

Thimza: Stateless Threshold Signatures at Optimal Bandwidth

(t, n)-Threshold Signature over Module Lattices with $O(1)$ Signer State

Navid Abapour
Surrey Centre for Cyber Security
University of Surrey, UK

Hamidreza Amini Khorasgani
Department of Computer Science
Purdue University, US

NIST Event for Threshold Call Talks #3, TCPT3 ▪ October 6, 2026

thimza@googlegroups.com

Outline

1. Introduction
2. Limitations of the Family and Security Model
3. Our `Thimza` Construction
4. Security Analysis
5. Parameters, Performance and the Standardization Profile
6. Conclusion

Overview of Thimza and Claims

Thimza[1] is a (t, n)-threshold signatur over module lattices whose output is a Raccoon [dPKPR24] signature, so it is accepted by the unmodified verifier of the single signer scheme.

1. Statelessness Settled
No session identifiers registry is needed. One token per session, consumed once and erased at once, is sufficient and minimal.

2. Network Model
No message authentication codes and no signer set at commit time, at *unchanged* lattice parameters.

3. Bandwidth and Time
16 736 bytes per signer at $t = 1024$, exactly independent of t, and the fastest signing in the family.

4. Machine-checked Proof
Unforgeability, interchangeability and the impossibility result are modeled in `EasyCrypt` [BDG+14].

at $t = 1024$, level I	**Thimza**	TRaccoon [dPKM+24]	TalonG [GTJ+26]	EKT [EKT24]	Ringtail [BKL+25]
communication per signer (B)	**16 736**	57 184	46 848	278 400	629 248
signing time per signer (ms)	**78.29**	122.00	179.20	710.00	1584.43
single signer verifier accepts	✓	✓	✗	✓	✓
persistent state	$O(1)$	$O(Q_s)$	$O(1)$	$O(1)$	$O(1)$

[1] Derives from the abbreviation "Th" for **Th**reshold and the Turkish word *imza*, meaning "*signature*"; Thimza: Threshold Signature.

Lattice-Based Threshold Signatures: State of the Art

Scheme	t	rd/on-rd	$\lvert\mathrm{tr}\rvert/t$	on	$\lvert\mathsf{vk}\rvert$	$\lvert\sigma\rvert$	interch.	Assumptions
Bendlin et al. [BKP13]	small	≥ 4	$> 10^3$	all	—	—	✗	SIS, generic MPC
Boneh et al. [BGG+18]	any	1	$> 10^3$	all	—	—	✗	LWE, threshold FHE
Agrawal et al. [ASY22]	any	1	$> 10^3$	all	—	—	✗	LWE, threshold FHE
Damgård et al. [DOTT21]	$t = n$	3/3	25.0	all	7.0	12.0	✗	MLWE, MSIS
Chen [Che23]	$t = n$	2/1	300.0	30.9	10.5	30.9	✗	MLWE, MSIS
Threshold Raccoon [dPKM+24]	1024	3/3	40.8	all	3.9	12.7	✓	MLWE, MSIS
Espitau et al. [EKT24]	1024	2/1	276.1	14.1	5.5	10.8	✓	AOM-MLWE, MSIS
Gur et al. [GKS24]	5	2/2	3072.0	all	13.0	46.0	✗	RLWE, RSIS
C-Apirom et al. [CTZ24]	5	2/1	1526.0	≈ 260	47.0	258.0	✗	MSIS
Ringtail [BKL+25]	1024	2/1	612.8	10.5	4.5	13.4	✓	MLWE, MSIS
del Pino, Niot [dPN25]	8	3/3	7.5	all	2.6	2.7	✗	MLWE, MSIS
TalonG [GTJ+26]	1024	2/2	26.9	all	2.0	17.7	✗	RLWE, RSIS, NTRU
Hermine [BCd+26]	64	2/1	71.5	19.5	2.8	11.0	✓	AOM-MISIS
Thimza [Our Work]	1024	3/3	**16.3**	all	3.8	12.8	✓	**MLWE, MSIS**

Sizes in KiB (kibibytes) at the 128 bit level. $\lvert\mathrm{tr}\rvert/t$: communication per signer of one signing execution. "on": the part that cannot be preprocessed. "rd/on-rd": number of rounds, and number of rounds that depend on the message. "interch.": acceptance by the unmodified verifier of the single signer scheme. Prior values are those reported by their developers.

`Thimza` is simultaneously smallest in communication, interchangeable, and competitive in signature size.

Threshold Signatures, Raccoon, and the Masking Requirement

Definition 1 (*threshold signature scheme*)

A (t, n)-threshold signature Σ has $\mathsf{KeyGen}(1^\lambda, t, n) \to (\mathsf{vk}, (\mathsf{sk}_i)_{i\in[n]})$, round algorithms $\mathsf{Sign}_1, \ldots, \mathsf{Sign}_\rho$, a combiner Combine for the messages of a signer set of size t, and a verifier Verify.

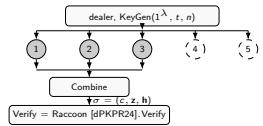
Algorithm 1 (*Raccoon [dPKPR24], the base scheme*)

1: $\mathbf{A} \leftarrow \mathcal{R}_q^{k\times\ell}$ from a 2λ bit seed; $\mathbf{s} \leftarrow D^\ell_{\sigma_\mathsf{t}}$, $\mathbf{e} \leftarrow D^k_{\sigma_\mathsf{t}}$
2: $\mathbf{t} := \lfloor \mathbf{As} + \mathbf{e} \rceil_{\nu_\mathsf{t}}$; **return** $\mathsf{vk} := (\mathbf{A}, \mathbf{t})$
3: $\mathbf{r} \leftarrow D^\ell_{\sigma_\mathsf{w}\sqrt{T_{\max}}}$, $\mathbf{e}' \leftarrow D^k_{\sigma_\mathsf{w}\sqrt{T_{\max}}}$; $\mathbf{w} := \mathbf{Ar} + \mathbf{e}'$
4: $c := H_c(\mathsf{vk}, \lfloor \mathbf{w} \rceil_{\nu_\mathsf{w}}, \mathsf{msg})$; $\mathbf{z} := c\mathbf{s} + \mathbf{r}$, with no rejection
5: $\mathbf{h} := \lfloor \mathbf{w} \rceil_{\nu_\mathsf{w}} - \lfloor \mathbf{Az} - 2^{\nu_\mathsf{t}} c\mathbf{t} \rceil_{\nu_\mathsf{w}}$; **return** $(c, \mathbf{z}, \mathbf{h})$

Raccoon [dPKPR24] is Fiat–Shamir *without* rejection, made short by flooding [Lyu12], so a threshold protocol has no abort to explain, at a width far above the secret width.

Definition 2 (*functional interchangeability*)

Σ is *functionally interchangeable* with a single signer scheme Σ' if $\mathsf{Verify} = \Sigma'.\mathsf{Verify}$ and every honest signature lies in the support of $\Sigma'.\mathsf{Sign}$ under the same key, so a relying party runs Verify alone [BP25].



$$c = H_c\left(\mathsf{vk},\ \left\lfloor \mathbf{Az} - 2^{\nu_\mathsf{t}}\,\mathbf{ct} \right\rceil_{\nu_\mathsf{w}} + \mathbf{h},\ \mathsf{msg}\right)$$
$$\wedge\ \|(\mathbf{z}, 2^{\nu_\mathsf{w}}\mathbf{h})\|_2 \le B$$

MLWE [LS15], SelfTargetMSIS [dPLS20] as in [KLS18] because the forking lemma [BN06] has no superposition equivalent, and Hint-MLWE [KLSS23], which reduces to MLWE.

Cyclotomic ring of degree φ (a power of 2): $\mathcal{R} = \mathbb{Z}[X]/(X^\varphi+1)$, Quotient ring: $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$, $L = \lceil \log_2 q \rceil = 49$; $\lfloor x \rceil_\nu$ drops the ν low bits; $\mathcal{C}$ ternary challenges of weight ω; D_σ discrete Gaussian; (k, ℓ) module dimensions; $\sigma_\mathsf{t}, \sigma_\mathsf{w}$ secret and flooding widths; $T_{\max} = 1024$; H_0, H_1, H_c quantum-accessible random oracles; Q_s, Q_h signing and hash queries; filled circles form T.

Shamir Sharing over the Ring and Forcing Mask

Shamir Sharing and reconstruction. [Sha79]

- Evaluation points $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_q^\times$ ($\alpha_i - \alpha_j$ invertible)
- Sample $\mathbf{p}_1, \ldots, \mathbf{p}_{t-1} \leftarrow \mathcal{R}_q^\ell$ and set $\mathbf{s}_i = \mathbf{s} + \sum_{u=1}^{t-1} \mathbf{p}_u \alpha_i^u$.
- For $|T| = t$,

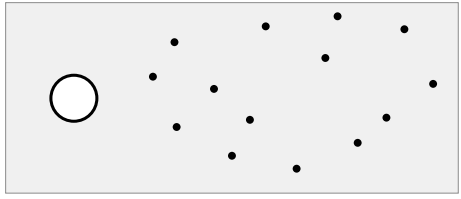
$$\lambda_{T,i} = \prod_{j \in T \setminus \{i\}} \alpha_j (\alpha_j - \alpha_i)^{-1}, \qquad \sum_{i \in T} \lambda_{T,i} \mathbf{s}_i = \mathbf{s},$$

- Any $t-1$ shares are uniform and independent of $\mathbf{s}$.

Obstruction.

- The coefficient $\lambda_{T,i} \in \mathcal{R}_q$ is uniform
- The contribution $c \cdot \lambda_{T,i} \cdot \mathbf{s}_i$ of a single signer is *not short*
- The ephemeral randomness of width $\sigma_{\mathrm{w}} = 2^{37}$ cannot flood a uniform element modulo $q = 2^{49}$.
- Use an additive mask $\mathbf{m}_i$ to hide the contribution
- Summation of masks over the signer set is $\sum_{i \in T} \mathbf{m}_i = 0$ [dPKM$^+$24].

$\mathcal{R}_q^\ell$, a box of side $q = 2^{49}$ in every coordinate



The white disc is $\mathbf{r}_i \sim D_{\sigma_{\mathrm{w}}}$, of radius about 2^{37}. The black dots are possible positions of $c\,\lambda_{T,i}\,\mathbf{s}_i$. A Gaussian of width 2^{37} hides nothing modulo 2^{49}, so an additive mask that is uniform over $\mathcal{R}_q^\ell$ is mandatory.

Threshold Raccoon [dPKM$^+$24], EKT [EKT24], Ringtail [BKL$^+$25], TalonG [GTJ$^+$26] and Thimza each transmit one uniform element of $\mathcal{R}_q^\ell$ per signer in the last round, which is 12 544 bytes at level I.

Threshold Raccoon: Protocol and One Signing Execution

Algorithm 2 (*signing in Threshold Raccoon [dPKM+24], code of signer i*)

Round 1. sid and the signer set T are inputs.

1: $\mathbf{r}_i \leftarrow D^{\ell}_{\sigma_{\mathrm{w}}}$, $\mathbf{e}'_i \leftarrow D^{k}_{\sigma_{\mathrm{w}}}$; $\mathbf{w}_i := \mathbf{A}\mathbf{r}_i + \mathbf{e}'_i$

2: expand the row mask $\mathbf{m}_i^{\mathrm{row}} \in \mathcal{R}_q^{\ell}$, at $t-1$ expansions and 12 544 bytes

3: broadcast $\mathsf{cmt}_i := H(\mathsf{sid}, i, \mathbf{w}_i)$ together with $\mathbf{m}_i^{\mathrm{row}}$

Round 2.

4: broadcast the untruncated $\mathbf{w}_i$, which is 15 680 bytes

5: broadcast $\tau_{i\to j} := \mathsf{MAC}(\mathsf{k}_{i,j}, \text{view of round 1})$ for $j \in T$, 16 bytes each

Round 3.

6: verify every tag and opening, which realizes the authenticated channel

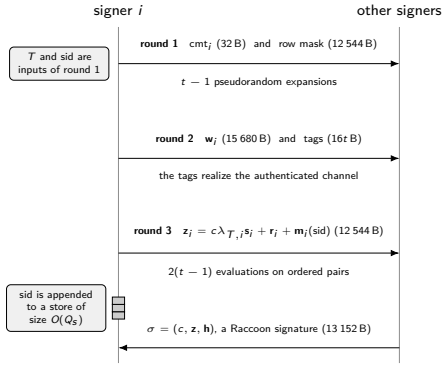
7: $\mathbf{w} := \left\lfloor \sum_{j\in T} \mathbf{w}_j \right\rceil_{\nu_{\mathrm{w}}}$; $c := H_c(\mathsf{vk}, \mathbf{w}, \mathsf{msg})$

8: $\mathbf{m}_i(\mathsf{sid}) := \sum_{j\in T\setminus\{i\}} (\mathsf{PRF}(\mathsf{sd}_{i,j}, \mathsf{sid}) - \mathsf{PRF}(\mathsf{sd}_{j,i}, \mathsf{sid}))$, which is $2(t-1)$ evaluations over $2(n-1)$ seeds

9: $\mathbf{z}_i := c \cdot \lambda_{T,i} \cdot \mathbf{s}_i + \mathbf{r}_i + \mathbf{m}_i(\mathsf{sid})$

10: $\mathcal{S}_i := \mathcal{S}_i \cup \{\mathsf{sid}\}$, where the registry never shrinks

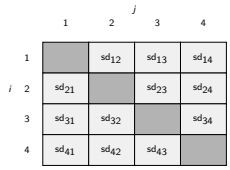
Mask is keyed by a *session identifier*; cancellation needs identical views, so *authenticated channels* are assumed; first round already names T and sid.



per signer: 40 848 + 16t bytes and $3(t-1)$ pseudorandom vectors of $\mathcal{R}_q^{\ell}$

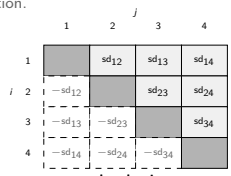
$\mathsf{sd}_{i,j}$ seed of the *ordered* pair (i,j); $\mathsf{k}_{i,j}$ key of a message authentication code; $\mathcal{S}_i$ the registry of answered identifiers; cmt_i commitment hash; vw transcript digest.

Pairwise Masking and the Canonical Linear Response Class



ordered pairs
TRaccoon [dPKM$^+$24], EKT [EKT24], Ringtail [BKL$^+$25]

$2(n-1)$ seeds stored and $2(t-1)$ evaluations per session; cancellation requires a second evaluation.



unordered pairs
Thimza

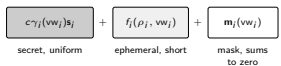
$n-1$ seeds stored and $t-1$ evaluations per session; cancellation follows from the antisymmetric sign $\varepsilon_{ij} = -\varepsilon_{ji}$.

Definition 3 (*canonical linear response scheme*)

The message of the first round is $\mathsf{Cmt}(\mathsf{sk}_i; \rho_i)$, the challenge of the last round is $c = \mathsf{Chl}(\mathsf{vw}_i)$, and the message of the last round is

$$\mathbf{z}_i = c\gamma_i(\mathsf{vw}_i)\mathbf{s}_i + f_i(\rho_i, \mathsf{vw}_i) + \mathbf{m}_i(\mathsf{vw}_i),$$

with ρ_i a fresh randomness, γ_i a public reconstruction coefficient, f_i independent of $\mathbf{s}_i$, and $\mathbf{m}_i$ computable from sk_i and vw_i.



scheme	in class	mask keyed by
TRaccoon [dPKM$^+$24]	✓	session identifier
EKT [EKT24]	✓	session identifier
Ringtail [BKL$^+$25]	✓	session identifier
TalonG [GTJ$^+$26]	✓	session identifier
C-Apirom et al. [CTZ24]	✓	no mask, short coeff.
FROST [KG20], group	✓	no mask
Thimza	✓	**the view vw**
Hermine [BCd$^+$26]	✓	no mask, short shares
threshold FHE [BGG$^+$18, ASY22]	✗	no commitment round

Negative statements are proved for this class, so it applies to all of these constructions and not only to ours.

Three Limitations, and the Security Models of the Family

Limitation 1. Unbounded signer state

- The mask of the pair (i, j) is $\mathrm{PRF}(\mathsf{seed}_{i,j}, \mathsf{sid})$
- A signer must store *every* identifier it has ever answered and refuse a repetition.

"a stateless signature scheme is an important open problem" [dPKM$^+$24]

Limitation 2. Channels, coalitions, parameters

- Masks cancel only under identical views.
- TRaccoon authenticates every view.
- Ringtail [BKL$^+$25] assumes authenticated channels & an offline oracle knowing T.
- [ZT25, JTWZ26] remove those restrictions by reproving [EKT24] under another lattice problem
- That problem reduces to MLWE and MSIS in a large-parameter regime
- 30–50 KiB signatures instead of 11.

Limitation 3. Communication cost

Let $t = 1024$, and 128 bit level. Communication per signer:

- [dPKM$^+$24] : 40.8 KiB
- [EKT24] : 276 KiB
- [BKL$^+$25] : 613 KiB
- [GTJ$^+$26] : 26.9 KiB
- [BCd$^+$26]: 71.5 KiB

No scheme is at once smallest in communication, competitive in signature size, and accepted by the verifier of the single signer scheme.

scheme	auth. ch.	T at rd. 1	assumption
TRaccoon [dPKM$^+$24]	required	required	MLWE, MSIS
Ringtail [BKL$^+$25]	required	required	MLWE, MSIS
EKT [EKT24]	no	no	AOM-MLWE
EKT via [ZT25]	no	no	MLWE, MSIS, larger
Thimza	**no**	**no**	**MLWE, MSIS**

Can the strong network model be obtained *at the parameters of the weak one*, so that no assumption is traded for the removal of the channels?

Signer State: Is Statelessness Impossible?

Definition 4 (*stateless partial signing*)

The algorithm of the last round of every signer is a deterministic function of $(\mathsf{sk}_i, \mathsf{vw}_i)$.

Definition 5 (*session-bounded state*)

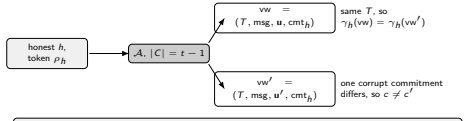
The persistent store consists only of tokens created in the first round of an open session, each token is consumed by at most one execution of the last round and erased immediately afterwards, and the store is empty whenever no session is open.

stateless Definition 4	persistent store is empty at all times	**impossible** Theorem 1
session-bounded Definition 5	one token per open session, erased on use	**attained** by Thimza
identifier registry TRaccoon [dPKM$^+$24]	S_i holds every sid ever answered	**unbounded** size $O(Q_S)$

The gap between the two definitions is only one bit per open session!

Theorem 1 (*impossibility of stateless partial signing*)

Let Σ be a canonical linear response threshold signature with $\rho \geq 2$ rounds in which ρ_i is sampled before the view that determines the challenge is complete. If Σ has stateless partial signing, then there is an adversary that corrupts $t-1$ parties, makes one query of the first round and two queries of the last round to a single honest signer h, and recovers $\gamma_h \mathbf{s}_h$ up to a public invertible factor with probability at least $1 - \varphi/q - 2^{-\lambda}$. In particular Σ is not unforgeable whenever $t \leq n$.



$$\mathbf{z}_h - \mathbf{z}'_h = (c - c')\gamma_h \mathbf{s}_h + \underbrace{\left(\bar{f}_h(\rho_h, \mathsf{vw}) - \bar{f}_h(\rho_h, \mathsf{vw}')\right)}_{\text{vanishes, or solved by } \ell\varphi \text{ repetitions}} + \underbrace{\left(\mathbf{m}_h(\mathsf{vw}) - \mathbf{m}_h(\mathsf{vw}')\right)}_{\text{computable by } \mathcal{A}}$$

$c - c'$ is invertible except with probability φ/q, so $\lambda_{T,h}\mathbf{s}_h$ follows, and then $\mathbf{s}$ by interpolation with the corrupt shares.

Remark 1 (*Scope*)

It holds for *every* member of Definition 3, hence for [dPKM$^+$24, EKT24, BKL$^+$25, CTZ24, GTJ$^+$26], for FROST [KG20] in the group setting and for Thimza alike. It does not rule out stateless threshold signatures altogether: constructions from **threshold fully homomorphic encryption** [BGG$^+$18, ASY22] have no separate commitment round and are indeed stateless, at the price of a homomorphic evaluation of the signing circuit.

Signer State: Sufficiency of Bounded Session

Call a masking term *derived from the view* if $\mathbf{m}_i(\mathsf{vw}_i) = \sum_{j \in T \setminus \{i\}} \varepsilon_{ij} \mathsf{PRF}(\mathsf{sd}_{\{i,j\}}, \mathsf{vw}_i)$ with $\varepsilon_{ij} = -\varepsilon_{ji} \in \{\pm 1\}$ and one seed per unordered pair.

Lemma 1 (*replay*)

Let Σ be a canonical linear response scheme with masking derived from the view, and let a signer h hold a fixed token ρ_h. If h is invoked twice in the last round on views $\mathsf{vw} = \mathsf{vw}'$, then the two responses are equal, so the second invocation is perfectly simulatable from the first.

Case 1, the same view. Every summand of $\mathbf{z}_h$ is a deterministic function of $(\mathsf{sk}_h, \rho_h, \mathsf{vw})$, so the response is identical bit for bit and $\mathcal{A}$ could have copied it.

Case 2, a different view. The token has already been consumed and erased, so the query is refused, which is precisely the event Theorem 1 shows must be refused.

Corollary 1 (*minimality*)

- Unforgeable with session-bounded state iff Unforgeable with a store that additionally records every session identifier.
- Session-bounded state is minimal, since by Theorem 1 no smaller store suffices.

In [dPKM+24] the mask is keyed by sid, which the adversary controls and may repeat while it varies T. In Thimza it is keyed by vw, which already determines T, the message and every commitment, so repeating the key of the mask is repeating the *entire* query.

Views and Channels: the View Partition Lemma

Definition 6 (TS-UF-CA, *unforgeability with oracles agnostic to the channel and to the signer set*)

The standard game with two changes:

- $\mathcal{O}_1(i, \text{msg})$ takes *no signer set*, so the message of the first round is produced before T exists.
- $\mathcal{O}_3(\text{eid}, T, (\text{cmt}_j, \tilde{\mathbf{w}}_j)_{j \in T})$ performs *no consistency check* relating the delivered openings to what the honest signers sent

Note that:

- $\mathcal{A}$ may supply forged, reordered or mutually inconsistent openings
- Statelessness is built in: $\mathcal{O}_3$ closes the record before returning and a replay of a closed handle returns $\perp$.
- The three hash oracles are queried in superposition and the three signing oracles are classical.

Theorem 2 (*transfer to the strengthened model*)

- Let Σ be canonical linear response with three rounds
- Antisymmetric masking derived from the view
- A first round free of the signer set
- The Raccoon [dPKPR24] verification relation

If Σ is unforgeable with authenticated channels and oracles aware of the signer set, then it is unforgeable in the game of Definition 6, with

$$\mathrm{Adv}^{\text{ts-uf-ca}}_{\Sigma,\mathcal{A}} \le \mathrm{Adv}^{\text{Hint-MLWE}}_{\mathcal{B}_1} + \mathrm{Adv}^{\text{SelfTargetMSIS}}_{\mathcal{B}_2} + \mathrm{Adv}^{\text{PRF}}_{\mathcal{B}_3} + C\frac{(Q_h+Q_s)^3}{2^{2\lambda}} + \frac{3Q_s}{2}\sqrt{\frac{Q_h}{2^{\mu}}},$$

and the parameters of the two lattice instances are unchanged from the weak model.

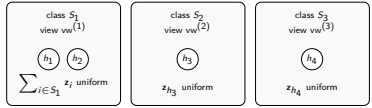
Lemma 2 (*view partition*)

- Fix a session, and partition honest signers by their views into $S_1, \ldots, S_m$
- View-derived antisymmetric pairwise masks, for every $S_a \neq H$ (the set of honest members)

$$\sum_{i \in S_a} \vec{z}_i \approx_c U(\mathcal{R}_q^{\ell}).$$

- If all honest signers have the same view ($m = 1$),

$$\sum_{i \in H} \vec{z}_i = c \sum_{i \in H} \lambda_{T,i} \vec{s}_i + \sum_{i \in H} f_i + \text{adversary-known term}.$$



- **Consistent to arbitrary views:** A simulator for sessions with agreeing honest views can also handle sessions with inconsistent views. The inconsistent-view classes are hidden by the unmatched masks.
- **MACs are unnecessary:** Since security holds even with inconsistent views, MACs are no longer needed to enforce view consistency.
- **No parameter loss:** Since the first round is independent of T, the simulator can choose T in the last round without additional random-oracle reprogramming; hence the parameters remain unchanged.

Two Matching Lower Bounds on the Masking Mechanism

Theorem 3 (*lower bound on pseudorandom material*)

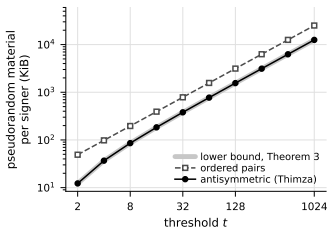
- **Lower bound:** Security against $t-2$ corruptions requires each signer to use pairwise pseudorandom material with all other $t-1$ signers:

$$\geq (t-1)\ell\varphi\lceil\log_2 q\rceil \quad \text{bits per signer/session.}$$

- **Optimality:** Antisymmetric masking with one seed per unordered pair, $\mathbf{m}_i = \sum_{j\in T\setminus\{i\}} \varepsilon_{ij}\mathsf{PRF}(\mathsf{sd}_{\{i,j\}}, \mathsf{vw}_i)$, achieves this bound with equality
- **Comparison:** The ordered construction of [dPKM$^+$24, EKT24, BKL$^+$25] uses $2t$ PRF evaluations and $2n$ seeds—approximately twice the optimum.

Corollary 2 (*antisymmetric construction optimality*)

$\mathbf{m}_i = \sum_{j\in T\setminus\{i\}} \varepsilon_{ij}\mathsf{PRF}(\mathsf{sd}_{\{i,j\}}, \mathsf{vw}_i)$ with one seed per unordered pair meets Theorem 3 *with equality*, whereas the ordered construction of [dPKM$^+$24, EKT24, BKL$^+$25] uses $2t$ evaluations and $2n$ seeds, **twice the optimum in both**.

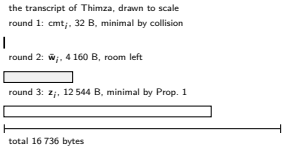


Pseudorandom material per signer and per session. The antisymmetric curve lies exactly on the bound.

Proposition 1 (*incompressibility of a masked partial signature*)

- Reconstruction coefficients $\gamma_i \in \mathcal{R}_q^\times$ can take at least two values.
- Security holds against $t-2$ corruptions.
- Then each honest signer's last-round message is uniform over $\mathcal{R}_q^\ell$ conditioned on the adversary's view.
- Hence it is **incompressible** and requires at least

$$\ell\varphi\log_2 q \quad \text{bits.}$$



Theorem 3 says the *work* of masking cannot fall below $t-1$ ring vectors; Proposition 1 says the *output* cannot be compressed below one ring vector. Thimza attains both, so the only remaining freedom is in the commitment round, and Theorem 4 fixes how far it may be truncated.

Thimza Design: Four Mechanisms, and the Trust Assumptions

M1. Commitment free of the signer set.

- **Signer-set-independent commitment:** $\mathsf{cmt}_i = H_0(\mathsf{vk}, \mathsf{msg}, i, \tilde{\mathbf{w}}_i)$ does not depend on T.
- Signers can commit before T is known.
- T can be finalized from the signers responding in Round 2.

Removes: the oracle aware of the coalition of [dPKM$^+$24, BKL$^+$25].

M2. Transmission of the leading bits.

- Signer i publishes the rounded value $\tilde{\mathbf{w}}_i = \left\lfloor \mathbf{w}_i \right\rceil_{\nu_c}$ instead of $\mathbf{w}_i$.
- The resulting perturbation in the aggregate $\mathbf{W} = \sum_{j \in T} 2^{\nu_c} \tilde{\mathbf{w}}_j$ is absorbed by the hint.

Removes: $k \varphi \nu_c$ bits, that is 15 680 $\rightarrow$ 4 160 bytes at level I.

M3. Antisymmetric masking derived from view.

- $\mathbf{m}_i = \sum_{j \in T \setminus \{i\}} \varepsilon_{ij} \mathsf{PRF}(\mathsf{sd}_{\{i,j\}}, \mathsf{vw})$, with one seed per unordered pair.
- vw is the digest of the entire Round-2 transcript.
- **Optimal** by Corollary 2; **no authentication tags** needed by Lemma 2.

Removes: half the seeds and evaluations, the row mask of 12 544 bytes and the 16t bytes of tags.

M4. No persistent store. By Corollary 1 a signer keeps only $\mathsf{st}_i = (\mathbf{r}_i, \tilde{\mathbf{w}}_i)$ between round 1 and round 3 and erases it afterwards, so the store is empty whenever no session is open.

Removes: the registry of size $O(Q_s)$ of [dPKM$^+$24], and the requirement that the store never be rolled back.

The module dimensions, the modulus, the widths and the two roundings ν_t, ν_w are those of [dPKM$^+$24], so the MLWE and SelfTargetMSIS instances, and hence the estimated bit security, are the same. **The only new parameter in the whole scheme is ν_c.**

Trust Assumptions

1. A trusted dealer runs KeyGen once and erases $(\mathbf{s}, \mathbf{e})$ after distributing shares and pairwise seeds privately.
2. A static adversary corrupts at most $t - 1$ parties before key generation.
3. The broadcast medium is unauthenticated and unreliable, so it may drop, reorder, duplicate or forge any message.
4. Honest parties consume and erase each token at most once, which is unavoidable by Theorem 1 and sufficient by Corollary 1.
5. H_0, H_1, H_c are quantum-accessible random oracles and PRF is a pseudorandom function.
6. MLWE and SelfTargetMSIS are hard (for the given parameters) against Q_s signing queries.

Two assumptions of [dPKM$^+$24, BKL$^+$25] are absent, which are authenticated channels between honest signers and knowledge of the signer set at round 1.

Two further assumptions are needed for liveness but not for unforgeability, which is a synchronous network and honest behavior inside the signer set. Thimza, like every scheme of the landscape table except [BCd$^+$26, dPE$^+$25], does not identify who caused a failure.

The Scheme: Key Generation, Signing, Combination and One Execution

Algorithm 3 (*Thimza*.KeyGen$(1^\lambda, t, n)$)

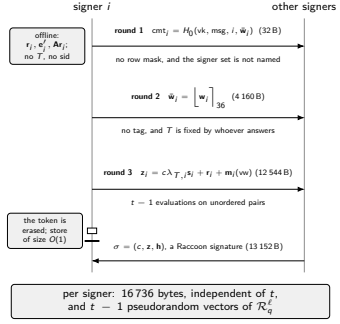
1: $\mathsf{seed}_\mathbf{A} \leftarrow \{0,1\}^{2\lambda}$; $\mathbf{A} := \mathsf{Expand}(\mathsf{seed}_\mathbf{A}) \in \mathcal{R}_q^{k\times\ell}$
2: $\mathbf{s} \leftarrow D^\ell_{\sigma_\mathbf{t}}$, $\mathbf{e} \leftarrow D^k_{\sigma_\mathbf{t}}$; $\mathbf{t} := \lfloor \mathbf{As}+\mathbf{e} \rceil_{\nu_\mathbf{t}}$; $\mathsf{vk} := (\mathsf{seed}_\mathbf{A}, \mathbf{t})$
3: $\mathbf{p}_1, \ldots, \mathbf{p}_{t-1} \leftarrow \mathcal{R}_q^\ell$; $\mathbf{s}_i := \mathbf{s} + \sum_{u=1}^{t-1} \mathbf{p}_u \alpha_i^u$ for $i \in [n]$
4: $\mathsf{sd}_{\{i,j\}} \leftarrow \{0,1\}^\lambda$ for each *unordered* pair, which is $\binom{n}{2}$ seeds
5: **return** vk and $\mathsf{sk}_i := (\mathbf{s}_i, (\mathsf{sd}_{\{i,j\}})_{j\neq i}, \mathsf{vk})$ for $i \in [n]$

Algorithm 4 (*Thimza signing, the complete code of signer i*)

Round 1. $\mathsf{Sign}_1(\mathsf{sk}_i, \mathsf{msg})$, in which T is *not* an input
1: $\mathbf{r}_i \leftarrow D^\ell_{\sigma_\mathbf{w}}$; $\mathbf{e}'_i \leftarrow D^k_{\sigma_\mathbf{w}}$; $\mathbf{w}_i := \mathbf{Ar}_i + \mathbf{e}'_i$; $\tilde{\mathbf{w}}_i := \lfloor \mathbf{w}_i \rceil_{\nu_\mathbf{c}}$
2: $\mathsf{st}_i := (\mathbf{r}_i, \tilde{\mathbf{w}}_i)$; **return** $\mathsf{cmt}_i := H_0(\mathsf{vk}, \mathsf{msg}, i, \tilde{\mathbf{w}}_i)$, which is 32 bytes
Round 2. $\mathsf{Sign}_2(\mathsf{st}_i)$
3: **return** $\tilde{\mathbf{w}}_i$, which is 4 160 bytes and needs no computation
Round 3. $\mathsf{Sign}_3(\mathsf{sk}_i, \mathsf{st}_i, T, (\mathsf{cmt}_j, \tilde{\mathbf{w}}_j)_{j\in T}, \mathsf{msg})$
4: **if** $\exists j \in T : \mathsf{cmt}_j \neq H_0(\mathsf{vk}, \mathsf{msg}, j, \tilde{\mathbf{w}}_j)$ **then abort**
5: $\mathsf{vw} := H_1(\mathsf{vk}, \mathsf{msg}, T, (\mathsf{cmt}_j)_{j\in T}, (\tilde{\mathbf{w}}_j)_{j\in T})$, the digest that keys the masks
6: $\mathbf{W} := \sum_{j\in T} 2^{\nu_\mathbf{c}} \tilde{\mathbf{w}}_j \bmod q$; $\mathbf{w} := \lfloor \mathbf{W} \rceil_{\nu_\mathbf{w}}$; $c := H_c(\mathsf{vk}, \mathbf{w}, \mathsf{msg})$
7: $\mathbf{m}_i := \sum_{j\in T\setminus\{i\}} \varepsilon_{ij} \mathsf{PRF}(\mathsf{sd}_{\{i,j\}}, \mathsf{vw})$, $t-1$ evaluations, $\varepsilon_{ij} = +1$ iff $i < j$
8: $\mathbf{z}_i := c\lambda_{T,i}\mathbf{s}_i + \mathbf{r}_i + \mathbf{m}_i \bmod q$, which is 12 544 bytes
9: erase st_i, after which the store is empty; **return** $\mathbf{z}_i$

Algorithm 5 (*Thimza*.Combine *and Thimza*.Verify)

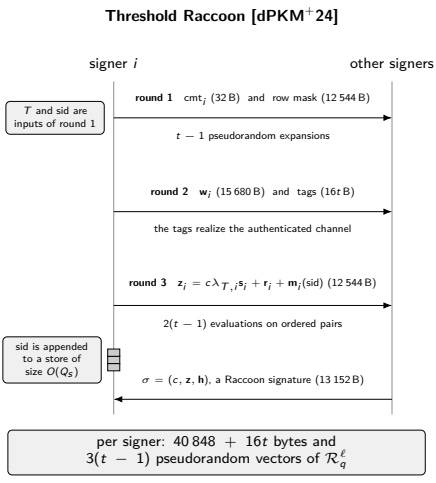
1: recompute $\mathbf{w}$ and c as in Round 3; $\mathbf{z} := \sum_{j\in T} \mathbf{z}_j \bmod q$, at which point the masks cancel
2: $\mathbf{h} := \mathbf{w} - \lfloor \mathbf{Az} - 2^{\nu_\mathbf{t}} \mathbf{ct} \rceil_{\nu_\mathbf{w}} \bmod q_{\nu_\mathbf{w}}$; **return** $\sigma := (c, \mathbf{z}, \mathbf{h})$
3: Verify: **return** $[c = H_c(\mathsf{vk}, \lfloor \mathbf{Az} - 2^{\nu_\mathbf{t}} \mathbf{ct} \rceil_{\nu_\mathbf{w}} + \mathbf{h}, \mathsf{msg})] \wedge [\|(\mathbf{z}, 2^{\nu_\mathbf{w}}\mathbf{h})\|_2 \leq B]$, identical to Raccoon [dPKPR24]

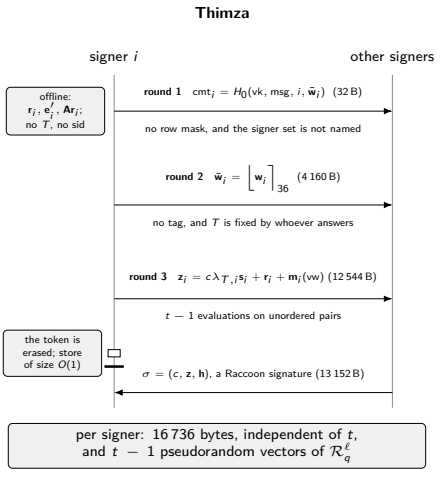


Verify **is same as the Raccoon [dPKPR24] verifier**, which is the formal content of interchangeability. Round 1 is 32 bytes and names neither the signer set nor an identifier; round 2 costs nothing, since it forwards a value already computed; round 3 carries the whole cost and produces the only component of the transcript that Proposition 1 shows to be incompressible.

$\mathsf{seed}_\mathbf{A}$ seed of the public matrix; $\mathbf{p}_u$ coefficients of the sharing polynomial; α_i evaluation point of party i; st_i the session token; $\mathbf{W}$ the rebuilt aggregate.

The Two Protocols of Family



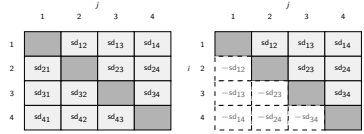


Four differences: the note before round 1, the payload of round 1, the payload of round 2, and the store marker on the lifeline.

Summary of the Differences, and the Structure of the Mask

	TRaccoon [dPKM$^+$24]	**Thimza**	saving
input of round 1	T and sid already required	the message only	—
round 1 payload	cmt_i and the row mask	cmt_i only	12 576 → 32 B
round 1 work	$t-1$ expansions	one matrix-vector product	40.23 → 1.19 ms
round 2 payload	untruncated $\mathbf{w}_i$ and t tags	truncated $\bar{\mathbf{w}}_i$	32 064 → 4 160 B
round 2 work	t authentications	none	1.20 → 0.00 ms
input of the mask	the identifier sid	the digest vw	$O(Q_s)$ → $O(1)$
mask structure	ordered, $2(n-1)$ seeds, $2(t-1)$ evaluations	unordered, $n-1$ seeds, $t-1$ evaluations	factor 2
round 3 payload	$\mathbf{z}_i \in \mathcal{R}_q^\ell$	$\mathbf{z}_i \in \mathcal{R}_q^\ell$	minimal in both
network model	authenticated channels	unauthenticated, inconsistent views	—
total per signer	**40 848 + 16t B**	**16 736 B, independent of t**	**3.42×**
time at $t = 1024$	**122.00 ms**	**78.29 ms**	**1.56×**

The two schemes share φ, q, σ_t, σ_w, (ℓ, k), ω, ν_t, ν_w, the verification key of 3 872 bytes and the signature of 13 152 bytes.



Left: ordered pairs, used by [dPKM$^+$24, EKT24, BKL$^+$25].
Right: unordered pairs, used by Thimza.

	ordered	antisymmetric
seeds per signer	$2(n-1)$	$n-1$
evaluations per session	$2(t-1)$	$t-1$
row mask transmitted	$\ell\varphi L$ bits	none
zero-sum property	✓	✓

Difference 1. The cancellation is obtained from the *sign* rather than from a second evaluation. Since $\varepsilon_{ij} + \varepsilon_{ji} = 0$, the pair $\{i, j\}$ contributes the same pseudorandom value twice with opposite signs, exactly as the ordered construction does, but each signer evaluates it once instead of twice. At $n = 5$ a signer stores 128 bytes of seeds against 320, and by Theorem 3 the right column meets the lower bound with equality.

Correctness

Lemma 3 (*aggregation identity*)

If all signers in T follow the protocol on a common view, then $\mathbf{z} = \sum_{j \in T} \mathbf{z}_j = c\mathbf{s} + \sum_{j \in T} \mathbf{r}_j \bmod q$ and

$$\tilde{\mathbf{e}} = \mathbf{W} - \left(\mathbf{A}\mathbf{z} - 2^{\nu_t} c\mathbf{t}\right) = \underbrace{\sum_{j \in T} \mathbf{e}'_j}_{\text{aggregated noise}} + \underbrace{\boldsymbol{\delta}}_{\text{truncation}} + \underbrace{c\mathbf{e} - c\boldsymbol{\rho}}_{\text{key terms}},$$

with $\|\boldsymbol{\delta}\|_\infty \le t 2^{\nu_c - 1}$ and $\|\boldsymbol{\rho}\|_\infty \le 2^{\nu_t - 1}$.

Theorem 4 (*correctness*)

If $\left\| \left(\sum_{j \in T} \mathbf{r}_j,\ \tilde{\mathbf{e}} \right) \right\|_2 + 2^{\nu_w + 1} \sqrt{k\varphi} \le B$, then $\mathsf{Verify}(\mathsf{vk}, \mathsf{msg}, \mathsf{Combine}(\cdot)) = 1$.
With appropriate selection of the parameters this holds except with probability at most $2^{-\lambda}$ for every $t \le T_{\max}$, and the choice $\nu_c = \lfloor \log_2 \sigma_w \rfloor - 1$ inflates the left hand side by at most one per cent.

t	$\max \|(\mathbf{z}, 2^{\nu_w}\mathbf{h})\|_2$	B	ratio
4	$2.98 \cdot 10^{13}$	$4.52 \cdot 10^{14}$	0.066
16	$4.48 \cdot 10^{13}$	$4.52 \cdot 10^{14}$	0.099
64	$8.05 \cdot 10^{13}$	$4.52 \cdot 10^{14}$	0.178
256	$1.55 \cdot 10^{14}$	$4.52 \cdot 10^{14}$	0.344
1024	$3.10 \cdot 10^{14}$	$4.52 \cdot 10^{14}$	0.685

Numerical verification at level I over 200 trials per row, with every quantity drawn from its exact distribution. The dominant summand is $\sum_j \mathbf{e}'_j$; the term $c\mathbf{e}$ is $2^{29.7}$ against 2^{42}; the term $c\boldsymbol{\rho}$ has ratio 0.36 and is already present in [dPKM+24]; the new term $\boldsymbol{\delta}$ has ratio 0.144.

Unforgeability in the QROM

Theorem 5 (*unforgeability of Thimza*)

- Unforgeable in the game ts-uf-ca (Definition 6)
- Session-bounded state
- Under MLWE and SelfTargetMSIS and the pseudorandomness of PRF against quantum distinguishers

For every quantum $\mathcal{A}$:

- Corrupting $\leq t-1$ signers
- Making $\leq Q_s$ classical signing queries
- Making $\leq Q_h$ quantum superposition queries to H_0, H_1 and H_c

there are $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ running in essentially the time of $\mathcal{A}$ with

$$\mathsf{Adv}^{\text{ts-uf-ca}}_{\text{Thimza},\mathcal{A}} \leq \mathsf{Adv}^{\text{Hint-MLWE}_{q,k,\ell,Q_s,\sigma_t,\sigma_w,\mathcal{C}}}_{\mathcal{B}_1} + \mathsf{Adv}^{\text{SelfTargetMSIS}_{q,k,\ell+1,\mathcal{C},\beta}}_{\mathcal{B}_2} + \mathsf{Adv}^{\text{PRF}}_{\mathcal{B}_3} + C\,\frac{(Q_h+Q_s)^3}{2^{2\lambda}} + \frac{3Q_s}{2}\sqrt{\frac{Q_h}{2^{\mu}}},$$

- $\beta = B + \sqrt{\omega} + (\omega 2^{\nu_t} + 2^{\nu_w+1})\sqrt{k\varphi}$
- Min-entropy of the rounded aggregate commitment: $\mu = k\varphi \log_2(q/2^{\nu_w}) - O(\lambda)$

Proposition 2 (*comparison with the base notion*)

The game of Definition 6 is at least as strong as TS-UF-0 of [BCK+22], since every adversary that wins the latter against a canonical linear response scheme also wins the former, with the same advantage and running time.

Parameters, and Asymptotic Complexity

level	λ	Q_s	$\sigma_w\sqrt{T_{max}}$	ν_t	ν_w	ν_c	ℓ	k	ω
I	128	2^{60}	2^{42}	37	40	36	4	5	19
III	192	2^{64}	2^{42}	36	40	36	6	7	31
V	256	2^{60}	2^{41}	35	41	35	7	8	44

All sets use $\varphi = 512$, $L = \lceil \log_2 q \rceil = 49$, $\sigma_t = 2^{20}$ and $T_{max} = 1024$.

- Each row corresponds to one NIST security level.
- Q_s: number of signatures a key may produce.
- $\sigma_w\sqrt{T_{max}}$: width of the aggregated ephemeral randomness; determines the signature size.
- ν_t: number of bits dropped from the verification key.
- ν_w: number of bits dropped from the aggregate commitment.
- ν_c: number of bits dropped from the transmitted commitment share.
- ℓ: module dimension of the secret.
- k: module dimension of the samples.
- ω: Hamming weight of the challenge.

Three constraints fix the sets, and they are those of [dPKM+24] plus one.

- $\sigma_w \geq \eta_\varepsilon(\mathbb{Z}^\varphi)\omega\sqrt{Q_s}$ for the Hint-MLWE reduction with Q_s hints; at Level I, $\sigma_w \geq 2^{35.8}$, so we take $\sigma_w = 2^{37}$.
- $q \geq 2^6\sigma_w\sqrt{T_{max}}$, giving $L = 49$.
- ν_t: largest value such that $\omega 2^{\nu_t}\sqrt{k\varphi}$ remains below the aggregated noise.
- ν_c is set according to Theorem 4.

The MLWE instance and the SelfTargetMSIS instance are the ones already analysed in [dPKM+24], so the estimated hardness is unchanged.

Procedure **Thimza**	TRaccoon [dPKM+24]	EKT [EKT24]	Ringtail [BKL+25]
KeyGen $n(k+\ell)\varphi \log \varphi$	$n(k+\ell)\varphi \log \varphi$	$n(k+\ell)\varphi \log \varphi$	$n(k+\ell)\varphi \log \varphi$
Sign_1 $k\ell\varphi \log \varphi$	$k\ell\varphi \log \varphi + t\ell\varphi$	$k\ell\rho\varphi \log \varphi$	$k\ell\rho\varphi \log \varphi$
Sign_2 0	t	$k\rho\varphi \log \varphi + 2t\ell\varphi$	$k\rho\varphi \log \varphi + \varphi k^2\bar{d} + 2t\ell\varphi$
Sign_3 $t\ell\varphi + k\ell\varphi \log \varphi$	$2t\ell\varphi + k\ell\varphi \log \varphi$	—	—
Combine $t\ell\varphi + k\ell\varphi \log \varphi$	$2t\ell\varphi + k\ell\varphi \log \varphi$	$t\ell\varphi + k\ell\varphi \log \varphi$	$t\ell\varphi + k\ell\varphi \log \varphi$
Verify $k\ell\varphi \log \varphi$	$k\ell\varphi \log \varphi$	$k\ell\varphi \log \varphi$	$k\ell\varphi \log \varphi$
$\lvert \mathsf{tr} \rvert / t$ $k\varphi(L-\nu_c) + \ell\varphi L$	$2\ell\varphi L + k\varphi L + 128t$	$k\rho\varphi L + \ell\varphi L$	$k\rho\varphi L + \ell\varphi L + 128t$
$\lvert \sigma \rvert$ $\ell\varphi \log \sigma_z + k\varphi \log \frac{\sigma_z}{2\nu_w}$	same	same	same
$\lvert \mathsf{vk} \rvert$ $k\varphi(L-\nu_t) + 2\lambda$	same	same	same
$\lvert \mathsf{sk}_i \rvert$ $\ell\varphi L + \lambda(n-1)$	$\ell\varphi L + 2\lambda n$	$\ell\varphi L + 2\lambda n$	$\ell\varphi L + 2\lambda n$
state $O(1)$ token	$O(Q_s)$ identifiers	$O(1)$ token	$O(1)$ token

- **Time:** $\mathcal{R}_q$ operations per signer; **space:** bits sent per signer.
- t: threshold; ρ: number of columns of the first-round matrix.
- $\rho = \bar{d} + 1$ for [BKL+25]; $\rho =$ rep for [EKT24].
- NTT of one ring element: $\Theta(\varphi \log \varphi)$.
- Coefficientwise product or pseudorandom expansion: $\Theta(\varphi)$.

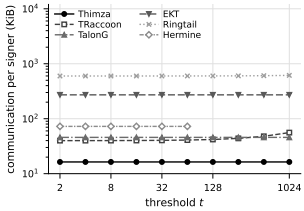
Thimza : $\Theta\left(k\ell\varphi \log \varphi + t\ell\varphi\right)$ TRaccoon [dPKM+24] : $\Theta\left(k\ell\varphi \log \varphi + 3t\ell\varphi\right)$

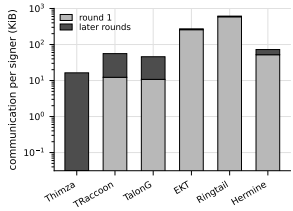
EKT [EKT24] : $\Theta\left(k\ell\rho\varphi \log \varphi + 2t\ell\varphi\right)$ Ringtail [BKL+25] : $\Theta\left(k\ell\rho\varphi \log \varphi + \varphi k^2\bar{d} + 2t\ell\varphi\right)$

Thimza:

- Removes the row mask: saves $\ell\varphi L$ bits.
- Truncates the commitment share: saves $k\varphi\nu_c$ bits.
- Removes authentication tags: saves $128t$ bits.
- **Only scheme with communication exactly independent of t.**
- At Level I, the leading term is 70% smaller than [dPKM+24].
- For $\rho = 49$ [BKL+25] and $\rho = 15$ [EKT24], their commitment term is 1–2 orders of magnitude larger.

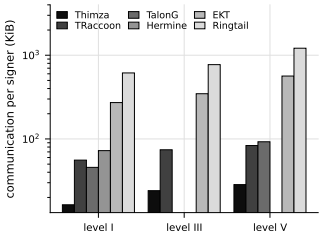
Communication: Totals, Components and the Threshold



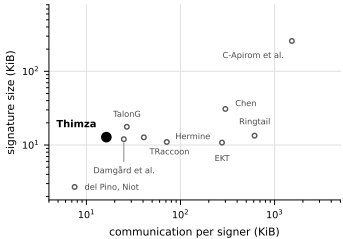


Left: communication per signer against the threshold. Right: the same volume split by round at $t = 1024$, and at $t = 64$ for Hermine [BCd+26], with the light part of each bar the first round.

Communication Across the Levels, and the Size Trade-off

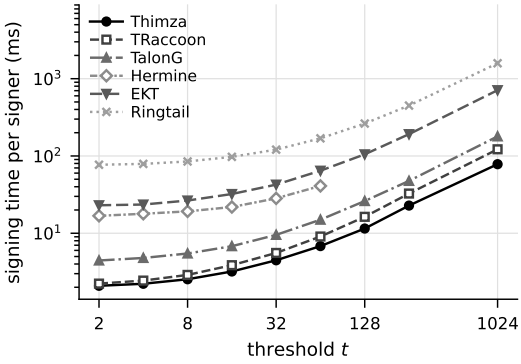


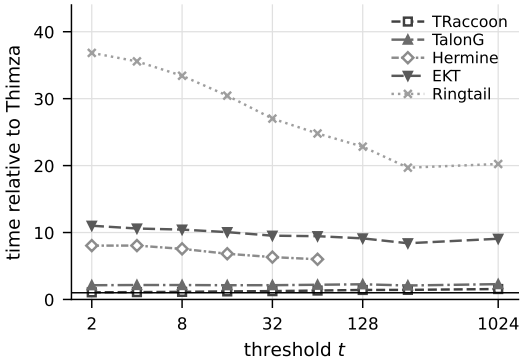
Communication per signer grouped by security level on a logarithmic axis. A missing bar means that the scheme has no published parameter set at that level.



Signature size against communication per signer at $t = 1024$, both on logarithmic axes, so that the lower left dominates. Values are those of the landscape table.

Signing Time





Advantages, and Limitations

Advantages

1. **Smallest communication**: 16 736 bytes/signer at level I (independent of t), up to 37.6× lower than alternatives [dPKM$^+$24, GTJ$^+$26, BCd$^+$26, EKT24, BKL$^+$25].
2. **Fastest signing** across all measured threshold values.
3. **Interchangeable**: Verify is identical to standard Raccoon [dPKPR24] verifier.
4. **Strongest network model** at weak-model parameter cost.
5. **Minimal state**: $O(1)$ size and empty between sessions.
6. **Standard assumptions**: no extra algebraic variants.
7. **Provably minimal**: two transcript components minimal.

Limitations

1. **Message-dependent rounds**: All 3 rounds depend on msg (higher latency at $t \leq 64$, but scales better at $t = 1024$).
2. **Larger verification key**: 3 872 B vs. 1 312 B [GTJ$^+$26] and 2 848 B [BCd$^+$26].
3. **Larger signature**: vs. [EKT24, BCd$^+$26] under uniform serializer.
4. **Feature gaps**: No identifiable abort or proactive refresh [BCd$^+$26, dPE$^+$25].
5. **Trusted dealer**: Assumed (common across landscape).

**Note: Size savings in other schemes require a 1^{st} round of 11–53 KiB (vs. 32 B in Thimza).*

Open Question

Can we construct secret sharing over $\mathcal{R}_q$ with **both** short reconstruction coefficients and compact shares? (Open even in classical setting).

References

[ADPS16] E. Alkim, L. Ducas, T. Pöppelmann, P. Schwabe. Post-Quantum Key Exchange, A New Hope. USENIX Security 2016, 327–343.

[APS15] M. R. Albrecht, R. Player, S. Scott. On the Concrete Hardness of Learning with Errors. Journal of Mathematical Cryptology 9(3), 169–203, 2015.

[ASY22] S. Agrawal, D. Stehlé, A. Yadav. Round-Optimal Lattice-Based Threshold Signatures, Revisited. ICALP 2022, LIPIcs 229, 8:1–8:20.

[BCK+22] M. Bellare, E. C. Crites, C. Komlo, M. Maller, S. Tessaro, C. Zhu. Better than Advertised Security for Non-interactive Threshold Signatures. CRYPTO 2022, Part IV, LNCS 13510, 517–550.

[BCd+26] G. Borin, S. Celi, R. del Pino, T. Espitau, S. Katsumata, G. Niot, T. Prest, K. Takemure. Hermine: An Efficient Lattice-Based FROST-like Threshold Signature. Cryptology ePrint Archive, 2026.

[BDG+14] G. Barthe, F. Dupressoir, B. Grégoire, C. Kunz, B. Schmidt, P.-Y. Strub. EasyCrypt: A Tutorial. Foundations of Security Analysis and Design VII, 146–166, 2014.

[BGG+18] D. Boneh, R. Gennaro, S. Goldfeder, A. Jain, S. Kim, P. M. R. Rasmussen, A. Sahai. Threshold Cryptosystems from Threshold Fully Homomorphic Encryption. CRYPTO 2018, Part I, LNCS 10991, 565–596.

[BKL+25] C. Boschini, D. Kaviani, R. W. F. Lai, G. Malavolta, A. Takahashi, M. Tibouchi. Ringtail: Practical Two-Round Threshold Signatures from Learning with Errors. IEEE S&P 2025, 149–164.

References

[BKP13] R. Bendlin, S. Krehbiel, C. Peikert. How to Share a Lattice Trapdoor: Threshold Protocols for Signatures and (H)IBE. ACNS 2013, LNCS 7954, 218–236.

[BLL+21] F. Benhamouda, T. Lepoint, J. Loss, M. Orrù, M. Raykova. On the (in)Security of ROS. EUROCRYPT 2021, Part I, LNCS 12696, 33–53.

[BN06] M. Bellare, G. Neven. Multi-signatures in the Plain Public-Key Model and a General Forking Lemma. ACM CCS 2006, 390–399.

[BP25] L. T. A. N. Brandão, R. Peralta. NIST First Call for Multi-Party Threshold Schemes. NIST IR 8214C, 2025.

[BTT22] C. Boschini, A. Takahashi, M. Tibouchi. MuSig-L: Lattice-Based Multi-signature with Single-Round Online Phase. CRYPTO 2022, Part II, LNCS 13508, 276–305.

[BZ13] D. Boneh, M. Zhandry. Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World. CRYPTO 2013, LNCS 8043, 361–379.

[CKM23] E. C. Crites, C. Komlo, M. Maller. Fully Adaptive Schnorr Threshold Signatures. CRYPTO 2023, Part I, LNCS 14081, 678–709.

[CTZ24] R. Chairattana-Apirom, S. Tessaro, C. Zhu. Partially Non-interactive Two-Round Lattice-Based Threshold Signatures. ASIACRYPT 2024, Part IV, 268–302.

[Che23] Y. Chen. DualMS: Efficient Lattice-Based Two-Round Multi-signature with Trapdoor-Free Simulation. CRYPTO 2023, Part V, LNCS 14085, 716–747.

References

[DEF+19] M. Drijvers, K. Edalatnejad, B. Ford, E. Kiltz, J. Loss, G. Neven, I. Stepanovs. On the Security of Two-Round Multi-Signatures. IEEE S&P 2019, 1084–1101.

[DF90] Y. Desmedt, Y. Frankel. Threshold Cryptosystems. CRYPTO'89, LNCS 435, 307–315.

[DKL+18] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, D. Stehlé. CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme. TCHES 2018(1), 238–268.

[DOTT21] I. Damgård, C. Orlandi, A. Takahashi, M. Tibouchi. Two-Round *n*-out-of-*n* and Multi-signatures and Trapdoor Commitment from Lattices. PKC 2021, LNCS 12710, 99–130.

[dPE+25] R. del Pino, T. Espitau, S. Katsumata, G. Niot, T. Prest. Unmasking TRaccoon: A Lattice-Based Threshold Signature with an Efficient Identifiable Abort Protocol. CRYPTO 2025.

[dPKM+24] R. del Pino, S. Katsumata, M. Maller, F. Mouhartem, T. Prest, M.-J. O. Saarinen. Threshold Raccoon: Practical Threshold Signatures from Standard Lattice Assumptions. EUROCRYPT 2024, LNCS 14652, 219–248.

[dPKPR24] R. del Pino, S. Katsumata, T. Prest, M. Rossi. Raccoon: A Masking-Friendly Signature Proven in the Probing Model. CRYPTO 2024, Part I, LNCS 14920, 409–444.

[dPLS20] R. del Pino, V. Lyubashevsky, G. Seiler. Post-Quantum Zero-Knowledge Proofs for Accumulators, Merkle Trees, and More. CRYPTO 2020, LNCS 12171, 684–713.

[dPN25] R. del Pino, G. Niot. Finally! A Compact Lattice-Based Threshold Signature. PKC 2025.

References

[EKT24] T. Espitau, S. Katsumata, K. Takemure. Two-Round Threshold Signature from Algebraic One-More Learning with Errors. CRYPTO 2024, Part VII, LNCS 14926, 387–424.

[GHHM21] A. B. Grilo, K. Hövelmanns, A. Hülsing, C. Majenz. Tight Adaptive Reprogramming in the QROM. ASIACRYPT 2021, Part I, LNCS 13090, 637–667.

[GKS24] K. D. Gur, J. Katz, T. Silde. Two-Round Threshold Lattice-Based Signatures from Threshold Homomorphic Encryption. PQCrypto 2024, 266–300.

[GPV08] C. Gentry, C. Peikert, V. Vaikuntanathan. Trapdoors for Hard Lattices and New Cryptographic Constructions. STOC 2008, 197–206.

[GTJ+26] L. Gao, G. Tang, D. Jia, Y. Liu, B. Liu, X. Lu, K. Wang, Y. Yin. TalonG: Bandwidth-Efficient Two-Round Threshold Signatures from Lattices. EUROCRYPT 2026.

[JTWZ26] K. Jiang, S. Tessaro, H. Wee, C. Zhu. Tweed: Adaptively Secure Lattice-Based Two-Round Threshold Signatures. EUROCRYPT 2026.

[KG20] C. Komlo, I. Goldberg. FROST: Flexible Round-Optimized Schnorr Threshold Signatures. SAC 2020, LNCS 12804, 34–65.

[KLS18] E. Kiltz, V. Lyubashevsky, C. Schaffner. A Concrete Treatment of Fiat–Shamir Signatures in the Quantum Random-Oracle Model. EUROCRYPT 2018, Part III, LNCS 10822, 552–586.

[KLSS23] D. Kim, D. Lee, J. Seo, Y. Song. Toward Practical Lattice-Based Proof of Knowledge from Hint-MLWE. CRYPTO 2023, Part V, LNCS 14085, 549–580.

References

[KRT24] S. Katsumata, M. Reichle, K. Takemure. Adaptively Secure 5 Round Threshold Signatures from MLWE/MSIS and DL with Rewinding. CRYPTO 2024, Part VII, LNCS 14926, 459–491.

[LPR13] V. Lyubashevsky, C. Peikert, O. Regev. On Ideal Lattices and Learning with Errors over Rings. Journal of the ACM 60(6), 43:1–43:35, 2013.

[LS15] A. Langlois, D. Stehlé. Worst-case to average-case reductions for module lattices. Journal of Cryptology 28(3), 570–600, 2015.

[Lyu12] V. Lyubashevsky. Lattice Signatures without Trapdoors. EUROCRYPT 2012, LNCS 7237, 738–755.

[MP12] D. Micciancio, C. Peikert. Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. EUROCRYPT 2012, LNCS 7237, 700–718.

[MR07] D. Micciancio, O. Regev. Worst-Case to Average-Case Reductions Based on Gaussian Measures. SIAM Journal on Computing 37(1), 267–302, 2007.

[NIS15] National Institute of Standards and Technology. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. FIPS 202, 2015.

[NIS24] National Institute of Standards and Technology. Module-Lattice-Based Digital Signature Standard. FIPS 204, 2024.

[NRS21] J. Nick, T. Ruffing, Y. Seurin. MuSig2: Simple Two-Round Schnorr Multi-signatures. CRYPTO 2021, Part I, LNCS 12825, 189–221.

References

[PFH+20] T. Prest, P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte, Z. Zhang. FALCON: Fast-Fourier Lattice-Based Compact Signatures over NTRU. NIST Post-Quantum Cryptography Standardization, 2020.

[Red80] J. W. Redhouse. Redhouse's Turkish Dictionary, in Two Parts, English and Turkish, and Turkish and English. 2nd edition, B. Quaritch, London, 1880.

[Sha79] A. Shamir. How to Share a Secret. Communications of the ACM 22(11), 612–613, 1979.

[SY25] K. Sedghighadikolaei, A. A. Yavuz. A Survey of Threshold Signatures: NIST Standards, Post-Quantum Cryptography, Exotic Techniques, and Real-World Applications. ACM Computing Surveys 58(6), 143:1–143:39, 2025.

[Thi] Implementation and `EasyCrypt` development of Thimza. `https://github.com/navid-divan/thimza`

[TZ23] S. Tessaro, C. Zhu. Threshold and Multi-signature Schemes from Linear Hash Functions. EUROCRYPT 2023, Part V, LNCS 14008, 628–658.

[Zha15] M. Zhandry. A Note on the Quantum Collision and Set Equality Problems. Quantum Information & Computation 15(7–8), 557–567, 2015.

[ZT25] C. Zhu, S. Tessaro. The Algebraic One-More MISIS Problem and Applications to Threshold Signatures. CRYPTO 2025, Part I, LNCS 16000, 548–581.



Thimza: Stateless Threshold Signatures at Optimal Bandwidth

Thank you



https://github.com/navid-divan/thimza

thimza@googlegroups.com