Canonical Liftings for Group Actions

Beyond Ring Signatures?

From *On Canonical Liftings, Group Actions, and Linkable Ring Signatures*
A. Budroni, G. D'Alconzo, L. Errati, E. Persichetti

Politecnico di Torino
Department of Mathematical Sciences

ALPEC summer school, 2026-09-03, Trento

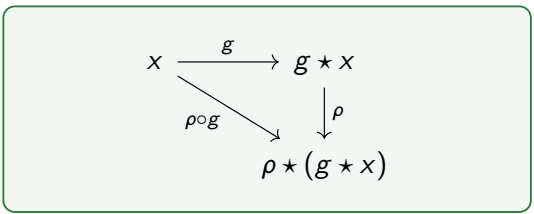
Group Actions

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

$$\star : G \times X \to X$$

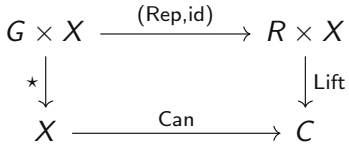
compatible with the group operation:

$$\mathrm{id}_G \star x = x$$
$$g \star (h \star x) = (g \circ h) \star x$$



Canonical Liftings I

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



$$\mathsf{Rep} : G \to R$$
$$\mathsf{Can} : X \to C$$
$$\mathsf{Lift} : R \times X \to C$$

Defining Property

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

Canonical Liftings II

A canonical lifting is *effective* if

1. it is efficient to find a g with given representative r
2. if $\mathsf{Can}(x) = \mathsf{Can}(y)$, it is efficient to find g with $y = g \star x$.

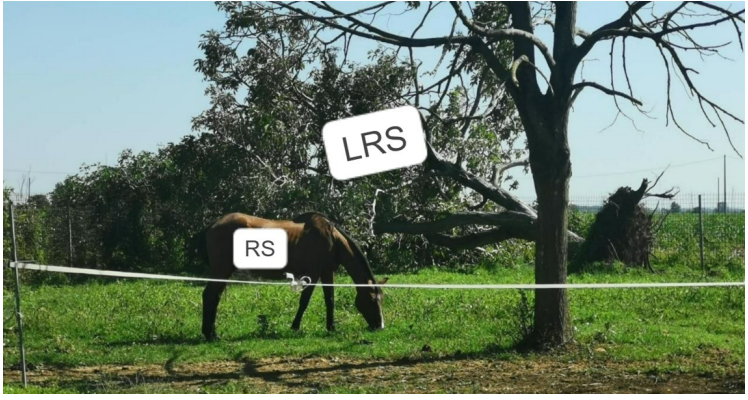
CLCP

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

If a canonical lifting is *effective*, GAIP and CLCP are PPT-equivalent.

Advanced Signatures via Canonical Liftings

Signature: Fiat–Shamir on the sigma protocol. Security problem: CLCP.
RS: Fiat–Shamir on the OR sigma protocol. Security problem: CLCP.
LRS: Fiat–Shamir on the OR-t sigma protocol. Security problem: *non-classical*.

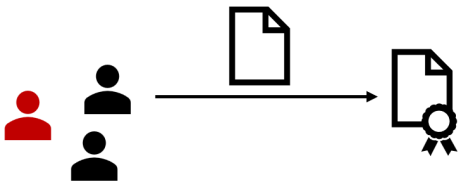


Ring Signatures [RST01]

ring of public keys $\mathcal{R} = (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$

A *ring signature* allows an user to sign on behalf of $\mathcal{R}$ without revealing its identity.

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

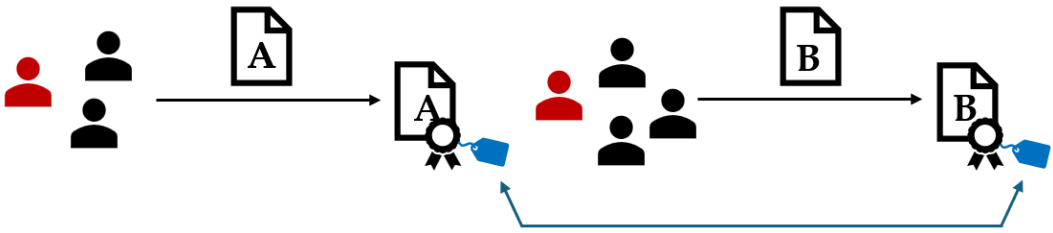


Linkable Ring Signatures [LWW04]

ring of public keys $\mathcal{R} = (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$

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

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



LRS from Group Actions [BKP20]

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

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

LRS: tag-key relation via witness-reuse.

With LEP, witness-reuse leads to key recovery attacks [BCDD+24].

$$\mathrm{pk}_i = \boldsymbol{QG}, \qquad \mathrm{tg}_i = \boldsymbol{Q}^{-1}\boldsymbol{G}$$

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

LRS from Canonical Liftings

The case of LEP

Idea: tag-key relation is g, g' related by $\mathrm{Rep}(g) = \mathrm{Rep}(g')$.
LEP: $\boldsymbol{Q} = \boldsymbol{P}\boldsymbol{D}, \boldsymbol{Q}' = \boldsymbol{P}\boldsymbol{D}'$ related by $\boldsymbol{P}$: $\mathrm{pk}_i = \boldsymbol{Q}_i\boldsymbol{G}$, $\mathrm{tg}_i = \boldsymbol{Q}'_i\boldsymbol{T}$

Left-compatibility

1. if $\boldsymbol{Q}, \boldsymbol{Q}'$ share permutation, so do $\boldsymbol{M}\boldsymbol{Q}, \boldsymbol{M}\boldsymbol{Q}'$
2. sampling uniform $\boldsymbol{Q}''$ with same permutation is efficient

linkability

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

linkable anonimity

best known attacks are those on LEP

non-frameability

best known attacks are those on LEP

Summary

What we showed

- Canonical liftings abstract compression techniques
- They can build classical and (linkable) ring signatures

Open problems

- Different group actions
- New techniques from liftings
- For code-based LRS: tag compression techniques

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, Giuseppe D'Alconzo, Leonardo Errati, and Edoardo Persichetti, *On canonical liftings, group actions, and linkable ring signatures*, Cryptology ePrint Archive, Paper 2026/1348, 2026.
- Ward Beullens, Shuichi Katsumata, and Federico Pintore, *Calamari and falafl: 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.

References II

- 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.
- Iñigo Diaz Iribarnegaray, Václav Gregor, and Florian L'écu 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.

References III

- 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.
- 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

LRS from Canonical Liftings

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

Left-compatibility

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

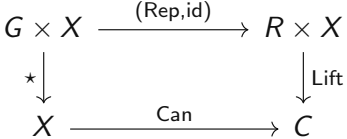
linkability	*linkable anonimity*	*non-frameability*
non-splitting + left-compatible	**2-pseudorandom** + left-compatible	**frame one-way** + left-compatible

Which lifting for CELeReS?

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

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

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



$$\mathrm{Rep} : \boldsymbol{PD} \mapsto \boldsymbol{P}$$
$$\mathrm{Can} : \boldsymbol{M} \mapsto \mathrm{CF}(\boldsymbol{M})$$
$$\mathrm{Lift} : (\boldsymbol{M}, \boldsymbol{P}) \mapsto \mathrm{CF}(\boldsymbol{MP})$$

Security Properties of LRS

linkability

Find α in $\mathrm{MAut}(\boldsymbol{G}) \setminus \mathrm{MAut}(\boldsymbol{T})$.

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

linkable anonimity

Distinguish between

$(\mathrm{RREF}(\boldsymbol{GQ}), \mathrm{RREF}(\boldsymbol{TQ}'))$

$(\mathrm{RREF}(\boldsymbol{GQ}_0), \mathrm{RREF}(\boldsymbol{GQ}_1))$

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

non-frameability

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

The best attacks are those on LEP.

Performance of CELeReS

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
Falafl [BKP20]	NIST-I	33	34	36	39.3	41	MSIS, MLWE
DualRing-PRF [ZSL+24]	128 bit	–	–	45	64	–	Residue PRFs

Scheme	Ring size	KeyGen	Sign	Verify
CELeReS	2^1	$1.32\,M\ /\ 4.5 \times 10^{-4}\,s$	$421\,M\ /\ 0.141\,s$	$397\,M\ /\ 0.137\,s$
	2^3		$2419\,M\ /\ 0.806\,s$	$2035\,M\ /\ 0.678\,s$
	2^6		$9300\,M\ /\ 3.090\,s$	$7865\,M\ /\ 2.631\,s$

CELeReS-o (I)

Variant with self-orthogonal tag matrices.

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

Ring size	KeyGen	Sign	Verify
2^1	55.0 M/0.018 s	511 M/0.171 s	477 M/0.159 s
2^3		2508 M/0.834 s	2090 M/0.697 s
2^6		9836 M/3.255 s	7647 M/2.543 s

CELeReS-o (II)


GLUTEN FREE
GEFEN
Choco
CELeReS
MADE WITH REAL
COCOA


GEFEN
REAL COCOA-FLAVORED
CELeReS-O'S
KOSHER FOR PASSOVER
with self-orthogonal tags!
CHOLESTEROL FREE
FAT FREE