

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

Title: Pilaf: Fully Tight Two-Round Threshold Signatures

Subtitle: Adaptive, Pairing-Free Threshold Signing from MDDH

Version: Preview Writeup 0.1 (2026-08-07)¹

Team name: Pilaf

Team members: Chen Qian, Xingyu Zhao, Hao Cheng, Zengpeng Li, Puwen Wei, Quan Yuan

Abstract: Pilaf is a pairing-free, two-round threshold Schnorr-type signature scheme designed to combine practical signing with fully tight adaptive security. It distributes a signing key among N parties so that any subset of at least t parties can jointly produce a compact, publicly verifiable signature, while fewer than t parties cannot forge. Pilaf’s message-independent first round can be generated offline, before the message to be signed is known. To address the resulting challenge of adaptive corruptions, the scheme uses a linearly homomorphic dual-mode commitment with targetable openings and a profile-wise zero-sum masking mechanism with posterior completion. These mechanisms allow a security simulator to explain previously published commitments and reveal local randomness consistently when parties are corrupted after participating in earlier sessions. Pilaf supports concurrent signing sessions, adaptively chosen messages and signer sets, and corruption of up to $t - 1$ parties. Its security is proved in the random-oracle model under the Matrix Diffie-Hellman assumption, without bilinear pairings or the algebraic group model, and the reduction incurs only constant loss.

Proposed crypto-systems: Threshold Signatures (Category S1).

Keywords: Threshold Cryptography; NIST Threshold Call; Schnorr Signatures; Tightness; Adaptive Security

¹Preliminary version submitted to NIST-MPTC for review

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: Chen Qian^{i1,a1}, Xingyu Zhao^{i2,a1}, Hao Cheng^{i3,a1}, Zengpeng Li^{i4,a1}, Puwen Wei^{i5,a1}, Quan Yuan^{i6,a1}

Open Researcher and Contributor Identifiers (ORCID):

i1 (0000-0003-4429-7267); i2 (0009-0002-4650-6616); i3 (0009-0004-4802-6370); i4 (0000-0003-0758-7230); i5 (0000-0003-3978-4183); i6 (0000-0001-8367-389X)

Affiliations: ^{a1} School of Cyber Science and Technology, Shandong University, Qingdao, China

Main contacts:

- **Team mailing list:** pilaf@googlegroups.com
- **Primary technical contact person:** Chen Qian, chen.qian@sdu.edu.cn

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

Pilaf is a two-round threshold Schnorr-type signature scheme with fully tight adaptive security, submitted to Category S1 of the NIST Threshold Call [NIST-IR8214C]. Threshold signatures grew out of Desmedt’s proposal to distribute signing authority and Desmedt–Frankel’s threshold cryptosystems [Des90; DF90]; they distribute a signing key among N parties so that any subset of at least t parties can jointly produce a valid signature, while fewer than t parties cannot forge signatures. Modern definitions model dynamically selected signer sets and malicious leaders [BCKMTZ22]; fully adaptive security further allows corruptions to depend on earlier protocol transcripts [CKM23]. Threshold Schnorr signatures have a linear structure that is particularly suitable for thresholdization: signers can locally generate signature shares that aggregate into a compact signature while preserving the public verification interface of the underlying Schnorr primitive [KG20].

The primary design goal of Pilaf is to combine two-round signing, offline preprocessing, adaptive-corruption security, and fully tight concrete security in a single pairing-free construction. Existing work covers these ingredients separately, but not their exact combination under Pilaf’s model and assumptions. FROST provides practical two-round signing with offline preprocessing, but is analyzed against static corruptions [KG20]. Fully adaptive FROST-style analyses include Sparkle+, HARTS, FaFROST, and ms-FROST. These analyses rely on the AGM and/or OMDL/AOMDL-type assumptions; HARTS additionally targets robustness under a distinct threshold model [CKM23; BLSW24; BGCRSY25; BCLTZ26]. Under standard pairing-free assumptions, Twinkle, Glacius, Gargos, and Rackle require at least three signing rounds, whereas the two-round Dazzle and Gerhart et al. constructions have non-tight reductions; the latter additionally assumes bounded signing between public-key refreshes [BLTWZ24; BDLR25b; BDLR25a; NRT26; Che25; GCRS26]. Chen’s partially non-interactive construction likewise has query-dependent security loss [Che26]. Fully tight alternatives include the three-round Dazzle-T and Twinkle-T, the higher-round Glitter, and the two-round but statically secure Earpicks [Che25; BW26; TJZ25; BC26]. Pilaf targets the remaining combination while staying pairing-free and relying only on the Matrix Diffie-Hellman assumption in the random-oracle model [EHKRV13].

In a two-round threshold signing protocol, the first-round messages are generated before the message is known and may be preprocessed offline [KG20; BCKMTZ22]. This creates a fundamental difficulty for adaptive security: if a signer is corrupted after first-round messages have appeared in previous transcripts, the simulator must reveal local randomness that is consistent with those already published messages. The construction relies on a linearly homomorphic dual-mode commitment with targetable opening, which allows the proof to explain first-round commitments after the Fiat-Shamir challenge and the relevant aggregate target are known. It also uses a profile-wise zero-sum masking mechanism with posterior completion, which ensures that later corruptions reveal local randomness distributed consistently with previously published transcripts.

By providing a complete specification, reference implementation, and experimental evaluation of such a two-round adaptively secure and fully tight threshold signature scheme, the planned package contributes to the Threshold Call’s goal of building a public body of reference material for threshold cryptography.

2. Specification

2.1. System Model

The system consists of N parties and a threshold parameter t , where $1 \leq t \leq N$. Any signer set S of size $|S| \geq t$ can jointly produce a valid signature under a common aggregate verification key, whereas any signer set of size $|S| < t$ cannot forge signatures.

The signing protocol consists of two rounds. In the first round, each signer independently generates a message-independent preprocessing message and stores the corresponding local state. These first-round messages can be generated before the message to be signed is known. In the second round, after the message and the complete first-round transcript are fixed, each signer produces a signature share. Any party acting as a combiner may aggregate t valid second-round shares into a publicly verifiable signature.

2.2. Proposed Cryptosystem

The Pilaf threshold signature scheme is defined as $\text{Pilaf} = (\text{Setup}, \text{KGen}, \text{Sig}_0, \text{Sig}_1, \text{SAgg}, \text{Ver})$.

- **Setup** $\text{Setup}(1^\lambda)$. The setup algorithm takes as input the security parameter λ and outputs public parameters pp for the linear function family, commitment scheme, and masking scheme.
- **KGen** $\text{KGen}(N, t)$. The dealer uses Shamir secret sharing with threshold t to distribute x among the N parties. Signers P_ℓ receive shares x_ℓ of the signing key x , and the aggregate verification key is $\text{vk}_\Sigma := F(x)$. Any t shares reconstruct x through Lagrange interpolation. In addition to the signing-key shares, the dealer generates pairwise masking seeds for the parties. Each party receives only the seeds needed to compute its own masks. These seeds are used to derive correlated random values whose weighted sum is zero for every signing set. The local secret key of P_ℓ therefore consists of its Shamir share and its masking seeds. The aggregate verification key vk_Σ is public.
- **Sig₀** $\text{Sig}_0(\text{vk}_\Sigma, \ell, \text{id}, \text{sk}_\ell, S, m)$. This round is independent of m and can therefore be preprocessed offline. Signer P_ℓ samples $a_{\ell,0}$ and sets $a_{\ell,1} := x_\ell - a_{\ell,0}$. For each branch $b \in \{0, 1\}$, it derives commitment keys from $H(\text{vk}_\Sigma, \text{id})$, samples a nonce preimage $z_{\ell,b}$, and computes $X_{\ell,b} := F(a_{\ell,b})$ and $R_{\ell,b} := F(z_{\ell,b})$. It commits separately to $X_{\ell,b}$ and $R_{\ell,b}$, masks the resulting commitment pair using the first-round masks for (id, S, b) , and returns the two masked branch commitments together with local state st_ℓ .
- **Sig₁** $\text{Sig}_1(\text{vk}_\Sigma, \ell, \text{id}, \text{st}_\ell, \{m_i\}_{i \in S}, S, m)$. After the message and complete first-round transcript are known, each signer aggregates the first-round commitments $c_b = (x_b, r_b)$ using the Lagrange coefficients. Because the first-round masks have a weighted sum of zero, this produces a common pair of aggregate commitments for each branch. The signer then computes a Fiat-Shamir challenge $h := H(\text{vk}_\Sigma, x_0, r_0, x_1, r_1, \text{id}, S, m)$. P_ℓ computes its second-round signature share for each branch b as $\rho_{\ell,b} := z_{\ell,b} + h \cdot a_{\ell,b}$, where $z_{\ell,b}$ is the nonce used in the first round. Before these values are released, they are masked using fresh masks derived from the complete second-round transcript. In particular, the masking

context contains the first-round transcript supplied to the signer. This ensures that the second-round share is bound to the exact first-round transcript on which it was computed.

- **S_{Agg}** $\text{SAgg}(\text{vk}_\Sigma, \{\sigma_i\}_{i \in S}, id, S, m)$. The aggregator first checks that all shares contain the same c_b for each branch. It then aggregates the branch values X_b , nonce values R_b , responses ρ_b , and commitment openings ω_b using the Lagrange coefficients. The second-round masks cancel, yielding the aggregate signature $\sigma_\Sigma = \{X_b, R_b, \rho_b, \omega_b, c_b\}_{b \in \{0,1\}}$.
- **V_{er}** $\text{Ver}(\text{vk}_\Sigma, id, S, m, \sigma_\Sigma)$. The verification algorithm checks the validity of the aggregated signature against the aggregate verification key. The verifier parses $c_b = (x_b, r_b)$, derives the commitment keys from $H(\text{vk}_\Sigma, id)$, and recomputes $h := \text{HH}(\text{vk}_\Sigma, x_0, r_0, x_1, r_1, id, S, m)$. It checks $X_0 + X_1 = \text{vk}_\Sigma$ and, for each branch b , verifies the Schnorr relation $R_b = F(\rho_b) + X_b h$ and the openings of both commitments x_b and r_b .

2.3. Security

- **Underlying assumptions.** The concrete Pilaf instantiation is pairing-free and is proved secure in the random-oracle model (ROM). Security relies on the Matrix Diffie-Hellman assumption for indistinguishability between the two modes and on the MDDH-based properties of the underlying linear function family. The construction does not rely on bilinear pairings, the algebraic group model, or any other non-standard assumptions.
- **Fully tight security.** For the final forgery, the hidden branch has not been exposed. The reduction can therefore select this branch with only a constant loss and switch its commitments to binding mode. A valid forgery must then satisfy the extracted relation $R^* = F(\rho^*) + Xh$, which contradicts the lossy soundness of the underlying linear function family except with the stated error probability.
- **Adaptive security.** Pilaf is secure against an adaptive adversary that may run multiple signing sessions concurrently, choose the messages and signer sets, request signature shares, and corrupt up to $t - 1$ parties during the execution. When a party is corrupted, the adversary obtains its secret-key share and all local state from previous signing sessions, including the randomness used in the first and second rounds. The dual-mode commitment allows the simulator to produce openings consistent with the challenge after the first-round transcript has already been fixed.

3. Open-Source Implementation

Since the current preview focuses on the cryptographic specification and security claims, the experimental evaluation is preliminary and the implementation is not yet fully open-source. The final submission package will include an open-source reference implementation and a systematic experimental report, following the NIST Threshold Call requirements. The evaluation will measure per-party communication, round complexity, signing latency, verification cost, and the overhead introduced by the dual-mode commitment, masking mechanism, and dual-branch signing structure.

We will benchmark representative threshold configurations and compare the implementation with existing two or three round threshold schemes.

4. Licensing, Patent Claims, and Funding

1. A Chinese invention patent application (application no. 202611078393.7), concerning an adaptively secure two-round threshold signature method and system with fully tight security, was filed with and accepted for processing by the China National Intellectual Property Administration on July 20, 2026. The applicant is Shandong University, and Chen Qian and Xingyu Zhao are named as the inventors. The application relates to the Pilaf scheme and is currently pending. It is intended for defensive purposes only and is not intended to restrict the free use of the scheme by any entity.
2. The research that led to the scheme was supported by the National Natural Science Foundation of China (Grant 62302272), the Shandong Provincial Outstanding Young Scientists Fund (Overseas) (Grant 2024HWYQ-013), the National Natural Science Foundation of China (Grant 62472255), and the National Key Research and Development Program of China (Grant 2022YFE0114300).

References

- [BC26]** Renas Bacho and Yanbo Chen. “Earpicks: Tightly Secure Two-Round Multi and Threshold Signatures”. In: *Advances in Cryptology—EUROCRYPT 2026, Part I*. Vol. 16541. Lecture Notes in Computer Science. Springer, 2026, pp. 154–183. DOI: [10.1007/978-3-032-25291-3_6](https://doi.org/10.1007/978-3-032-25291-3_6).
- [BCKMTZ22]** Mihir Bellare, Elizabeth C. Crites, Chelsea Komlo, Mary Maller, Stefano Tessaro, and Chenzhi Zhu. “Better than Advertised Security for Non-Interactive Threshold Signatures”. In: *Advances in Cryptology—CRYPTO 2022, Part IV*. Vol. 13510. Lecture Notes in Computer Science. Springer, 2022, pp. 517–550. DOI: [10.1007/978-3-031-15985-5_18](https://doi.org/10.1007/978-3-031-15985-5_18).
- [BCLTZ26]** Renas Bacho, Yanbo Chen, Julian Loss, Stefano Tessaro, and Chenzhi Zhu. “Adaptively Secure Partially Non-Interactive Threshold Schnorr Signatures in the AGM”. In: *Advances in Cryptology—EUROCRYPT 2026, Part I*. Vol. 16541. Lecture Notes in Computer Science. Springer, 2026, pp. 33–62. DOI: [10.1007/978-3-032-25291-3_2](https://doi.org/10.1007/978-3-032-25291-3_2).
- [BDLR25a]** Renas Bacho, Sourav Das, Julian Loss, and Ling Ren. “Adaptively Secure Three-Round Threshold Schnorr Signatures from DDH”. In: *Advances in Cryptology—CRYPTO 2025, Part VI*. Vol. 16005. Lecture Notes in Computer Science. Springer, 2025, pp. 390–422. DOI: [10.1007/978-3-032-01887-8_13](https://doi.org/10.1007/978-3-032-01887-8_13).
- [BDLR25b]** Renas Bacho, Sourav Das, Julian Loss, and Ling Ren. “Glacius: Threshold Schnorr Signatures from DDH with Full Adaptive Security”. In: *Advances in Cryptology—EUROCRYPT 2025, Part II*. Vol. 15602. Lecture Notes in Computer Science. Springer, 2025, pp. 304–334. DOI: [10.1007/978-3-031-91124-8_11](https://doi.org/10.1007/978-3-031-91124-8_11).
- [BGCRSY25]** Ruben Baecker, Paul Gerhart, Davide Li Calsi, Luigi Russo, Dominique Schröder, and Arkady Yerukhimovich. *Fully Adaptive FROST in the Algebraic Group Model From Falsifiable Assumptions*. Cryptology ePrint Archive, Paper 2025/1950. 2025. URL: <https://eprint.iacr.org/2025/1950>.
- [BLSW24]** Renas Bacho, Julian Loss, Gilad Stern, and Benedikt Wagner. “HARTS: High-Threshold, Adaptively Secure, and Robust Threshold Schnorr Signatures”. In: *Advances in Cryptology—ASIACRYPT 2024, Part III*. Vol. 15486. Lecture Notes in Computer Science. Springer, 2024, pp. 104–140. DOI: [10.1007/978-981-96-0891-1_4](https://doi.org/10.1007/978-981-96-0891-1_4).
- [BLTWZ24]** Renas Bacho, Julian Loss, Stefano Tessaro, Benedikt Wagner, and Chenzhi Zhu. “Twinkle: Threshold Signatures from DDH with Full Adaptive Security”. In: *Advances in Cryptology—EUROCRYPT 2024, Part I*. Vol. 14651. Lecture Notes in Computer Science. Springer, 2024, pp. 429–459. DOI: [10.1007/978-3-031-58716-0_15](https://doi.org/10.1007/978-3-031-58716-0_15).
- [BW26]** Renas Bacho and Benedikt Wagner. “Tightly Secure Threshold Signatures over Pairing-Free Groups”. In: *IACR Communications in Cryptology* 2.4 (2026), p. 8. DOI: [10.62056/ay73z10k](https://doi.org/10.62056/ay73z10k).

- [Che25]** Yanbo Chen. “Dazzle: Improved Adaptive Threshold Signatures from DDH”. In: *Public-Key Cryptography—PKC 2025, Part III*. Vol. 15676. Lecture Notes in Computer Science. Springer, 2025, pp. 233–261. DOI: [10.1007/978-3-031-91826-1_8](https://doi.org/10.1007/978-3-031-91826-1_8).
- [Che26]** Yanbo Chen. *Partially Non-Interactive Two-Round Threshold and Multi-Signatures with Tighter and Adaptive Security*. Cryptology ePrint Archive, Paper 2026/373. 2026. URL: <https://eprint.iacr.org/2026/373>.
- [CKM23]** Elizabeth Crites, Chelsea Komlo, and Mary Maller. “Fully Adaptive Schnorr Threshold Signatures”. In: *Advances in Cryptology—CRYPTO 2023, Part I*. Vol. 14081. Lecture Notes in Computer Science. Springer, 2023, pp. 678–709. DOI: [10.1007/978-3-031-38557-5_22](https://doi.org/10.1007/978-3-031-38557-5_22).
- [Des90]** Yvo Desmedt. “Abuses in Cryptography and How to Fight Them”. In: *Advances in Cryptology—CRYPTO ’88*. Vol. 403. Lecture Notes in Computer Science. Springer, 1990, pp. 375–389. DOI: [10.1007/0-387-34799-2_29](https://doi.org/10.1007/0-387-34799-2_29).
- [DF90]** Yvo Desmedt and Yair Frankel. “Threshold Cryptosystems”. In: *Advances in Cryptology—CRYPTO ’89*. Vol. 435. Lecture Notes in Computer Science. Springer, 1990, pp. 307–315. DOI: [10.1007/0-387-34805-0_28](https://doi.org/10.1007/0-387-34805-0_28).
- [EHKRV13]** Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Villar. “An Algebraic Framework for Diffie–Hellman Assumptions”. In: *Advances in Cryptology—CRYPTO 2013, Part II*. Vol. 8043. Lecture Notes in Computer Science. Springer, 2013, pp. 129–147. DOI: [10.1007/978-3-642-40084-1_8](https://doi.org/10.1007/978-3-642-40084-1_8).
- [GCRS26]** Paul Gerhart, Davide Li Calsi, Luigi Russo, and Dominique Schröder. “Fully-Adaptive Two-Round Threshold Schnorr Signatures from DDH”. In: *Advances in Cryptology—EUROCRYPT 2026, Part II*. Vol. 16542. Lecture Notes in Computer Science. Springer, 2026, pp. 251–283. DOI: [10.1007/978-3-032-25317-0_9](https://doi.org/10.1007/978-3-032-25317-0_9).
- [KG20]** Chelsea Komlo and Ian Goldberg. “FROST: Flexible Round-Optimized Schnorr Threshold Signatures”. In: *Selected Areas in Cryptography—SAC 2020*. Vol. 12804. Lecture Notes in Computer Science. Springer, 2020, pp. 34–65. DOI: [10.1007/978-3-030-81652-0_2](https://doi.org/10.1007/978-3-030-81652-0_2).
- [NRT26]** Guilhem Niot, Michael Reichle, and Kaoru Takemure. “Adaptively-Secure Three-Round Threshold Schnorr from DL”. In: *Advances in Cryptology—EUROCRYPT 2026, Part I*. Vol. 16541. Lecture Notes in Computer Science. Springer, 2026, pp. 3–32. DOI: [10.1007/978-3-032-25291-3_1](https://doi.org/10.1007/978-3-032-25291-3_1).
- [TJZ25]** Shaolong Tang, Peng Jiang, and Liehuang Zhu. “Glitter: A Fully Adaptive and Tightly Secure Threshold Signature”. In: *Information Security and Privacy—ACISP 2025, Part I*. Vol. 15658. Lecture Notes in Computer Science. Springer, 2025, pp. 184–204. DOI: [10.1007/978-981-96-9095-4_10](https://doi.org/10.1007/978-981-96-9095-4_10).
- [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).