LoTRS: Practical Post-Quantum Structured Threshold Ring Signatures from Lattices

TCPT2: NIST Event for Threshold Call Preview Talks #2

2026-07-08

Muhammed F. Esgin [1], **Nikai Jagganath** [1,2], **Dongxi Liu** [2], **Markku-Juhani O. Saarinen** [3], **Amin Sakzad** [1], **Ron Steinfeld** [1]

Monash University [1], CSIRO's Data61 [2], Tampere University [3]
nikai.jagganath@monash.edu

Outline

- Motivation:
  - Threshold Ring Signatures in a post-quantum setting
  - Structured Threshold Ring Signatures: What is relaxed and why?
  - Applications
  - Ad-hoc Threshold Selection
- State-of-the-art comparison
- LoTRS construction: Multisignature layer [Che23] + Selection-hiding layer [ESS+19]
- Security proof map and assumptions
- Concrete parameters & Implementation

Motivation

Threshold Ring Signatures (TRS)

Introduced by Bresson et al. [BSS02] to strengthen both

- Ring signatures
- Threshold signatures

Definition. TRS

A classic TRS lets any T signers among N produce one signature such that

- at least T distinct keys signed (validity)
- which T keys signed is hidden (anonymity)

- Signer-set anonymity $1/\binom{N}{T}$
- Per-signer anonymity T/N

Full anonymity over every possible $\binom{N}{T}$ signer-set $\rightarrow$ T-out-of-N (expensive) ZK proof.

Structured Threshold Ring Signatures (sTRS)

Definition. sTRS

$$\text{sTRS} := \underline{\text{s}}\text{tructured ring} + \underline{\text{TRS}}$$

- Public ring instance + descriptor: (R, Ψ)
- Public admissible signer-set family:

$$\mathcal{F}_\Psi(R) \subseteq_\Psi \{U \subseteq R : |U| = T\}$$

- Anonymity only between admissible signer sets.

Example:

Table $PK := (R, \Psi)$ of size $M := T \times N$
$\mathcal{F}_\Psi(R) := \{\text{columns of table}\}$

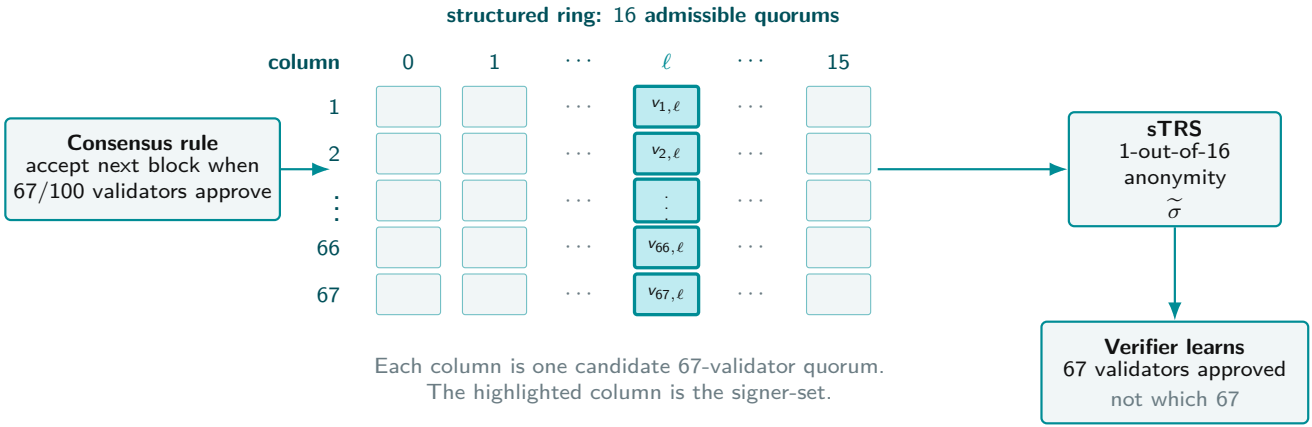
The Anonymity Tradeoff:

- Signer-set anonymity $1/N$
- Per-signer anonymity $1/N$

$t_{0,0}$	$t_{0,1}$	$t_{0,\ell}$	$t_{0,3}$	$t_{0,4}$
$t_{1,0}$	$t_{1,1}$	$t_{1,\ell}$	$t_{1,3}$	$t_{1,4}$
$t_{2,0}$	$t_{2,1}$	$t_{2,\ell}$	$t_{2,3}$	$t_{2,4}$
$t_{3,0}$	$t_{3,1}$	$t_{3,\ell}$	$t_{3,3}$	$t_{3,4}$

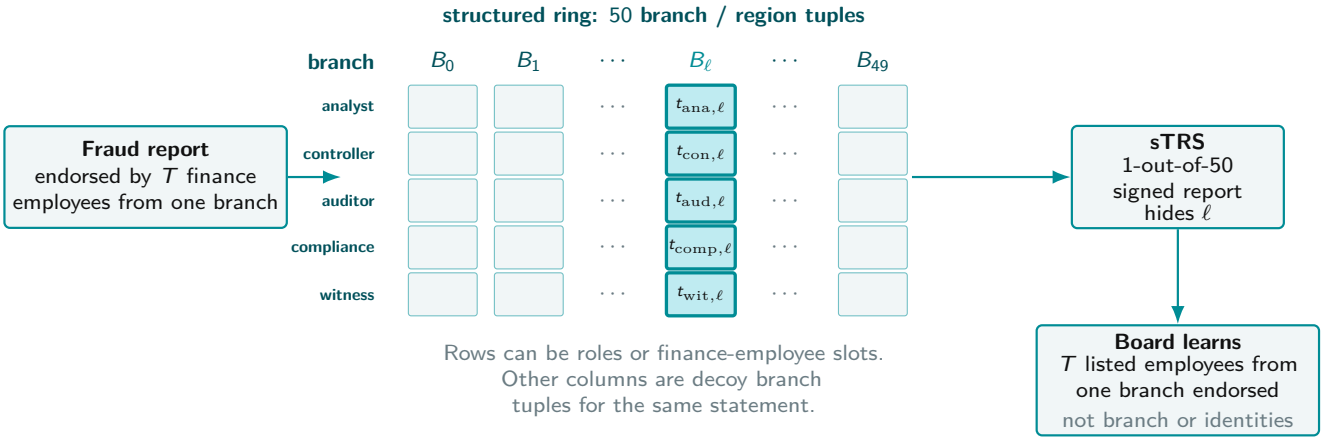
hidden admissible column

Application: Blockchain Supermajority Voting



Anonymity tradeoff: signer-set anonymity $1/16$ rather than $1/\binom{100}{67}$;
sTRS hides one structured quorum instead of proving a general 67-out-of-100 subset.

Application: Whistleblowing



Privacy tradeoff: signer-set anonymity 1/50 rather than combinatorial anonymity over all cross-branch T-subsets; sTRS proves one hidden branch tuple instead of a general T-out-of-M subset.

Ad-hoc Threshold Selection

Dynamic keys

- Ring $\rightarrow$ each signer has own secret key
- No distributed secret key $\rightarrow$ enables dynamic ring sizes

Dynamic ring sizes

- Structured ring:

$$\mathsf{PK} = (R, \Psi), \qquad |\mathsf{PK}| = M = T \cdot N.$$

- Only the T real signers in column ℓ need to be active.
- If a signer drops out:
  - sign with $T - 1$ parties using a new $(T - 1) \times N$ table, if policy allows;
  - or replace the inactive signer and restructure PK.

State-of-the-art comparison

Comparison

Table: Comparison of our sTRS construction with other TRS schemes for ($N = 100$, $T = N/2$). Note that the full ring size in LoTRS is $M = N \cdot T$. See 'Comparing TRS and sTRS anonymity' in text for a discussion on the anonymity tradeoff between TRS and sTRS in https://ia.cr/2026/974.

Work	Asymptotic Sig. Size	Analytic Sig. Size	Security
⋆ Melchor et al.[MCGL11]	$O(N)$	2 MB	80 bit
⋆ Cayrel et al.[CLRS10]	$O(N)$	47 MB	111 bit
† Cayrel et al.[CLRS10]	$O(N)$	45 MB	111 bit
† Bettaieb et al.[BS13]	$O(NT)$	13 MB	111 bit
† GC-TRS(LTRS) [LWW+25]	$O(N)$	–	–
† GC-TRS(CTRS) [LWW+25]	$O(T \log N)$	–	–
† RFTRS [WZZ+25]	$O(N)$	168 KB	120 bit
† LastRings [JHT25]	$O(\log(NT))$	122 KB	128 bit
† LoTRS (**This work**)	polylog(N, T)	36 KB	128 bit
$*(N = 32, T = N/2)$		23 KB	128 bit
$*(N = 16, T = N/2)$		20 KB	128 bit

Key: ⋆ Code-based, † Lattice-based, $*$ smaller N estimates for LoTRS. Sizes are analytic estimates from each work's parameter selection.

LoTRS Construction

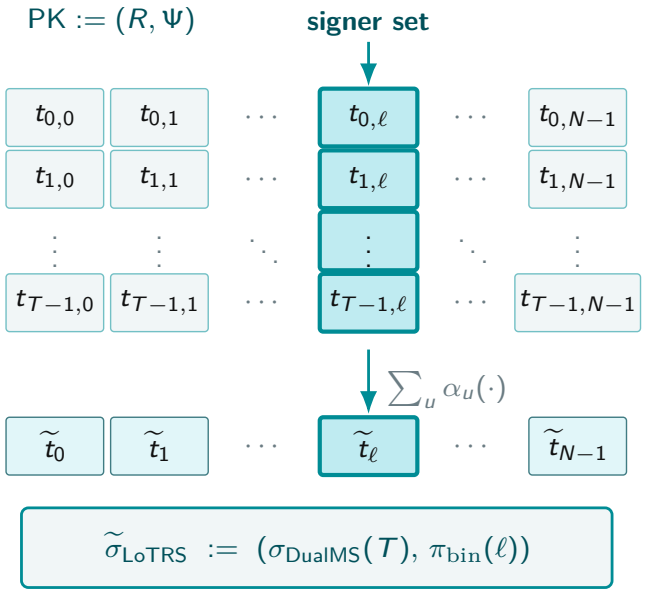
LoTRS: Our sTRS at a glance

T real signers in hidden column ℓ

Multisignature aggregated signing relation

1-out-of-N proof hides which aggregate column is valid

LoTRS signature



- Threshold authenticity comes from the DualMS [Che23] multisignature layer
- Anonymity comes from hiding the aggregate column using 1-out-of-N proof [ESS+19]

"Lord of The RingS: One Ring (Proof) to Rule them all"

Compatibility trick

Naive composition issue

A 1-out-of-N proof might select one aggregate, while the multisignature equation verifies against another combination of public keys.

LoTRS modifies the DualMS commitments and final responses for compatibility with 1-out-of-N proof:

$$w_{u,j} = \bar{A} y_{u,j} + \bar{B} r_{u,j} + \alpha_u \sum_i p_{i,j} t_{u,i},$$

$$z_u = x^\kappa \alpha_u s_u - \sum_{j=0}^{\kappa-1} x^j y_{u,j}.$$

These terms force the anonymity layer and signing layer to agree on the same hidden column.

KGen

Run DualMS KGen:

- Each signer u has public key $\quad pk_u : t_u := \bar{A}s_u \quad \in \mathcal{R}_q^k := \mathbb{Z}_q/(X^d + 1)$

KAgg

- Derive row aggregation coefficients

$$\alpha_u = H_{\text{agg}}(\text{PK}, u).$$

- Aggregate each candidate column:

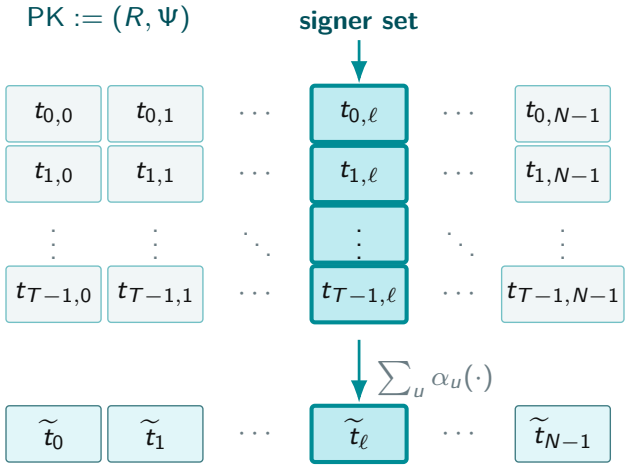
$$\widetilde{t}_i = \sum_{u=0}^{T-1} \alpha_u t_{u,i}.$$

Verifier's view

The proof should convince the verifier that the signing relation holds for one hidden $\widetilde{t}_\ell$, without revealing ℓ.

Pre-signing

- T members from $P = \{pk_0, pk_1, pk_2, \ldots\}$ agree to sign.
- Arrange public keys as a $T \times N$ table:
  - signer public keys $t_{u,\ell}$ in column ℓ
  - $T \times (N-1)$ decoys from P



- Signers share common secret seed ρ via authenticated channel.

$\mathbf{Sign}_1(\mu, \ell, \mathsf{PK})$

Analogous to DualMS, each signer u:

- Derives 'dual' public matrix: $B := H_{\mathrm{com}}(\mathsf{PK}, \mu)$
- Samples randomness: $y_{u,j} \xleftarrow{\$} D_y, \qquad r_{u,j} \xleftarrow{\$} D_r$

Computes j terms:

$$\bar{A}y_{u,j} + \bar{B}r_{u,j}$$

For the 1-out-of-N compatibility, each signer u:

- Derives masking terms: $a_{j,i} := \mathsf{Expand}(\rho, D_a)$
- Computes coefficients: $p_{i,j} \leftarrow (a_{j,i}, \ell)$

Computes sum over row u:

$$\sum_{i=0}^{N-1} p_{i,j}\alpha_u t_{u,i}$$

Sends j commitments to other signers:

$$w_{u,j} = \bar{A}y_{u,j} + \bar{B}r_{u,j} \; + \alpha_u \sum_{i=0}^{N-1} p_{i,j} t_{u,i} \,,$$

Forms j aggregated commitments: $\widetilde{w}_j := \sum_{u=0}^{T-1} w_{u,j}$

Selector proof intuition

Write $N = \beta^\kappa$ and encode the hidden signer column index as

$$\ell = (\ell_0, \ldots, \ell_{\kappa-1}) \quad \text{in base } \beta.$$

The binary proof hides one-hot selector vectors $b_{\ell_j,i}$ and reveals masked values

$$f_{j,i} = a^1_{j,i} + x b_{\ell_j,i}.$$

For each column, write $i = (i_0, \ldots, i_{\kappa-1})$,

$$\sum_{i=0}^{N-1} \left(\prod_{j=0}^{\kappa-1} f_{j,i_j} \right) \tilde{t}_i = x^\kappa \tilde{t}_\ell + \sum_{j=0}^{\kappa-1} x^j \sum_{i=0}^{N-1} p_{i,j} \tilde{t}_i.$$

So, algorithm $\mathsf{Sign}_{\mathsf{bin}}$ forms commitments and responses to guarantee this condition.

Outputs $\pi := (x, \mathbf{f}, \ldots, \widetilde{w}_1, \ldots, \widetilde{w}_{\kappa-1})$ where challenge $x := H(\mu, \widetilde{w}_0, \ldots, \widetilde{w}_{\kappa-1}, \ldots, \mathsf{PK})$.

[1] Same $a_{j,i}$'s derived from ρ.

$\mathbf{Sign}_2(\mu, \ell, \mathsf{PK})$

Each signer u computes:

$$z_u = x^{\kappa} \alpha_u s_u - \sum_{j=0}^{\kappa-1} x^j y_{u,j}.$$

$$r_u = - \sum_{j=0}^{\kappa-1} x^j r_{u,j}$$

SAgg

- Check $\pi'_u = \pi_u$, for all signers
- Aggregate responses

$$\tilde{z} = \sum_{u=0}^{T-1} z_u, \qquad \tilde{r} = \sum_{u=0}^{T-1} r_u$$

Signature

$$\tilde{\sigma}_{\mathsf{LoTRS}} = \left((\tilde{z}, \tilde{r}), \pi := (x, \mathbf{f}, \ldots, \widetilde{w}_1, \ldots, \widetilde{w}_{\kappa-1}) \right)$$

Verification

Given $\tilde{\sigma}_{\mathsf{LoTRS}} = \big((\tilde{z}, \tilde{r}), \pi := (x, \mathbf{f}), \ldots\big)$, compute

$$
\begin{aligned}
\widehat{w}_0 &= \sum_{i=0}^{N-1} \Big(\prod_{j=0}^{\kappa-1} f_{j,i_j} \Big) \tilde{t}_i - (\bar{A}\tilde{z} + \bar{B}\tilde{r}) - \sum_{j=1}^{\kappa-1} x^j \, \widetilde{w}_j \\
&= \ldots \\
&= x^{\kappa} \tilde{t}_\ell + \qquad\qquad - x^{\kappa} \tilde{t}_\ell + \qquad\qquad \\
&= \ldots \\
&= \sum_{j=0}^{\kappa-1} x^j \sum_{u=0}^{T-1} \Big(\bar{A} y_{u,j} + \bar{B} r_{u,j} + \alpha_u \sum_{i=0}^{N-1} p_{i,j} t_{u,i} \Big) - \sum_{j=1}^{\kappa-1} x^j \sum_{u=0}^{T-1} w_{u,j}
\end{aligned}
$$

Need $\widehat{w}_0 = \widetilde{w}_0$.

Check

$$
H(\mu, \widetilde{w}_0, \ldots, \widetilde{w}_{\kappa-1}, \ldots, \mathsf{PK}) := \quad x \stackrel{?}{=} x' \quad := H(\mu, \widehat{w}_0, \ldots, \widetilde{w}_{\kappa-1}, \ldots, \mathsf{PK})
$$

Security and Implementation

Security Proof Summary

Unforgeability

Mostly analogous to DualMS proofs

$$\begin{aligned} \text{UF-CMA} &\Rightarrow \text{sel-UF-CMA} \\ &\Rightarrow \text{sel-UF-KOA} + \text{MLWE} \\ &\Rightarrow \text{MSIS} + \text{MLWE} \end{aligned}$$

Except for final reduction due to x^κ term $\rightarrow$ degree κ-extraction needed.

- Tree-Finder [DPLS19]
- Vandermonde "one-shot" technique [ESLL19]

Anonymity

- Hybrid argument between admissible signer-set columns S_0, S_1.
- Assumptions:
  - MLWE
  - Simulated transcript indistinguishability
  - Rejection sampling indistinguishability

Parameters & Implementation

κ	d	$q = \hat{q}$
1	128	$\approx 2^{38}$

N	T	Signature	Sign / Verify
32	16	25.0 KiB	149 ms / 43 ms
100	50	35.8 KiB	789 ms / 250 ms

- Python reference implementation for test vectors.
- Rust implementation for performance benchmarking.

  Benchmarks on a laptop with an AMD Ryzen AI 9 HX 370, 32 GB RAM, Debian Linux, Rust release build, and rayon parallelism across 24 hardware threads. Sign/verify times are averages over 100 signatures per cell.
- Full pipeline: Setup, Key generation, Aggregation, Signing, Verification and Serialization.

Takeaways

- Introduce LoTRS; a structured TRS
- Post-Quantum; Assumes hardness of MLWE and MSIS.
- Threshold authenticity is enforced by the multisignature layer.
- A 1-out-of-N proof hides (anonymity) the selected signer column.
- Main technical point: Making these two layers algebraically compatible.

N	T	Signature	Sign / Verify
100	50	35.8 KiB	789 ms / 250 ms

Email: nikai.jagganath@monash.edu

https://ia.cr/2026/974

References

Slim Bettaieb and Julien Schrek.
Improved lattice-based threshold ring signature scheme.
In *International Workshop on Post-Quantum Cryptography*, pages 34–51. Springer, 2013.

Emmanuel Bresson, Jacques Stern, and Michael Szydlo.
Threshold ring signatures and applications to ad-hoc groups.
In *Annual International Cryptology Conference*, pages 465–480. Springer, 2002.

Yanbo Chen.
DualMS: Efficient lattice-based two-round multi-signature with trapdoor-free simulation.
In *Advances in Cryptology – CRYPTO 2023*, pages 716–747. Springer Nature Switzerland, 2023.

Pierre-Louis Cayrel, Richard Lindner, Markus Rückert, and Rosemberg Silva.
A lattice-based threshold ring signature scheme.
In *International Conference on Cryptology and Information Security in Latin America*, pages 255–272. Springer, 2010.

Rafaël Del Pino, Vadim Lyubashevsky, and Gregor Seiler.
Short discrete log proofs for FHE and ring-LWE ciphertexts.
In *IACR International Workshop on Public Key Cryptography*, pages 344–373. Springer, 2019.

Muhammed F Esgin, Ron Steinfeld, Joseph K Liu, and Dongxi Liu.
Lattice-based zero-knowledge proofs: New techniques for shorter and faster constructions and applications.
In *Annual International Cryptology Conference*, pages 115–146. Springer, 2019.

Muhammed F Esgin, Ron Steinfeld, Amin Sakzad, Joseph K Liu, and Dongxi Liu.
Short lattice-based one-out-of-many proofs and applications to ring signatures.
In *International Conference on Applied Cryptography and Network Security*, pages 67–88. Springer, 2019.