



UNIVERSITÀ
POLITECNICA
DELLE MARCHE

LEAST: Linear Equivalence Action Threshold Signature

Baldi Marco, **Battagliola Michele**¹, Borin Giacomo, Di Crescenzo Giovanni, El Mechri Rahmi, Meneghetti Alessio, Persichetti Edoardo, Santini Paolo, Floyd Zweyding

¹Università Politecnica delle Marche

NIST Workshop on Multi-Party Threshold Schemes 2026 - 29th January 2026

www.least-project.org

Contact us: info@least-project.org

Definition

Let X be set, and G a group. A (left) group action is a function:

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

such that

- $e \star x = x$ for all $x \in X$
- $g_1 \star (g_2 \star x) = (g_1 g_2) \star x$ for all $x \in X, g_1, g_2 \in G$.

We usually require the following properties:

- *Transitive*, for every $x_1, x_2 \in X$, there exists $g \in G$ such that $x_2 = g \star x_1$;
- *Free* if, for all $x \in X$, $g \star x = x$ implies $g = e$;
- *Regular*, if it is free and transitive.

A group action said to be *cryptographic* if it satisfy additional properties:

- *Efficiently evaluation*;
- *One way*: hard to invert.

Group Action Inverse Problem

Definition (Group Action Inverse Problem)

Let (X, G, \cdot) be a group action. Given x and y in X , find, if there exists, an element $g \in G$ such that $x = g \star y$.

Sometimes called Group Action Discrete Logarithm Problem (**gaDLOG**) or with names referring to the precise group action.

Definition

Let p be a prime and \mathbb{F}_p be the field with p elements. In our scheme, the set X will be the set of $[n, k]$ codes over \mathbb{F}_p , while G will be the group M_n of $n \times n$ monomial matrices with coefficients in \mathbb{F}_p . The action considered is the following

$$\begin{aligned} \star : M_n \times X &\longrightarrow X \\ (\mathbf{Q}, \mathbf{G}) &\longmapsto \text{SF}(\mathbf{G}\mathbf{Q}), \end{aligned}$$

where \mathbf{G} represents the generator matrix of the code and SF represents the reduction to standard form.

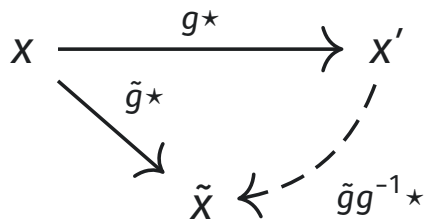
Advantages

- Solid Security Foundations
- Quantum-safety, Diversity
- Compatibility with LESS (almost)
- Compactness
- Non-Commutativity: less quantum attacks.

Disadvantages

- Limited number of parties
- Large public key
- Slow group action
- Round robin structure
- Non-Commutativity: worse performances

The Identification Protocol



Public key : x, x'	Responses to challenges
Secret Key : g	on 0 discloses \tilde{g}
Commitment : \tilde{x}	on 1 discloses $\tilde{g}g^{-1}$

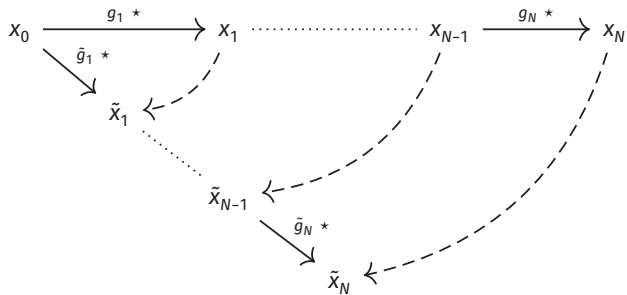
When \star is the Linear Code Equivalence this is the (textbook) LESS signature.

Overview

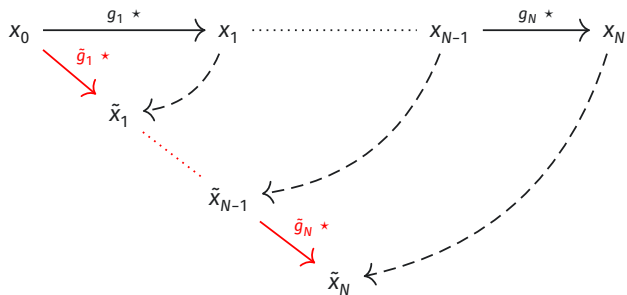
To obtain a full-threshold scheme for group actions we need to modify the signature schemes in a way that N users can collaborate in order to prove the mutual knowledge of a secret key.

- The secret key is splitted as $g = g_1 \cdots g_N$.
- The Verifier view of the protocol should remain unchanged.
- This scheme can be executed without a Trusted Third Party.

Protocol Sketch

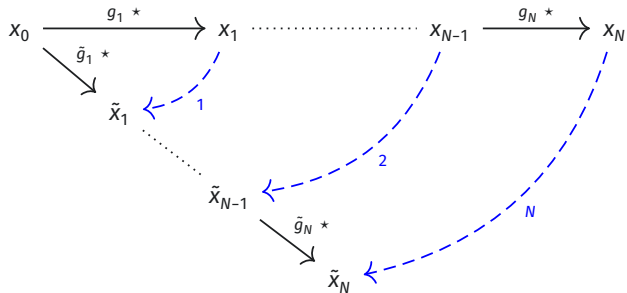


Protocol Sketch



The response when the challenge is 0 can be computed without round robin.

Protocol Sketch



The response when the challenge is 1 needs a round robin. The first party compute the first partial response and sends it to the second. The second use the first partial response, its own secret and its own randomness to compute the second and so on.

Theorem

Under the hardness of the group action inverse problem and in the random oracle model, the threshold signature scheme is existentially unforgeable under chosen-message attack.

Question

How can we do a multiplicative threshold-secret-sharing?

- Shamir secret sharing requires a field (two operations), while G is only a group (one operation).
- Moreover we cannot operate on the set elements in X directly.
- Finally, we cannot rely on commutativity

Replicated Secret Sharing

Let us consider I be the family of all the subsets of $\{P_1, \dots, P_N\}$ having exactly $N - T + 1$ elements and $m = |I|$ (thus $I = \{I_1, \dots, I_m\}$). We define $g = g_1 \cdot \dots \cdot g_l$, then we send g_i to P_j if and only if $P_j \in I_i$. It is possible to prove that any set of T party can reconstruct g , thus the previous protocol can be generalized. Unfortunately $m = \binom{N}{T-1}$ thus it is exponentially large.

Second Solution (less bad)

Recursive Secret Sharing

- if $t = n$ then split $g = g_1 \cdot \dots \cdot g_n$ and gives g_i to P_i
- if $t = 1$, gives g to all P_i .
- if $1 < t < n$ split in two sides P_l and P_r of size $c = \frac{n}{2}$ then for any ℓ
 $\max(t - c, 0) \leq \ell \leq \min(c, t)$ do
 - if $\ell = 0$ (resp. $\ell = t$), do a (t, n) secret sharing of g on P_l (resp. P_r).
 - otherwise g as $g_1 \cdot g_2$ and recursively do a (ℓ, c) sharing of g_1 on P_l and a $(t - \ell, c)$ sharing of g_2 on P_r .

The number of shares used to recover the secret key is not exponential as it was for the replicated secret sharing and it is always n . Still every user have multiple shares.

NO DECENTRALIZED VERSION (YET?)

Table 1: Performance and Parameters for LEASTSignature Schemes.

NIST Cat.	Parameter Set	Prot. Params			Keys	Rep.	pk size (B)	Signature size (B)
		n	k	q	s	τ		
1	LEAST-252-2	252	126	127	2	128	13940	4160
	LEAST-252-4				4	64	41788	2112
	LEAST-252-8				8	43	97484	1440
3	LEAST-400-2	400	200	127	2	192	35074	9696
	LEAST-400-4				4	96	105174	4896
5	LEAST-548-2	548	274	127	2	256	65793	17792
	LEAST-548-4				4	128	197315	8960

Table 2: Number and size of shares, both per users and in total.

NIST Cat.	N	T	Per User		Total	
			# Shares	Size (B)	# Shares	Size (B)
1	3	2	2	64	4	55696
	5	3	4	128	11	153164
	8	5	6	192	30	417720
3	3	2	2	100	4	140200
	5	3	4	200	11	385550
	8	5	6	300	30	417720
5	3	2	2	138	4	263044
	5	3	4	276	11	1051500
	8	5	6	414	30	1972830

- High-level Rust implementation of the LEASTthreshold protocol and the associated networking model. Since the primary computational bottlenecks lie in Gaussian elimination and canonical form computation, we adopt the same approach as LESS by introducing optimized implementations using AVX2, AVX512, and NEON instruction sets.
- Decentralized version of the recursive secret sharing.

Thank you for your attention!

Find us at



info@least-project.org



www.least-project.org

Acknowledgment of support

- the Italian Ministry of University and Research (MUR) under the PRIN PNRR 2022 program with project “Mathematical Primitives for Post Quantum Digital Signatures” (P2022J4HRR) funded by the European Union - Next Generation EU, Missione 4 “Istruzione e Ricerca” del Piano Nazionale di Ripresa e Resilienza
- the Italian Ministry of University and Research (MUR) under the PRIN PNRR 2022 program with project “POst quantum Identification and eNcryption primiTives: dEsign and Realization (POINTER)” (2022M2JLF2)
- the Italian Fund for Applied Science (FISA 2022), project “Quantum-safe cryptographic tools for the protection of national data and information technology assets” (QSAFEIT) - No. FISA 2022-00618 (CUP I33C24000520001)



**Finanziato
dall'Unione europea**
NextGenerationEU



**Ministero
dell'Università
e della Ricerca**