

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

Title: Threshold Signatures in the Head (TSitH)

Subtitle: A framework for threshold MPC-in-the-Head signatures

Version: Preview Writeup 0.1 (2026-07-30)¹

Team name: TSitH team

Team members: Thibauld Feneuil, Matthieu Rivain, Damien Vergnaud, Auguste Warmé-Janville

Abstract: This submission specifies a family of threshold signature schemes based on the MPC-in-the-Head paradigm with threshold-friendly Merkle-tree commitments. It builds on the recent Threshold-Signatures-in-the-Head (TSitH) framework which enables the construction of threshold signatures from a broad class of one-way functions.

The submission includes three concrete instantiations of the framework, based respectively on the block cipher AES, the multivariate quadratic problem (MQ), and the syndrome decoding problem (SD). These variants are intended to provide plausibly post-quantum security: no efficient quantum or classical attacks are known against the underlying symmetric primitives used in the MPC-in-the-Head construction, nor against the hard problems on which the three instantiations rely.

The TSitH framework was introduced as a preprint in mid-2026. The present submission aims to develop that framework into concrete threshold signature schemes suitable for consideration in the NIST MPTC process. These schemes combine techniques from hash-based proof systems (MPC-in-the-Head with Merkle tree commitments) and generic secure multiparty computation in order to obtain practical threshold signatures schemes based on various security assumptions.

Proposed crypto-systems: (I) TSitH: A framework for threshold signatures (Categories S1).

Keywords: Threshold Cryptography; NIST Threshold Call

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: Thibault Feneuil ^{i1,a1}, Matthieu Rivain ^{i2,a1}, Damien Vergnaud ^{i3,a2}, Auguste Warmé-Janville ^{i4,a1a2}

Open Researcher and Contributor Identifiers (ORCID):

i1 ([0000-0001-9342-2859](#)); i2 ([0000-0002-9855-4161](#)); i3 ([0000-0002-2113-3967](#)); i4 ([0009-0001-9844-8414](#))

Affiliations:

^{a1} CryptoExperts @ Paris, France

^{a2} LIP6, Sorbonne Université @ Paris, France

Main contacts:

- **Team mailing list:** tsith@cryptoexperts.com
- **Primary technical contact person:** Matthieu Rivain, matthieu.rivain@cryptoexperts.com
- **Secondary contact person:** Auguste Warmé-Janville, auguste.warme-janville@cryptoexperts.com

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

This submission project aims to provide threshold signatures constructed using the Threshold-Signature-in-the-Head (TSitH) framework presented in [FRVW26]. The threshold signatures in the head framework constructs threshold signatures using MPC-in-the-Head techniques translated to a threshold setting. While the efficient MPCitH schemes (e.g. the signatures competing for the NIST's standardization) use GGM trees, our framework uses MPCitH with Merkle trees, that is more suited for secure computation over shared data (see [FRW25; FRVW26]). This submission falls into the category S1 (threshold signatures that do not match existing NIST's standardized primitives).

MPCitH popularity has been growing in recent years, but its threshold analogue is still new (to our knowledge, [CC24] is the only other paper trying to realize threshold MPCitH signatures). One of the main reasons is the impossibility result from [DKR24] which shows that threshold MPCitH signatures must either rely on the thresholdization of the underlying symmetric primitives (inducing huge computation and communication overheads) or have a signature size that increases with the number T of signing parties (which is not desirable in practice). In [FRVW26], we succeed in constraining this overhead to 0.2–0.3 KB per party, allowing for signature sizes that scale reasonably with the number of signing parties.

While this linear factor is not really desirable, threshold MPCitH signatures have interesting upsides. First, they differ from the lattice threshold schemes (which represent the majority of PQ threshold schemes), adding diversity to this field of research. They also have minimal security assumptions: they only rely on symmetric primitives and the random oracle model, as well as an arbitrary one-way function (which allow for modular designs). By setting the OWF to a symmetric primitive (specifically AES), we obtain a threshold signature whose security only relies on symmetric cryptography. This is what we aim for in the TSitH-AES variant. We will also propose instances based on the multivariate quadratic (MQ) and syndrome decoding (SD) problems. All will target a small to medium threshold $T \leq 64$, while the total number of parties N shall be bounded by the size of the base field (which is likely to be $\text{GF}(256)$).

2. Specification

Organization:

The specification will include the following contents:

- A high level description of the construction from [FRVW26] and the intuitions behind it. It will briefly introduce the notions of threshold polynomial commitment scheme (TPCS) and hybrid-sigma polynomial interactive oracle proof (HS-PIOP), and how they can be compiled into a distributed protocol to achieve threshold signatures.
- An introduction to the external building blocks required by the protocol: a secure protocol for generating authenticated Beaver triples (offline MPC part) and a broadcast communication channel.

- A description of the algorithms comprising the protocol –namely, key generation, partial signing, and verification– for each concrete threshold-signature instantiation (AES, MQ, and SD). These algorithms will rely on a common set of primitives, including the threshold DECS (degree-enforcing commitment scheme), which instantiates the threshold PCS within the TSitH framework, as well as other symmetric-key cryptographic primitives.
- A security analysis specifying the adversarial model, underlying security assumptions, and security properties of the proposed threshold signature schemes (notably unforgeability under chosen-message attacks in the threshold setting).
- A part dedicated to the practical evaluation of the scheme. It will contain experimental benchmarks of the implementation, and a discussion of the estimated costs for the external building blocks.

System model:

We consider an MPC model that allows for the active corruption of up to $T - 1$ parties, where T is the number of required signing parties to produce a valid signature. We assume a static corruption, which means that the set of $\leq T - 1$ corrupted parties is fixed once and for all. We further assume a trusted setup for the distributed key generation.

The parties communicate over a broadcast channel. They use two different sharing schemes:

- Shamir’s secret sharing is used for the long term shares part of the secret key.
- Additive secret sharing is used within a signing session. Once a set of signing parties is identified at the beginning of a new signing session, the active parties convert their Shamir shares into additive shares. This is done locally by scaling the Shamir shares using Lagrange coefficients.

Both types of sharing will be authenticated using MAC à la SPDZ to achieve active security.

The parameters T (number of required signing parties) and N (total number of parties) will typically be limited to satisfy $N \leq 256$ and $T \leq \min(N, 64)$. The first constraint arises from use Shamir secret sharing over the base field $\text{GF}(256)$. The second is more arbitrary as we target applications with small to medium thresholds. T might be restricted to smaller values depending on potential implementation constraints.

Security:

The scheme’s unforgeability is proven in the random oracle model, under the security of the underlying OWF (AES, MQ or SD). We further assume an actively secure offline phase for generating authenticated Beaver triples.

3. Open-Source Implementation

We will provide a C (or Rust) implementation of the signing algorithm executed by each party, according to the algorithmic description detailed in the specification, including (but not limited to):

- The threshold DECS,
- The PIOP protocols for each OWF (AES, MQ, SD),
- The online phase of the MPC framework (in our case, the implementation of secure multiplications using authenticated Beaver triples).

The code will be made available publicly on a Github repository.

For the moment, we do not plan to implement the external building blocks, which include the networking layer as well as the secure generation of authenticated Beaver triples.

4. Experimental Performance Evaluation

TSitH can be used to build threshold signatures from AES and MQ, with the sizes and communication costs reported in [FRVW26]. We will propose a third arithmetisation of the syndrome decoding (SD) problem, and possible improvements to the AES arithmetisation, which corresponding signature sizes and communication costs will be reported in the specification.

	$ \mathbb{E} $	$ \sigma $	$N_{\text{mult}}^{\text{ABB}}$	Presign com.	Sign com.	Total com.
AES	248	$22.54 + 0.64 \cdot T$	7750	483.53 (465.71)	24.4 (14.32)	507.93
AES-EM	248	$20.59 + 0.64 \cdot T$	6200	418.43 (403.71)	20.4 (12.32)	438.83
MQ- $\mathbb{F}_{256}$	255	$7.09 + 0.32 \cdot T$	36000	447.55 (375.23)	3.58 (2.62)	451.13
MQ- $\mathbb{F}_{2^{16}}$	255	$7.52 + 0.32 \cdot T$	13600	483.52 (428.8)	4.4 (3.04)	487.92
AES	8192	$13.72 + 0.27 \cdot T$	1625	3565.57 (3558.08)	11.39 (7.11)	3576.96
AES-EM	8192	$12.83 + 0.27 \cdot T$	1300	3154.67 (3148.48)	9.69 (6.26)	3164.36
MQ- $\mathbb{F}_{256}$	8192	$7.06 + 0.19 \cdot T$	10752	7842.54 (7799.34)	3.82 (2.66)	7846.35
MQ- $\mathbb{F}_{2^{16}}$	8192	$6.4 + 0.19 \cdot T$	7616	6191.33 (6160.67)	2.88 (2.06)	6194.21
AES	65520	$12.59 + 0.21 \cdot T$	1425	28838.0 (28831.38)	8.79 (5.51)	28846.79
AES-EM	65520	$11.91 + 0.21 \cdot T$	1140	25560.86 (25555.38)	7.49 (4.86)	25568.35
MQ- $\mathbb{F}_{256}$	65535	$7.48 + 0.16 \cdot T$	8064	24281.03 (24248.61)	4.5 (3.54)	24285.53
MQ- $\mathbb{F}_{2^{16}}$	65535	$6.88 + 0.16 \cdot T$	5712	20470.29 (20447.28)	3.64 (2.96)	20473.93

Table 1: Table from [FRVW26]. Signature size $|\sigma|$ (in kB), number of field multiplications $N_{\text{mult}}^{\text{ABB}}$, presignature/signature communication per party (in kB). The number in brackets represent the threshold DECS communication costs. The communication costs are computed based on the SPDZ online protocol and exclude the offline phase for generating Beaver triples. $|\mathbb{E}|$ is the size of the evaluation domain, which is the number of leaves in the Merkle tree.

In addition, we will provide benchmarks of our implementation, including execution times and memory footprint of the partial signing algorithms on a target platform. We will also estimate as accurately as possible the actual costs of the external building blocks, for a given instantiation (e.g. MASCOT [KOS16] (or variants of it) for the generation of authenticated Beaver triples).

5. Licensing, Patent Claims, and Funding

The authors of the project do not hold, and do not intend to hold, any patent or patent application containing a claim — or that could be amended to include a claim — that may cover the cryptosystem or its implementations.

The content of the submitted package is intended to be open-source. To the best of their knowledge, the authors certify that there are no existing patents or patent applications that may cover the proposed cryptosystem or its source codes.

6. Comparison with Other Submissions

Our scheme is to be compared to the other post-quantum threshold signature submissions. Most of them rely on hard lattice problems. The other ones either rely on group actions (LEAST, Macaw) or structured MQ problems (Vinaigrette). The TSitH submission provides threshold signatures with a different technique, which upside is to be generic. As we require no trapdoor in our OWF, we can consider unstructured hard problems, providing conservative security guarantees.

References

- [CC24]** Eliana Carozza and Geoffroy Couteau. “On Threshold Signatures from MPC-in-the-Head”. In: (2024). URL: <https://eprint.iacr.org/2024/1897>.
- [DKR24]** Jack Doerner, Yashvanth Kondi, and Leah Namisa Rosenbloom. “Sometimes You Can’t Distribute Random-Oracle-Based Proofs”. In: 2024, pp. 323–358. DOI: [10.1007/978-3-031-68388-6_12](https://doi.org/10.1007/978-3-031-68388-6_12).
- [FRVW26]** Thibault Feneuil, Matthieu Rivain, Damien Vergnaud, and Auguste Warmé-Janville. “Threshold Signatures in the Head”. In: *Cryptology ePrint Archive* (June 2026). URL: <https://eprint.iacr.org/2026/1125>.
- [FRW25]** Thibault Feneuil, Matthieu Rivain, and Auguste Warmé-Janville. “Masking-Friendly Post-Quantum Signatures in the Threshold-Computation-in-the-Head Framework”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2025.4 (September 2025), pp. 667–710. DOI: [10.46586/tches.v2025.i4.667-710](https://doi.org/10.46586/tches.v2025.i4.667-710). URL: <https://tches.iacr.org/index.php/TCHES/article/view/12425>.
- [KOS16]** Marcel Keller, Emmanuela Orsini, and Peter Scholl. “MASCOT: Faster Malicious Arithmetic Secure Computation with Oblivious Transfer”. In: 2016, pp. 830–842. DOI: [10.1145/2976749.2978357](https://doi.org/10.1145/2976749.2978357).
- [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).