

“Preview Writeup”: In anticipation of a package submission to the NIST Threshold Call

Title: TalonG and P-DualTS

Subtitle: Two-Round Lattice-based Threshold Signatures

Version: Preview Writeup 1.0 (2026-10-12)

Team name: Octopus

Team members: Man Ho Au, Robert H. Deng, Liming Gao, Bowen Jiang, Xianhui Lu, Tian Qiu, Guofeng Tang, Ruida Wang, Haiyang Xue, Guomin Yang, Chengru Zhang

Abstract: This document previews our proposals for the NIST Multi-Party Threshold Cryptography Call, specifying two lattice-based two-round threshold signature schemes supporting general t -out-of- n access structures.

First, we propose TalonG, a lattice-based threshold signature scheme designed for large-scale threshold settings, focusing on reducing per-party communication overhead. Second, we propose P-DualTS, a lattice-based threshold signature scheme optimized for small-party deployments, achieving compact public keys, short signatures, and efficient communication.

Both schemes are designed to provide post-quantum security based on standard lattice assumptions and target the Category S1: [Special] Signing category of the NIST Threshold Cryptography Call.

Proposed crypto-systems:

- (I) TalonG: t -out-of- n lattice-based threshold signature (Categories S1)
- (II) P-DualTS: t -out-of- n lattice-based threshold signature (Categories S1)

Keywords: Threshold Cryptography; NIST Threshold Call; Lattice-based Threshold Signatures



Preview writeup. This document is provided to NIST for online publication, to foster public awareness and support public discussion within the scope of the NIST First Call for Multi-Party Threshold Schemes [NIST-IR8214C]. This “preview writeup” represents a good-faith plan for a subsequent “package submission”. However, until the deadline for package submission, the team may still modify its own composition and the submission plan, including possible changes to the technical scope, and/or the used techniques or achieved results.

Team members: Man Ho Au ^{i1,a1}, Robert H. Deng ^{i2,a3}, Liming Gao ^{i3,a2*}, Bowen Jiang ^{i4,a3*}, Xianhui Lu ^{i5,a2}, Tian Qiu ^{i6,a4}, Guofeng Tang ^{i7,a3}, Ruida Wang ^{i8,a2}, Haiyang Xue ^{i9,a3}, Guomin Yang ^{i10,a3}, Chengru Zhang ^{i11,a5}

Open Researcher and Contributor Identifiers (ORCID):

i1 (0000-0003-2068-9530); i2 (0000-0003-3491-8146); i3 (0009-0004-0211-4148); i4 (0009-0002-8867-866X); i5 (0000-0001-7091-5810); i6 (0009-0006-2429-8771); i7 (0000-0002-0121-5471); i8 (0009-0002-1276-1299); i9 (0000-0002-0173-7894); i10 (0000-0002-4949-7738); i11 (0009-0001-8755-5206)

Affiliations:

^{a1} Department of Computing, The Hong Kong Polytechnic University, Hong Kong, China

^{a2} Institute of Information Engineering, Chinese Academy of Sciences, China

^{a3} SCIS, Singapore Management University, Singapore

^{a4} Digital Trust Centre, Nanyang Technological University, Singapore

^{a5} Ethereum Foundation, Switzerland

Associateship clarifications:

* Ph.D. student (non-employee).

Main contacts:

- **Team mailing list:** octopus_mptc@googlegroups.com
- **Primary technical contact person:** Liming Gao, gaoliming@iie.ac.cn
- **Secondary contact person 1:** Guofeng Tang, tang.guofeng789@gmail.com
- **Secondary contact person 2:** Haiyang Xue, haiyangxue@smu.edu.sg

Produced by humans. The team hereby confirms that the content in this preview writeup: (i) was produced by the team members, and (ii) was not produced by generative artificial intelligence (AI), with the possible exception of AI-proposed grammar improvements, minor integrated suggestions, or some well-identified and short localized portions of auxiliary content (e.g., some illustration); and (iii) was proofread by the team members.

1. Introduction

The scope of this preview document is to present our plan for submitting two lattice-based two-round threshold signature schemes supporting general t -out-of- n access structures.

We plan to propose two schemes: 1) TalonG [GTJLLWY26], a lattice-based threshold signature scheme designed for large-scale threshold settings, focusing on reducing per-party communication overhead; and 2) P-DualTS, a lattice-based threshold signature scheme optimized for small-party deployments, achieving compact public keys, short signatures, and low communication overhead.

Both submissions focus on post-quantum lattice-based threshold signatures and target Category S1: [Special] Signing of the NIST Threshold Call [NIST-IR8214C].

2. Specification

Organization. Our final submission will feature two lattice-based two-round threshold signature schemes, namely TalonG and P-DualTS, both supporting general t -out-of- n access structures, where any set of at least t parties can jointly produce a valid signature. The two schemes target different deployment scenarios. TalonG is designed for large-scale threshold settings and emphasizes low per-party communication, whereas P-DualTS is intended for small-scale settings and optimizes the overall efficiency in terms of public key size, signature size, and communication overhead.

TalonG, based on our previous work [GTJLLWY26], is a bandwidth-efficient two-round lattice-based threshold signature scheme designed for large-scale threshold settings (as large as 1024 parties). TalonG follows the Raccoon-like Fiat–Shamir framework and adopts techniques inspired by Raccoon and its threshold variants [PKPR24; PKMMPS24; EKT24; BKLMTT25], but its resulting threshold signatures are not directly interchangeable with standard Raccoon signatures.

P-DualTS is a two-round lattice-based threshold signature scheme designed for small-scale threshold settings, such as ≤ 16 parties. It includes the threshold profiles of Two (2), Three (3), Small (S) and part of Medium (M) as defined in Appendix C.3 in [NIST-IR8214C]. P-DualTS follows the ML-DSA-like Fiat–Shamir-with-rejection-sampling framework and adopts techniques from ML-DSA [Nat24] and recent threshold variants [DKLLSSS18; PN25; CPENP26], but its resulting threshold signatures are not directly interchangeable with standard ML-DSA signatures.

During key generation, a trusted dealer distributes secret-key shares using Shamir secret sharing in TalonG and replicated secret sharing in P-DualTS. The signing protocol consists of two interactive rounds, after which the partial signatures are combined into a publicly verifiable signature.

2.1. System model

The key generation of the proposed system follows the trusted-dealer model. A trusted dealer generates the master secret key, derives the public verification key, and distributes secret key

shares to the participating signers using Shamir secret sharing in TalonG, or using replicated secret sharing in P-DualTS.

The schemes support general t -out-of- n threshold configurations, where any set of at least t parties can jointly produce a valid signature. After the trusted setup phase, the signers execute a two-round interactive signing protocol over authenticated broadcast channels. The adversarial model allows a probabilistic polynomial-time adversary to statically corrupt up to $t - 1$ signers and obtain their secret key shares. It may additionally interact with the remaining honest parties through partial signing queries to obtain protocol messages with the objective of forging a valid threshold signature.

2.2. Key Idea

TalonG. Our aim is to construct a lattice-based threshold signature that runs in two rounds, the known minimum for this family, and scales to large committees ($t = 1024$) while keeping communication practical. At this scale, existing two-round lattice-based schemes require 275 and 618 KB of communication per party, respectively, making them impractical for large committees. TalonG reduces this to 26.9 KB per party.

The obstacle is structural. In the Fiat–Shamir paradigm, a signer publishes a commitment value w , derives a challenge $c = H(w\|msg)$, and responds with $\mathbf{z} = \mathbf{y} + sc$ mixing c into the secret key s . Security is argued by a simulator holding no key: it invents $(c, \mathbf{z}, \Delta)$, computes the $w = a\mathbf{z} - bc + \Delta$ that would have produced it, and programs the random oracle to return c on that input. This requires that w not be fixed before c is. Three-round protocols achieve this by hashing w_j in a first round and opening it in a second; deleting that round lets an adversary see the honest w_j and choose its own to influence the aggregate. Existing two-round schemes block this by having each signer send k candidate values $\{w_{j,i}\}_{i \in [k]}$ and combining them with random-oracle coefficients, so no one controls the result, but the proof forces k large, resulting in substantial communication overhead.

A cleaner route is a homomorphic trapdoor commitment: commit to w_j in round one, open in round two. The reduction then runs in trapdoor mode, committing to a value before the challenge is known and later opening it to whatever value is required by the simulation. The drawback is that the opening randomness must be included in the signature, and for standard lattice commitments it is bulky. TalonG keeps this idea and removes the cost, starting from the observation that *standard binding is more than the proof needs*. We allow the adversary without trapdoor to find pairs of distinct $(w^{(1)}, w^{(2)})$ such that $\text{Com}(w^{(1)}; \rho^{(1)}) = \text{Com}(w^{(2)}; \rho^{(2)})$ with distinct randomness $(\rho^{(1)}, \rho^{(2)})$, but neither $w^{(b)}$ can be expressed in the RLWE form $a\mathbf{z} - cb + \Delta$. This is exactly the type of collision produced by the forking lemma. Given two forgeries with different challenges, the reduction obtains

$$\text{Com}(a\mathbf{z}^{(1)} - c^{(1)}b + \Delta^{(1)}; \rho^{(1)}) = \text{Com}(a\mathbf{z}^{(2)} - c^{(2)}b + \Delta^{(2)}; \rho^{(2)}),$$

where both committed values have the required verification form. Such a collision can then be directly transformed into a short solution to the underlying lattice problem. Hence, the security proof only requires this restricted form of binding, which we call *semi-commitment*.

This weaker requirement enables a substantially more compact construction. Standard lattice-based commitments typically rely on trapdoors associated with wide matrices, whereas TalonG instead uses the compact NTRU-type trapdoor underlying Falcon: the commitment is $\tilde{w} = w + (r_1 + hr_2)$ for short randomness r_1, r_2 . The masking term $r_1 + hr_2$ provides statistical hiding, while equivocation can be performed using Falcon-style preimage sampling with the short basis for h . Thus, a commitment consists of a single ring element, and its opening consists of only two short polynomials. This allows each signer to broadcast a single polynomial in the first round, rather than k candidate commitments.

In the second round, the response shares are additionally masked by zero-sum terms, preventing the Lagrange coefficients used in the secret sharing from revealing individual secret shares. Two further techniques are important. First, the commitment key h is derived by hashing the message. This prevents the adversary from controlling the commitment key and allows the reduction to embed a trapdoor in h for signing queries while embedding the hard instance in the commitment key used for the forgery. Second, since part of $\tilde{w}$ is small, modulus switching allows the low-order information to be discarded, so that only the high-order bits need to be published. This further reduces both the signature and public-key sizes.

At 128-bit security with $t = 1024$, TalonG sends 26.9 KB per signer with a 2.0 KB public key, both the smallest among lattice-based threshold signatures, and signs in 140.7 ms against 2487.9 ms for the closest competitor on the same processor, roughly $18\times$, from the sharp drop in polynomial multiplications per round. The trade-offs are explicit: signatures are larger at 17.7 KB, though practical; both rounds run online, where the prior schemes precompute the first; and security additionally assumes NTRU. The semi-commitment is generic and should improve other trapdoor-commitment constructions.

P-DualTS. Our aim is to construct a lattice-based threshold signature that runs in two rounds and relies only on the standard MLWE and MSIS assumptions. Existing two-round schemes each incur additional costs to achieve this round complexity: two rely on stronger assumptions, namely AOM-MLWE or Hint-MLWE, with the latter reducing to standard MLWE only for sufficiently large Gaussian parameters, which in turn leads to larger concrete parameters, such as the modulus q . P-DualTS avoids these additional assumptions while substantially reducing the signature size and communication overhead, at the cost of restricting the protocol to small committees.

Our starting point is *dual simulation*, developed for two-round lattice multi-signatures. Security is argued by a simulator holding no secret key, so it must produce transcripts that look real. *Dual simulation* programs the random oracle to return an ephemeral matrix $\mathbf{B}$ for which there exists a short *dual* key $\mathbf{u}$ satisfying

$$[\mathbf{A} \mid \mathbf{I}] \mathbf{s} = [\mathbf{B} \mid \mathbf{I}] \mathbf{u},$$

and then swapping the roles of the two response components: the real $\mathbf{z} = \mathbf{y} + c\mathbf{s}$ is simulated as plain $\mathbf{y}$, while the real $\mathbf{r} = \mathbf{p}$ becomes $\mathbf{p} + c\mathbf{u}$. Both components are masked by rejection sampling rather than noise flooding, so signatures stay small, and no lattice trapdoor is needed anywhere.

Generalising this to a (t, n) threshold meets two obstacles. First, the simulator may need to simulate multiple honest parties simultaneously, up to $\min(t, n - t + 1)$ in a single signing session. Consequently, a single matrix $\mathbf{B}$ must admit a distinct short dual key $\mathbf{u}_i$ for each simulated party. Embedding a trapdoor in $\mathbf{B}$ could provide such dual keys, but requires $\mathbf{B}$ to have width

$l \approx 2m \log q$, substantially increasing the resulting parameter sizes. Second, rejection sampling requires each signer’s effective secret-key contribution to remain short. This is incompatible with Shamir secret sharing, since its Lagrange coefficients are taken modulo q and can be large, causing terms such as $y_i + c\lambda_i s_i$ to become too large for the rejection-sampling procedure to remain effective.

We resolve the first obstacle with *parallel-dual simulation*: rather than sampling each $\mathbf{u}_i$ through a trapdoor, we construct $\mathbf{B}$ and the $\mathbf{u}_i$ together by design. Each dual key takes the shape $\mathbf{u}_i = [\mathbf{e}_i^T \mid \mathbf{u}_{i,1}^T \mid \mathbf{u}_{i,2}^T]^T$ with $\mathbf{e}_i$ a canonical basis vector, and setting $\hat{\mathbf{B}}_1$ uniform with $\hat{\mathbf{B}}_0 = [\mathbf{b}_1 \mid \cdots \mid \mathbf{b}_t] - \hat{\mathbf{B}}_1 \mathbf{U}_1 - \mathbf{U}_2$. Then, $\mathbf{B} = [\hat{\mathbf{B}}_0 \mid \hat{\mathbf{B}}_1]$ is a valid dual matrix for every active party simultaneously, and its pseudorandomness following from MLWE applied to $\hat{\mathbf{B}}_1 \mathbf{U}_1 + \mathbf{U}_2$. This widens $\mathbf{B}$ by only t columns.

The second obstacle we resolve with replicated secret sharing: the dealer issues $\binom{n}{t-1}$ short vectors, each signer holds those indexed by subsets containing it, and reconstruction partitions them so each is contributed exactly once with coefficient 1. Since each $\mathbf{u}_i$ is zero in most of its leading coordinates, its mask can be too; mirroring that sparsity in the real protocol leaves only $m + k + 1$ non-zero entries to transmit, making per-party communication constant in t . Since $\mathbf{B}$ is built from the public key shares, which under replicated sharing depend on who is signing, we hash a salt derived from the active set into $\mathbf{B}$ and include it in the signature, preserving the binding while keeping verification independent of who signed.

At 128-bit security with $(t, n) = (5, 8)$, P-DualTS gives public keys of 1.72 KB, signatures of 7.67 KB, per-party communication of 10.72 KB, and per-party signing below 7 ms. That is an order of magnitude less communication than the One-More and Hint-based schemes and roughly half that of the NTRU-based one, with a much smaller modulus ($q \approx 2^{28}$ against $q > 2^{40}$). The trade-offs are explicit: both rounds run online like TalonG; signing is slower than TalonG, the price of dropping NTRU assumption; and the $\binom{n}{t-1}$ term confines the protocol to roughly $n \leq 16$, which covers the “two”, “three” and “small”-party profiles of NIST’s call.

2.3. Security

The security of TalonG is based on the hardness of the RLWE, RSIS and decisional NTRU problems, while the security of P-DualTS is based on the hardness of the MLWE and MSIS problems. Under these standard lattice assumptions, the schemes achieve correctness and selective existential unforgeability under chosen-message attacks in the random oracle model. More specifically, the security model allows an adversary to corrupt up to $t - 1$ parties, with the set of corrupted signers fixed before the adversary interacts with the signing oracle. We leave adaptive corruption as an interesting direction for future work. The current constructions provide security-with-abort rather than robustness.

The recommended parameter set targets NIST Security Category 1 (approximately 128-bit post-quantum security).

3. Open-Source Implementation

Code structure: The preliminary proof-of-concept implementation of both TalonG and P-DualTS is developed in Go for our research papers. The implementation adopts a modular design, including key generation, two-round partial signing, signature combination, signature verification, parameter configuration, and benchmarking. The two schemes share a common implementation framework, differing mainly in the parameter sets and the key-generation/secret-sharing module.

In the submission, we plan to update our code according to the requirements of NIST Threshold call [NIST-IR8214C].

Code progress and availability: A proof-of-concept implementation is already available through an anonymous public Git-compatible repository: <https://anonymous.4open.science/r/P-DualTS-4650/>. An optimized implementation supporting both TalonG and P-DualTS will be released with the final submission.

Implementation of the networking model: The current implementation targets a local deployment model in which all participating signers are executed on a single machine. Each signer maintains its own local state, and protocol messages are exchanged through local program interfaces. This implementation is intended to evaluate the local computational cost of each participant independently of network latency. We will update accordingly in the submission.

Testing: The current implementation provides correctness tests for the core algorithms and evaluates the performance under different threshold parameters.

Performance: Our preliminary experimental results demonstrate that both TalonG and P-DualTS achieve practical signing performance while maintaining competitive communication and signature efficiency. The final submission will include detailed benchmark results and comparisons with representative lattice-based threshold signature schemes.

4. Licensing and Patent Claims

1. The reference implementation of both TalonG and P-DualTS will be released under the Apache License 2.0.
2. We disclose one pending Chinese patent application that may cover part of the techniques underlying the proposed submission:
 - **Low-Communication Threshold Signature Method and System Based on Classical Lattice Hardness Assumptions**, Chinese Patent Application No. 2025115061877, applicant: Institute of Information Engineering, Chinese Academy of Sciences.

Table 1: **Comparison of lattice-based threshold signatures.** R denotes the number of rounds. $|\text{sig}|$ and $|\text{vk}|$ represent signature and public key sizes in kilobytes (KB), respectively. “Comm.” denotes per-party communication costs in KB. n denotes the number of parties, and t is the threshold value. “EKT-s” means small-scale EKT, and similar examples include “Ringtail-s” and “TalonG-s”.

Scheme	R	$ \text{sig} $	$ \text{vk} $	Comm.	n	Assumptions
ENP24 [ENP24]	4	12.3	12.8	364	16	RLWE, RSIS
TRaccoon [PKMMPS24]	3	12.7	3.9	40.8	1024	Hint-MLWE, MSIS
Finally! [PN25]	3	2.7	2.6	7.5	8	MLWE, MSIS
CPENP26[CPENP26]	6	2.4	1.3	$21 \sim 1005$	6	MLWE, MSIS
GKS24 [GKS24]	2	46	13	3072	5	RLWE, RSIS
CATZ24 [CTZ24]	2	258	47	1526	5	MSIS
EKT [EKT24]	2	10.8	5.5	276.1	1024	AOM-MLWE
Ringtail [BKLM25]	2	13.4	4.5	612.8	1024	Hint-MLWE, MSIS
TalonG [GTJLLWY26]	2	17.7	2.0	26.9	1024	Hint-RLWE, RSIS, NTRU
Hermine [BCDEKNPT26]	2	11.0	2.8	71.5	64	AOM-MISIS, MSIS
EKT-s [EKT24]	2	8.6	4.5	254.4	8	AOM-MLWE
Ringtail-s [BKLM25]	2	11.7	3.0	523.7	8	Hint-MLWE, MSIS
TalonG-s [GTJLLWY26]	2	15.1	1.3	26.0	8	Hint-RLWE, RSIS, NTRU
P-DualTS	2	$6.11 + 0.31t$	1.7	10.72	8	MLWE, MSIS

5. Comparison

Table 1 compares TalonG and P-DualTS with other lattice-based threshold signature schemes in terms of the number of rounds, signature size, public key size, per-party communication, and security assumptions.

TalonG is designed for large-scale threshold signing, where minimizing per-party communication is particularly important. For $n = 1024$, TalonG requires only 26.9 KB of communication per party, substantially less than EKT (276.1 KB) and Ringtail (612.8 KB), while maintaining a public key size of 2.0 KB. Its communication cost remains nearly unchanged in the small-scale configuration, demonstrating that its communication efficiency is largely independent of the number of parties. Although TalonG has larger signatures than EKT and Ringtail, it offers a favorable trade-off between signature size and communication overhead.

P-DualTS targets small-party deployments and prioritizes compact signatures and efficient communication. For $(t, n) = (5, 8)$, it achieves a public key size of approximately 1.7 KB and per-party communication of 10.72 KB, both substantially smaller than those of EKT-s, Ringtail-s, and TalonG-s. Its signature size is $6.11 + 0.31t$ KB, yielding 7.66 KB at $t = 5$, which is also considerably smaller than the signatures of these three small-scale configurations. Compared with Finally!, a three-round scheme with a 2.7 KB signature and 7.5 KB communication cost, P-DualTS reduces the number of signing rounds to two while maintaining competitive signature and communication sizes. These results make P-DualTS an attractive option for deployments where low interaction, compact signatures, and communication efficiency are all important.

References

- [BCDEKNPT26]** Giacomo Borin, Sofía Celi, Rafael Del Pino, Thomas Espitau, Shuichi Katsumata, Guilhem Niot, Thomas Prest, and Kaoru Takemure. “Hermine: An Efficient Lattice-based FROST-like Threshold Signature”. In: *Advances in Cryptology – ASIACRYPT 2026*. 2026. URL: <https://eprint.iacr.org/2026/419>.
- [BKLMTT25]** Cecilia Boschini, Darya Kaviani, Russell W. F. Lai, Giulio Malavolta, Akira Takahashi, and Mehdi Tibouchi. “Ringtail: Practical Two-Round Threshold Signatures from Learning with Errors”. In: *IEEE Symposium on Security and Privacy, SP 2025, San Francisco, CA, USA, May 12-15, 2025*. IEEE, 2025, pp. 149–164. DOI: [10.1109/SP61157.2025.00070](https://doi.org/10.1109/SP61157.2025.00070). URL: <https://eprint.iacr.org/2024/1113>.
- [CPENP26]** Sofia Celi, Rafael del Pino, Thomas Espitau, Guilhem Niot, and Thomas Prest. “Efficient Threshold ML-DSA”. In: *Proceedings of the 35th USENIX Security Symposium (USENIX Security '26)*. USENIX Association, 2026. URL: <https://www.usenix.org/conference/usenixsecurity26/presentation/celi>.
- [CTZ24]** Rutchathon Chairattana-Apirom, Stefano Tessaro, and Chenzhi Zhu. “Partially Non-interactive Two-Round Lattice-Based Threshold Signatures”. In: *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part IV*. Vol. 15487. Lecture Notes in Computer Science. Springer, 2024, pp. 268–302. DOI: [10.1007/978-981-96-0894-2_9](https://doi.org/10.1007/978-981-96-0894-2_9). URL: <https://eprint.iacr.org/2024/467>.
- [DKLLSSS18]** Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. “CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2018.1 (2018), pp. 238–268. DOI: <https://doi.org/10.13154/tches.v2018.i1.238-268>. URL: <https://pq-crystals.org/dilithium/>.
- [EKT24]** Thomas Espitau, Shuichi Katsumata, and Kaoru Takemure. “Two-Round Threshold Signature from Algebraic One-More Learning with Errors”. In: *Advances in Cryptology – CRYPTO 2024*. Vol. 14926. Lecture Notes in Computer Science. Cham: Springer Nature Switzerland, 2024, pp. 387–424. DOI: [10.1007/978-3-031-68394-7_13](https://doi.org/10.1007/978-3-031-68394-7_13). URL: <https://eprint.iacr.org/2024/496>.
- [ENP24]** Thomas Espitau, Guilhem Niot, and Thomas Prest. “Flood and Submerge: Distributed Key Generation and Robust Threshold Signature from Lattices”. In: *Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part VII*. Vol. 14926. Lecture Notes in Computer Science. Springer, 2024, pp. 425–458. DOI: [10.1007/978-3-031-68394-7_14](https://doi.org/10.1007/978-3-031-68394-7_14). URL: <https://eprint.iacr.org/2024/959>.
- [GKS24]** Kamil Doruk Gur, Jonathan Katz, and Tjerand Silde. “Two-Round Threshold Lattice-Based Signatures from Threshold Homomorphic Encryption”. In: *Post-Quantum Cryptography*. Cham: Springer Nature Switzerland, 2024, pp. 266–300. DOI: [10.1007/978-3-031-62746-0_12](https://doi.org/10.1007/978-3-031-62746-0_12). URL: <https://eprint.iacr.org/2023/1318>.

[GTJLLWY26] Liming Gao, Guofeng Tang, Dingding Jia, Yijian Liu, Bingqian Liu, Xianhui Lu, Kunpeng Wang, and Yongjian Yin. “TalonG: Bandwidth-Efficient Two-Round Threshold Signatures from Lattices”. In: *Advances in Cryptology – EUROCRYPT 2026*. Ed. by Joan Daemen and Emmanuel Thomé. Vol. 16541. Lecture Notes in Computer Science. Cham: Springer Nature Switzerland, 2026, pp. 94–123. DOI: [10.1007/978-3-032-25291-3_4](https://doi.org/10.1007/978-3-032-25291-3_4). URL: <https://eprint.iacr.org/2026/303>.

[Nat24] National Institute of Standards and Technology. *Module-Lattice-Based Digital Signature Standard*. Tech. rep. FIPS 204. National Institute of Standards and Technology, 2024. DOI: [10.6028/NIST.FIPS.204](https://doi.org/10.6028/NIST.FIPS.204).

[PKMMPS24] Rafael del Pino, Shuichi Katsumata, Mary Maller, Fabrice Mouhartem, Thomas Prest, and Markku-Juhani Saarinen. “Threshold Raccoon: Practical Threshold Signatures from Standard Lattice Assumptions”. In: *Advances in Cryptology – EUROCRYPT 2024*. Ed. by Marc Joye and Gregor Leander. Vol. 14652. Lecture Notes in Computer Science. Cham: Springer Nature Switzerland, 2024, pp. 219–248. DOI: [10.1007/978-3-031-58723-8_8](https://doi.org/10.1007/978-3-031-58723-8_8). URL: <https://eprint.iacr.org/2024/184>.

[PKPR24] Rafaël del Pino, Shuichi Katsumata, Thomas Prest, and Mélissa Rossi. “Raccoon: A Masking-Friendly Signature Proven in the Probing Model”. In: *Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part I*. Vol. 14920. Lecture Notes in Computer Science. Springer, 2024, pp. 409–444. DOI: [10.1007/978-3-031-68376-3_13](https://doi.org/10.1007/978-3-031-68376-3_13). URL: <https://eprint.iacr.org/2024/1291>.

[PN25] Rafael del Pino and Guilhem Niot. “Finally! A Compact Lattice-Based Threshold Signature”. In: *Public-Key Cryptography – PKC 2025*. Ed. by Tibor Jager and Jiaxin Pan. Vol. 15676. Lecture Notes in Computer Science. Cham: Springer Nature Switzerland, 2025, pp. 169–199. DOI: [10.1007/978-3-031-91826-1_6](https://doi.org/10.1007/978-3-031-91826-1_6). URL: <https://eprint.iacr.org/2025/872>.

[NIST-IR8214C] Luís T. A. N. Brandão and René Peralta. *NIST First Call for Multi-Party Threshold Schemes*. (National Institute of Standards and Technology) NIST Internal Report (NISTIR) 8214C. 2026. DOI: [10.6028/NIST.IR.8214C](https://doi.org/10.6028/NIST.IR.8214C).