

On Canonical Liftings, Group Actions, and Linkable Ring Signatures



Alessandro Budroni



Giuseppe D'Alconzo



Leonardo Errati



Edoardo Persichetti

Politecnico di Torino
Department of Mathematical Sciences

NordCrypt26, 30 October 2026

Section 1

Signature Compression

Group Actions I

Let $(G, \circ)$ be a group and X a set. A *group action of G on X* is a map

$$\star : G \times X \rightarrow X$$

compatible with the group operation:

$$\text{id}_G \star x = x$$

$$g \star (h \star x) = (g \circ h) \star x$$

Group Actions I

Let $(G, \circ)$ be a group and X a set. A *group action of G on X* is a map

$$\star : G \times X \rightarrow X$$

compatible with the group operation:

$$\text{id}_G \star x = x$$

$$g \star (h \star x) = (g \circ h) \star x$$

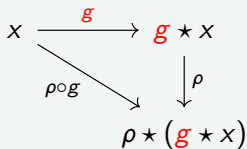


X = possible states of the cube

$$G = (Z_3^7 \times Z_2^{11}) \rtimes ((A_8 \times A_{12}) \rtimes Z_2).$$

Group Actions II

Remark: Sigma Protocol



$$\mathcal{R} = \{ \langle (x, y), g \rangle \mid x = g \star y \}$$

Definition: GAIP

Given $x, y \in X$, find $g \in G$ with $x = g \star y$.

Q1: can we compress responses?

Canonical Liftings I

A *canonical lifting* for a group action $(G, X, \star)$ is a tuple $(R, C, \text{Rep}, \text{Can}, \text{Lift})$ of sets and efficient maps such that this diagram commutes:

$$\begin{array}{ccc} G \times X & \xrightarrow{(\text{Rep}, \text{id})} & R \times X \\ \star \downarrow & & \downarrow \text{Lift} \\ X & \xrightarrow{\text{Can}} & C \end{array}$$

$$\begin{aligned} \text{Rep} &: G \rightarrow R \\ \text{Can} &: X \rightarrow C \\ \text{Lift} &: R \times X \rightarrow C \end{aligned}$$

Definition: Defining Property

$$\text{Can}(g \star x) = \text{Lift}(\text{Rep}(g), x)$$

Canonical Liftings II

CL is *effective* if it is efficient to

- 1 find g with given $r = \text{Rep}(g)$.
- 2 find g with $y = g \star x$ whenever $\text{Can}(x) = \text{Can}(y)$.

Definition: CLCP

Given $x, y \in X$, find $r, s \in R$ with $\text{Lift}(r, x) = \text{Lift}(s, y)$.

If CL is *effective*, $\text{GAIP} \simeq_{\text{PT}} \text{CLCP}$: compression without loss of hardness.
It abstracts / adds to known compression techniques.

Section 2

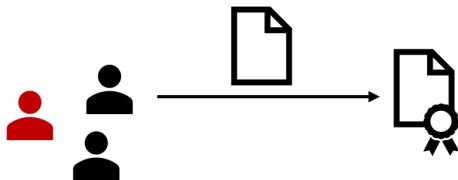
Advanced Signatures

Ring Signatures [RST01]

“*ring*” of public keys $R = \{pk_1, \dots, pk_n\}$

A *ring signature* allows a member of R to sign on behalf of R without revealing its index.

$RS = (\text{KeyGen}, \text{Sign}, \text{Verify})$

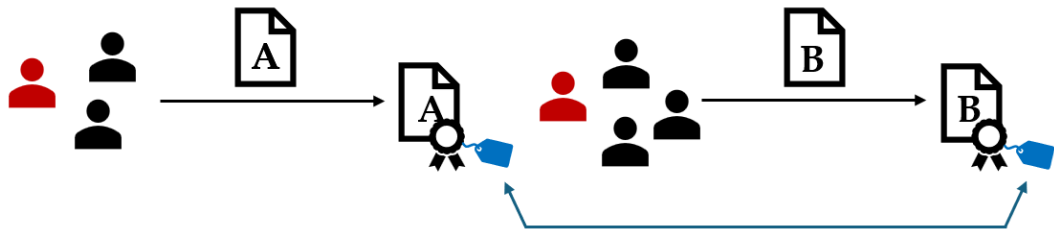


Linkable Ring Signatures [LWW04]

“*ring*” of public keys $R = \{pk_1, \dots, pk_n\}$

Linkable if it enables to verify whether two signatures were produced by the same sk_i .

LRS = (KeyGen, Sign, Verify, *Link*)



Linkable Ring Signatures [LWW04]

“*ring*” of public keys $R = \{pk_1, \dots, pk_n\}$

Linkable if it enables to verify whether two signatures were produced by the same sk_i .

$LRS = (\text{KeyGen}, \text{Sign}, \text{Verify}, \text{Link})$

Security properties:

Anonymity of signer.

Linkability of repeated uses of sk_i .

Non-frameability of an honest user.

Literature varies. We picked the strongest variants [BOA24].

Advanced Signatures via Canonical Liftings

base sigma protocol



signature

security problem: CLCP

slight modification: 5 to 8% faster LESS signing

OR sigma protocol



ring signature

security problem: CLCP

action commutativity is not required

Q2: Is it easy to add linkability?

Advanced Signatures via Canonical Liftings



OR-t sigma protocol



linkable ring signature

security problem:

non-classical

LRS from Group Actions [BKP20]

RS: for a commutative group action, apply Fiat-Shamir to a sigma protocol for

$$\mathcal{R}^{\text{OR}} = \left\{ \langle (x_1, \dots, x_N, y), w \rangle \in X^{N+1} \times W \mid \text{for some } i \in [N], (x_i, y, w) \in \mathcal{R} \right\}.$$

LRS: tag-key relation via *witness-reuse* from public pk, t.

$$\text{sk} = g \star \text{pk}, \quad \text{tg} = g \circ \text{t}$$

LRS from Group Actions [BKP20]

RS: for a commutative group action, apply Fiat-Shamir to a sigma protocol for

$$\mathcal{R}^{\text{OR}} = \left\{ \langle (x_1, \dots, x_N, y), w \rangle \in X^{N+1} \times W \mid \text{for some } i \in [N], (x_i, y, w) \in \mathcal{R} \right\}.$$

LRS: tag-key relation via *witness-reuse* from public pk , t .

$$\text{sk} = g \star \text{pk}, \quad \text{tg} = g \circ t$$

Non-commutative actions may not meet the security hypotheses of LRS [IGL26].

In codes & lattices, choosing $\star = \circ$ leads to key recovery [BCDD⁺24, BCDF25].

LRS from Canonical Liftings

Idea: tag-key relation is g, g' related by $\text{Rep}(g) = \text{Rep}(g')$.

Definition: Left-compatibility

- 1 $\text{Rep}(g) = \text{Rep}(h) \implies \text{Rep}(\rho \circ g) = \text{Rep}(\rho \circ h)$
- 2 given g , sampling uniform h such that $\text{Rep}(g) = \text{Rep}(h)$ is efficient

linkability

non-splitting
+ left-compatible

linkable anonimity

2-pseudorandom
+ left-compatible

non-frameability

frame one-way
+ left-compatible

CELeReS

CELeReS is the instantiation on code equivalence.

Scheme	Security	2^1	2^2	2^6	2^{10}	2^{12}	Assumption
CELeReS [BDEP26]	128 bit	26.7	27.8	32.3	36.7	39.0	OW, F-OW, 2-PR
	192 bit	69.2	72.3	85.1	97.8	104.2	
	256 bit	119.1	123.8	142.6	161.3	170.7	
Raptor [LAZ19]	100 bit	–	–	82.7	1301.9	5203.3	NTRU
Calamari [BKP20]	NIST-I	3.6	4.6	14.1	20.1	23.1	CSIDH-512
Falafel [BKP20]	NIST-I	33	34	36	39.3	41	MSIS, MLWE
DualRing-PRF [ZSL+24]	128 bit	–	–	45	64	–	Residue PRFs

Signature size (kB) for varying ring size. Comparison with post-quantum schemes adopting the strongest security definitions for LRS.

CELeReS-o

One possible tag compression technique: self-orthogonal tag matrices [[BMSS25](#)].
16.2 kB (of 26.7 kB) $\rightarrow$ 8.3 kB (of 18.9 kB)



faster key generation



smaller tags

Summary

What we showed

- This abstracts compression techniques
- They can build classical and (linkable) ring signatures

Open problems

- Different group actions?
- New techniques/functionalities?

<https://eprint.iacr.org/2026/1348>

References I

-  Alessandro Budroni, Jesús-Javier Chi-Domínguez, Giuseppe D'Alconzo, Antonio J Di Scala, and Mukul Kulkarni, *Don't use it twice! solving relaxed linear equivalence problems*, International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2024, pp. 35–65.
-  Alessandro Budroni, Jesús-Javier Chi-Domínguez, and Ermes Franch, *Don't use it twice: Reloaded! on the lattice isomorphism group action*, IACR Communications in Cryptology 2 (2025), no. 2.
-  Alessandro Budroni, Giuseppe D'Alconzo, Leonardo Errati, and Edoardo Persichetti, *On canonical liftings, group actions, and linkable ring signatures*, Cryptology ePrint Archive, Paper 2026/1348, 2026.

References II

-  Ward Beullens, Shuichi Katsumata, and Federico Pintore, *Calamari and falaf: logarithmic (linkable) ring signatures from isogenies and lattices*, International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2020, pp. 464–492.
-  Marco Baldi, Rahmi El Mechri, Paolo Santini, and Riccardo Schiavoni, *On the representation of self-orthogonal codes and applications to cryptography*, Cryptology ePrint Archive, Paper 2025/2279, 2025.
-  Xavier Bultel and Charles Olivier-Anclin, *On the anonymity of linkable ring signatures*, International Conference on Cryptology and Network Security, Springer, 2024, pp. 212–235.
-  Dung Hoang Duong, Xuan Thanh Khuc, Youming Qiao, Willy Susilo, and Chuanqi Zhang, *Blind signatures from cryptographic group actions*, Cryptology ePrint Archive, Paper 2025/397, 2025.

References III

-  Iñigo Diaz Iribarnegaray, Václav Gregor, and Florian Lécu Leal, *A note on the unsuitability of LIGA for linkable ring signatures: The perils of non-commutativity*, Cryptology ePrint Archive, Paper 2026/671, 2026.
-  Xingye Lu, Man Ho Au, and Zhenfei Zhang, *Raptor: a practical lattice-based (linkable) ring signature*, International Conference on Applied Cryptography and Network Security, Springer, 2019, pp. 110–130.
-  Joseph K Liu, Victor K Wei, and Duncan S Wong, *Linkable spontaneous anonymous group signature for ad hoc groups*, Australasian conference on information security and privacy, Springer, 2004, pp. 325–335.
-  Ronald L Rivest, Adi Shamir, and Yael Tauman, *How to leak a secret*, International conference on the theory and application of cryptology and information security, Springer, 2001, pp. 552–565.

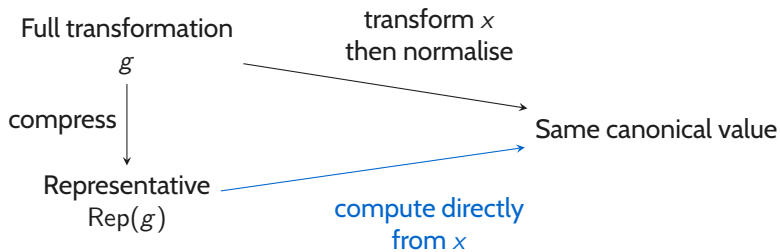
References IV

-  Xinyu Zhang, Ron Steinfeld, Joseph K Liu, Muhammed F Esgin, Dongxi Liu, and Sushmita Ruj, *Dualring-prf: Post-quantum (linkable) ring signatures from legendre and power residue prfs*, Australasian conference on information security and privacy, Springer, 2024, pp. 124–143.

EXTRA SLIDES

open in case of emergency

Canonical Liftings: enchore



Defining Property

$$\text{Can}(g \star x) = \text{Lift}(\text{Rep}(g), x)$$

Faster LESS signing

Extra payoff from canonical liftings

Instead of sampling a full ephemeral transformation, sample its representative directly.
This requires a well-defined efficient operation

$$r \odot g = \text{Rep}(g_r \circ g), \quad \text{Rep}(g_r) = r,$$

and sampling representatives with the correct induced distribution.

5 to 8% improvement in LESS signing time.

Which lifting for CELeReS?

The canonical form used in LESS is not left-compatible.
Instead, we adapt existing constructions.

$$X = \mathbb{F}_q^{k \times n}, \quad G = \text{Mon}_n(\mathbb{F}_q)$$

$$C = \text{CF}(X) \text{ [DKQ}^+25], \quad R = \text{Perm}_n(\mathbb{F}_q)$$

$$\begin{array}{ccc} G \times X & \xrightarrow{(\text{Rep}, \text{id})} & R \times X \\ \star \downarrow & & \downarrow \text{Lift} \\ X & \xrightarrow{\text{Can}} & C \end{array}$$

$$\begin{aligned} \text{Rep} &: \mathbf{PD} \mapsto \mathbf{P} \\ \text{Can} &: \mathbf{M} \mapsto \text{CF}(\mathbf{M}) \\ \text{Lift} &: (\mathbf{M}, \mathbf{P}) \mapsto \text{CF}(\mathbf{MP}) \end{aligned}$$

Security Properties of LRS

linkability

Find α in $\text{MAut}(\mathbf{G}) \setminus \text{MAut}(\mathbf{T})$.

If $\mathbf{G}, \mathbf{T}$ are random, they are trivial with overwhelming probability.

*linkable
anonymity*

Distinguish between
 $(\text{RREF}(\mathbf{GQ}), \text{RREF}(\mathbf{TQ}'))$
 $(\text{RREF}(\mathbf{GQ}_0), \text{RREF}(\mathbf{GQ}_1))$

A 2-sample version of
2-pseudorandomness for the
quotient action by $\text{Perm}_n(\mathbb{F}_q)$.
The best attacks are those on LEP.

non-frameability

(If $\text{MAut}(\mathbf{T})$ is trivial)
Given $(\mathbf{G}, \mathbf{G}')$ and $(\mathbf{T}, \mathbf{T}')$ pairs
of linear equivalent codes
under the same $\mathbf{P}$, find $\mathbf{P}$.

The best attacks are those on LEP.

LRS from Canonical Liftings: CELeReS

Code Equivalence Linkable Ring Signature

The lifting of LESS is not left-compatible. Our lifting has $\text{Rep}(Q) = P$.

Idea: $Q = PD, Q' = PD'$ related by P

Left-compatibility

- 1 if Q, Q' share permutation, so do MQ, MQ'
- 2 sampling uniform Q'' with same permutation is efficient

linkability

if $\text{Aut}(\mathbf{G}), \text{Aut}(\mathbf{T}) = \{1\}$,
it holds unconditionally

linkable anonymity

best known attacks are
those on LEP

non-frameability

best known attacks are
those on LEP

Performance of CELeReS-o

Security	2^1	2^2	2^6	2^{10}	2^{12}
128 bit	18.9	19.9	24.5	28.9	31.2
192 bit	50.8	54.0	66.7	79.5	85.9
256 bit	85.4	90.1	108.8	127.6	136.9