MPTS 2023 Call for Presentation Abstracts

- **Workshop date and place: 2023-Sep-26–28**, Virtual
- **Submission deadline: 2023-Sep-05**, 23:59:59 Anywhere on Earth (UTC−12)
- **Workshop webpage:** https://csrc.nist.gov/events/2023/mpts2023
- **Email address for submissions or questions:** workshop-mpts2023@nist.gov

The NIST workshop on **M**ulti-**P**arty **T**hreshold **S**chemes 2023 (MPTS 2023) is intended to gather diverse public feedback about the **process** envisioned in the *NIST First Call for Multi-Party Threshold Schemes* [NISTIR 8214C ipd (2023)] **(the "Threshold Call")**. The success of the envisioned process (collecting reference material, performing public analysis, devising recommendations) hinges on active involvement of the international cryptography community. To that effect, expert stakeholders are encouraged to **submit abstracts of short talks (5–15 min) to present at MPTS 2023**. The talks should aim to provide (i) feedback to improve the final version of the Threshold Call, or (ii) comments to motivate/facilitate a concerted community participation in submitting high-quality threshold schemes for cryptographic primitives, and their building blocks.

Suggested topics for presentations:

1. **Scope of the Threshold Call:** refinements to the description of **subcategories**.
2. **Submission requirements in the Threshold Call:** needed clarifications.
3. **Expressions of interest:** intended concrete submissions (and possible submitter team).
4. **Need and adoptability:** special features and primitives useful for specific applications.
5. **Inspiration:** suggestions to the community, for submission of concrete threshold schemes.
6. **Frameworks:** pertinent system models, security formulations, and threshold parameters.
7. **Pre/post quantum:** concrete pre-quantum versus post-quantum cases worth focusing on.
8. **Technicalities:** challenges about concrete primitives / threshold schemes / assumptions.
9. **External efforts:** other processes developing related reference material or specifications.

Technical areas of interest (non-exhaustive list): threshold cryptography, secure multi-party computation (MPC), distributed systems, fully-homomorphic encryption (FHE), zero-knowledge proofs (ZKP), threshold/ZKP/MPC/FHE-friendly symmetric primitives (e.g., hash functions and block-ciphers), identity/attribute-based encryption, gadgets, composability and modularity, cryptographic assumptions enabling techniques with advanced features, open-source implementations.

Submissions, selection, and presentations: Presentation abstracts should be submitted by email, using the provided attached submission form (PDF file), by **2023-Sep-05**. A subset of proposed presentations will be selected to be given at the workshop. Notification of acceptance will be sent to the submitters by **2023-Sep-12**. Live presentation is highly encouraged, but a pre-recorded video can optionally be accepted in a few cases. The selection will prioritize: (i) a balanced program within the allowed time; (ii) constructive comments to improve the "threshold call" document; (iii) motivation and suggestions for the community of potential future submitters of threshold schemes and/or gadgets. Additional talks may be invited.

Selected references with further context:

- Workshop: MPTS 2023 (September 2023) [Multi-Party Threshold Schemes]
- NISTIR 8214C ipd (January 2023) [Threshold Call], and received public comments
- NISTIR 8214B ipd (July 2022) [Threshold EdDSA/Schnorr], and received public comments
- Project MPTC [Multi-Party Threshold Cryptography]
- PEC-STPPA Series [Special Topics on Privacy and Public Auditability]
- Call 2021a for comments on criteria (July 2021) and received public comments
- Workshop: MPTS 2020 (November 2020) [Multi-Party Threshold Schemes]
- NISTIR 8214A (July 2020) [Roadmap Toward Criteria] and received public comments
- Workshop: NTCW 2019 (March 2019) [NIST Threshold Cryptography Workshop]

Some improvements expected for the Threshold Call (compared with NISTIR 8214C ipd):

- In Cat1: include signature and encryption schemes selected by the NIST PQC project.
- In Cat2: refine explanation of subcategories (ZKP/FHE/ABE) related to advanced features.
- In Cat2: enhance the list of examples of gadgets.
- Clarify the level of specification intended about KAT values and testability.
- Add templates of the "statements" required from the submitters.
- Include a LaTeX template for submission.
- Add diverse clarifications related to received public comments.

MPTS 2023 Submission Form

Submission deadline: 2023-Sep-05, 23:59:59 Anywhere on Earth (UTC−12)

The MPTS 2023 (Multi-Party Threshold Schemes) workshop — https://csrc.nist.gov/events/2023/mpts2023 — will be a fully-virtual event hosted by NIST (**2023-Sep 26–28**), to collect constructive comments useful for the "Threshold Call" process. Please read the workshop's Call for Presentation Abstracts. To submit, send this form attached in an email to workshop-mpts2023@nist.gov. Note: the metadata (though not the email address) of accepted submissions may be posted online.

Proposed speaker:

1. Email address: ______________________________

2. Name (First and Last): ______________________________

3. Affiliation(s): ______________________________

(If no institutional affiliation, then fill "Self". Include in parenthesis the countries of the institution of affiliation.)

4. Speaker intro ("bio"; max 60 words):

(Please fill how the host should introduce you in case your submission is accepted for a presentation.)

Intended presentation:

5. Desired time: □ 5 min □ 10 min □ 15 min **Likely to present live:** □ Yes □ No

6. Title of presentation (tentative): ______________________________

7. Main keywords/topics:

8. Abstract (max 350 words; include "In this presentation/talk"):

Possibly to be publicly display in the workshop program, if the presentation is accepted.

Additional context:

9. Related-references (including authored by the speaker):

(For each applicable reference, please include also a link/identifier (if possible succinct) for free public access, such as, doi.org/..., or ia.cr/....)

10. Optional extra comment to be considered during the review of the submission: