MPTS 2025 — Call for Talk Proposals

NIST Workshop on Multi-Party Threshold Schemes 2025

- **Workshop dates and place:** **2025-Nov-17–20**, Virtual
- **Submission period:*** **2025-Jul-14–Sep-10** (Anywhere on Earth)
- **Workshop webpage:** https://csrc.nist.gov/events/2025/mpts2025
- **Email address for submissions:** mpts2025-submit@list.nist.gov
- **Email address for inquiries and comments:** mpts2025@nist.gov

Updates about the workshop and/or this call will be announced in the MPTC-forum.

The NIST **W**orkshop on **M**ulti-**P**arty **T**hreshold **S**chemes (MPTS) 2025 will bring together multiple perspectives on Threshold Cryptography, in a learning and collaborative environment. The 4-day virtual workshop is organized within the scope of the NIST Multi-Party Threshold Cryptography (MPTC) project, to gather insights about the state of the art. In scope are topics related to the specification, implementation, analysis and deployment of threshold schemes (and threshold-friendly primitives). The event will include invited and externally-proposed talks, including "**previews**" of upcoming submissions in reply to the NIST Threshold Call.

Attendance and reference material. Online attendance is free but requires registration (see details in the workshop webpage). Talk proposals need to be submitted by email, using a specific form published in the workshop webpage. Participation in any capacity (speaker, panelist, moderator, attendee) requires abiding by the Code of Conduct for NIST Conferences. The presentations will be recorded and made publicly available online at a later time.

Two tracks for talk proposals:†

- **Regular talk.** Talk proposed to contribute with insights about threshold cryptography (and adjacent topics), preferably emphasizing at least one of the topics listed below. The presentations can cover previously published and unpublished results.
- **"Preview talk".** Talk conveying a planned package submission to the NIST Threshold Call (see NISTIR 8214C 2pd, Section 4). Preview talks (and the respective "preview writeup") should be submitted by **2025-Nov-03** (earlier submission is welcome).

* Regular talks can be proposed by September 10. "Preview talks" can be proposed until November 03.

† The abstracts in any talk proposal shall not be produced by generative artificial intelligence (with possible exception of AI-proposed grammar improvements and minor suggestions).

Welcomed topics for talk proposals

Submissions about threshold cryptography are welcome. The following are selected topics:

1. **Threshold security.** Security formulation (e.g., simulatable, game-based), analysis, and provability. Security against adaptive corruptions. Proactive security. Suitability of cryptographic and/or idealized assumptions (e.g., ROM, AGM, GGM) and conjectures. Consequences of (non-ideal) real instantiation of idealized components. Relevant security properties.
2. **Systematizations of knowledge.** Techniques, applications, and related context, about any topic of relevance within the scope of the NIST Threshold Call, including multi-party computation (MPC), zero-knowledge proofs (ZKP), fully-homomorphic encryption (FHE), threshold-friendly cryptographic primitives (e.g., key-generation, signatures, encryption/decryption, hashing) and their corresponding threshold schemes.
3. **Need and adoptability.** Application use cases (fulfilled, urgent, emerging, envisioned). Pertinent setup assumptions, threshold profiles (§C.3), and threshold interfaces (§C.4).
4. **Concrete threshold schemes.** Novel schemes (e.g., with new assumptions, lower number of rounds, better results in a metric of interest) and older pertinent schemes.
5. **Special properties.** Relation between threshold capabilities and other properties, such as succinctness, FHE/ZKP-friendliness, blinding, aggregation, batching.
6. **Building blocks and networking.** Garbled circuits, oblivious transfer, useful commitment schemes, vector oblivious linear evaluation, broadcast, consensus, etc. See §10.7 and §C.1.2 of NISTIR 8214C 2pd.
7. **Implementation, testing, validation, certification.** Criteria and techniques for validation/verification of implementations of threshold schemes. Test vectors and reproducibility challenges when testing distributed systems, and/or floating-point operations. Formal methods. Certification profiles.
8. **Quantum resistance/vulnerability.** Threshold schemes for PQC primitives. Pairing-based threshold schemes. Examples, challenges, advantages and other differences between quantum-resistant and quantum-vulnerable solutions. Levels of security strength.
9. **Development, education, standardization and other community efforts.** Perspectives on efforts related to techniques in scope of the NIST Threshold Call, including FHE, MPC, threshold schemes, ZKP, and useful building blocks.

Submission logistics. Talk should be proposed using the provided PDF form and emailed to mpts2025-submit@list.nist.gov. Submissions received by the deadline will be reviewed, and a notification of acceptance or rejection will be sent by email. During the review, submitters may be asked to refine their proposals for clarity and/or better alignment with the thematic and logistical needs of the workshop. The overall selection, including invited talks, will prioritize the creation of a high-quality balanced program, aligned with the MPTC project goals.