problem*, 2021

IS-LESS

idea: for $b = 1$, just consider the action of $\boldsymbol{Q}^{-1}\overline{\boldsymbol{Q}}$ on an information set J

But the verifier needs to compute the same code.

coordinates in J: equal up to invertible matrix $\bar{G}_J{}' = S\bar{G}_J$

coordinates outside J: equal up to invertible and monomial matrices $\bar{G}_{[n]\setminus J}{}' = S\bar{G}_{[n]\setminus J}Z$

solution: compute a «canonical form»

$$\begin{tikzcd}
\textbf{prover: } RREF(\bar{G}_J) \text{ w.r.t. } J \arrow[r] \arrow[d, phantom, "\nparallel"] & V = \bar{G}_J^{-1}\bar{G}_{[n]\setminus J} \arrow[r] & \text{scale \& sort columns in lexicographical order} \arrow[d, phantom, "\parallel"] \\
\textbf{verifier: } RREF(\bar{G}_J{}') \text{ w.r.t. } J \arrow[r] & V' = \bar{G}_J^{-1}\bar{G}_{[n]\setminus J}Z \arrow[r] & \text{scale \& sort columns in lexicographical order}
\end{tikzcd}$$

Persichetti, **Santini**, *A New Formulation of the Linear Equivalence Problem and Shorter LESS Signatures*, 2023

INTERLUDE: CRYPTOGRAPHIC GROUP ACTIONS

$$\begin{aligned} \star\ : G \times X &\to X \\ (g, x) &\mapsto x \star g \end{aligned}$$

Cryptographic if:

- **effective** (efficient sampling, membership testing, evaluation)
- pseudorandom outputs
- one-way
- …

Alamati, **De Feo**, **Montgomery**, **Patranabis**, *Cryptographic Group Actions and Applications*, 2020

INTERLUDE: CRYPTOGRAPHIC GROUP ACTIONS

$$\star\ : G \times X \to X$$
$$((S;(\alpha, Q)), A) \mapsto S\alpha(GQ)$$

$G = GL_k(q) \rtimes (Aut(F_q) \times M_n)$

$X \subset F_q^{k\times n}$ full-rank matrices

Alamati, **De Feo**, **Montgomery**, **Patranabis**, *Cryptographic Group Actions and Applications*, 2020

LESS team, *LESS: Linear Equivalence Signature Scheme (v2)*, 2025

INTERLUDE: CRYPTOGRAPHIC GROUP ACTIONS

$$\star\ : G \times X \to X$$
$$((S; (\alpha, Q)), A) \mapsto S\alpha(GQ)$$

$G = GL_k(q) \rtimes (Aut(F_q) \times M_n)$ monomial operations & change of basis

$X \subset F_q^{k\times n}$ full-rank matrices code generators

---

Alamati, **De Feo**, **Montgomery**, **Patranabis**, *Cryptographic Group Actions and Applications*, 2020

LESS team, *LESS: Linear Equivalence Signature Scheme (v2)*, 2025

INTERLUDE: CRYPTOGRAPHIC GROUP ACTIONS

$$\star\ : G \times X \to X$$
$$((S; (\alpha, Q)), A) \mapsto S\alpha(GQ)$$

$G = GL_k(q) \rtimes (Aut(F_q) \times M_n)$ monomial operations & change of basis

$X \subset F_q^{k\times n}$ full-rank matrices code generators

excellent framework!

Alamati, **De Feo**, **Montgomery**, **Patranabis**, *Cryptographic Group Actions and Applications*, 2020

LESS team, *LESS: Linear Equivalence Signature Scheme (v2)*, 2025

CF-LESS

idea: proving that C and C lie in the same equivalence class reduces witness size

$F \leq M_n$ subgroup such that any $\varphi \in F$ is decomposed as $(\varphi_k, \varphi_{n-k}) \in M_k \times M_{n-k}$

any isometry ψ is the permutation of a $\varphi \in F$

$CF: F_q^{k\times(n-k)} \to F_q^{k\times(n-k)} \cup \{\perp\}$ canonical form **invariant over** F

$CF(A) = CF(Q_{\varphi_k} \cdot A \cdot Q_{\varphi_{n-k}})$ *for any $\varphi \in F$*

$$\begin{tikzcd} G\bar{Q} \arrow[r] & (\, I_k \mid A) \arrow[r] & (\, I_k \mid CF(A)) \end{tikzcd}$$

only commit $h(CF(A))$, but we need to save the map $\pi: G\bar{Q} \to RREF(G\bar{Q})$ for the response

Chou, **Persichetti**, **Santini**, *On Linear Equivalence, Canonical Forms, and Digital Signatures*, 2025

CF-LESS

idea: proving that C and C lie in the same equivalence class reduces witness size

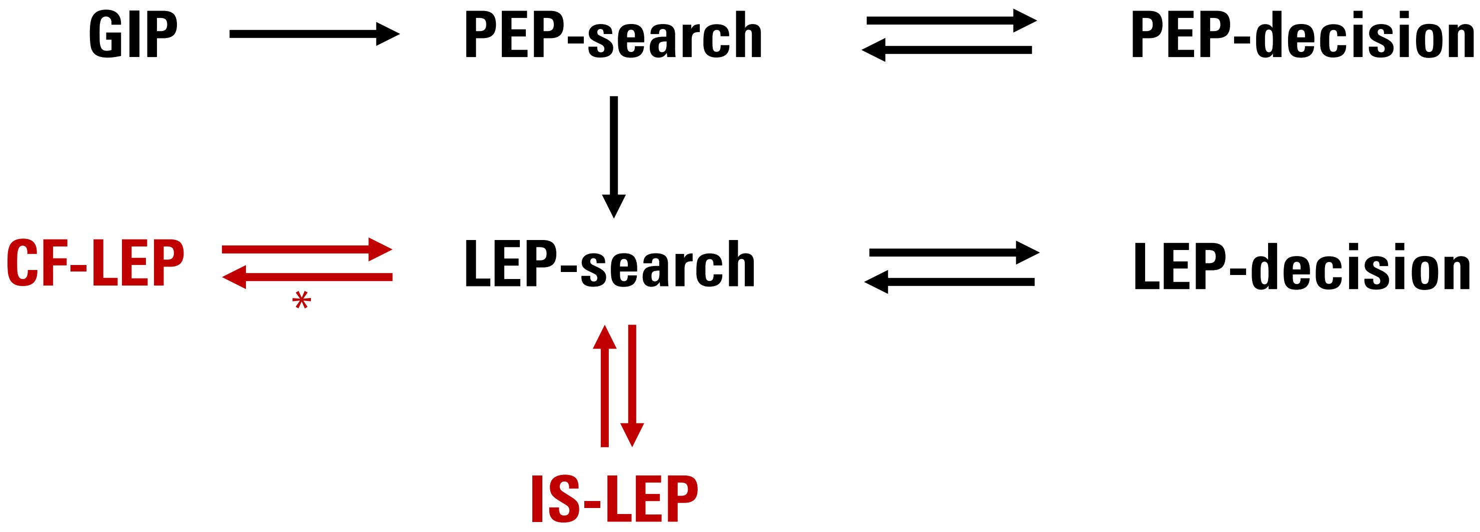
$$\begin{tikzcd}
\boldsymbol{G} \arrow[rr, dashed, "\textbf{witness}"] \arrow[dr, "\bar{\boldsymbol{Q}}_{\boldsymbol{i}}"'] & & \boldsymbol{G'} \arrow[dl, "\boldsymbol{Q^{-1}\bar{Q}_i}"] \\
& \boldsymbol{CF(A)} &
\end{tikzcd}$$

$$\begin{tikzcd}
G\bar{Q} \arrow[r] & (\, I_k \mid A) \arrow[r] & (\, I_k \mid CF(A))
\end{tikzcd}$$

only commit $h(CF(A))$, but we need to save the map $\pi: G\bar{Q} \rightarrow RREF(G\bar{Q})$ for the response

Chou, **Persichetti**, **Santini**, *On Linear Equivalence, Canonical Forms, and Digital Signatures*, 2025

CF-LESS



GIP
PEP-search
PEP-decision
CF-LEP
*
LEP-search
LEP-decision
IS-LEP

A → **B** A reduces to B

* if CF does not fail, i.e. $CF(*) \neq \perp$

TAKE AWAYS

- first code-based signature not using a SDP variation

TAKE AWAYS

- first code-based signature not using a SDP variation
- can adopt the framework of (non-commutative) group actions
  - identity-based signatures
  - ring signatures

Barenghi, **Biasse**, **Ngo**, **Persichetti**, **Santini**, *Advanced Signature Functionalities from the Code Equivalence Problem*, 2022

TAKE AWAYS

- first code-based signature not using a SDP variation
- can adopt the framework of (non-commutative) group actions
  - identity-based signatures
  - ring signatures
  - *threshold signatures??*

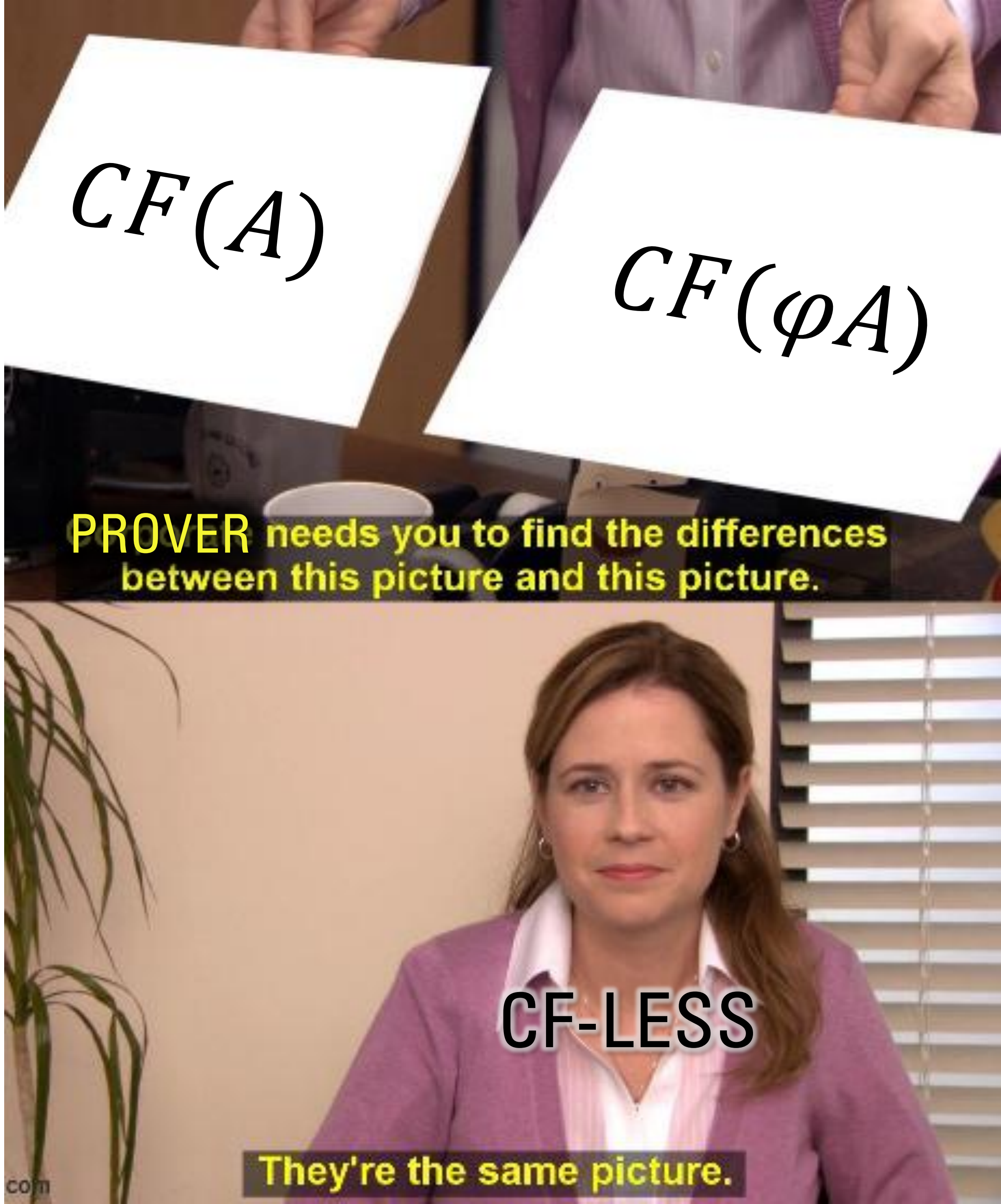
NIST Internal Report
NISTIR 8214C 2pd

NIST First Call for Multi-Party Threshold Schemes

Second Public Draft

Barenghi, **Biasse**, **Ngo**, **Persichetti**, **Santini**, *Advanced Signature Functionalities from the Code Equivalence Problem*, 2022
NIST, *First Call for Multi-Party Threshold Schemes (draft 2)*, 2025

THANKS!


$CF(A)$
$CF(\varphi A)$
PROVER needs you to find the differences between this picture and this picture.
CF-LESS
They're the same picture.