TCPT2 Welcome and Introduction

Presented* at NIST-TCPT2

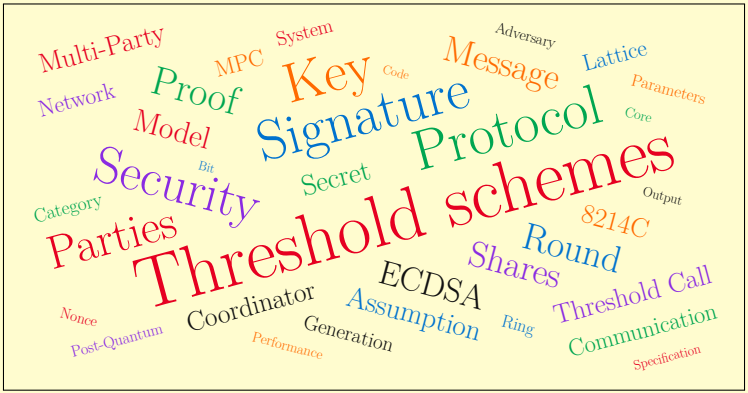
Threshold Call Preview Talks #2

July 7, 2026 | Virtual event (hosted from Maryland, USA)

* Luís Brandão: Contractor from Strativia. Presented within the scope of the NIST-MPTC project. Slides based on previous presentations. Expressed opinions are from the speaker. Edits on 2026-07-15.

Welcome to TCPT2

Threshold **C**all **P**review **T**alks, **2**nd Phase



We look forward to hearing the 10 new plans of upcoming submissions

Outline

1. **The MPTC project**
2. The NIST Threshold Call
3. Submitted previews
4. The TCPT2 Event

MPTC = Multi-Party Threshold Cryptography.
TCPT2 = Threshold Call Preview Talks, 2nd Phase.
NIST = National Institute of Standards and Technology.

Multi-Party Threshold Cryptography: NIST Project

Cryptographic primitives:

Signing

Encryption

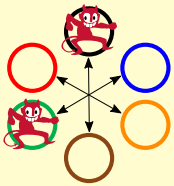
Hashing

KeyGen etc.

Threshold schemes (for cryptographic primitives)

1. Split (**secret-share**) the secret/private-key across multiple parties.
2. Use **MPC** to perform needed operation (with split key), e.g., sign.

   (MPC = secure multiparty computation ... or call it "Threshold Cryptography")



Threshold f Operation is secure if the number of corrupted parties is $\leq f$.

Decentralized trust Key remains split $\Rightarrow$ No party is a critical point of failure.

Outline

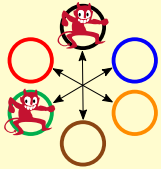
1. The MPTC project
2. **The NIST Threshold Call**
3. Submitted previews
4. The TCPT2 Event

MPTC = Multi-Party Threshold Cryptography.
TCPT2 = Threshold Call Preview Talks, 2nd Phase.
NIST = National Institute of Standards and Technology.

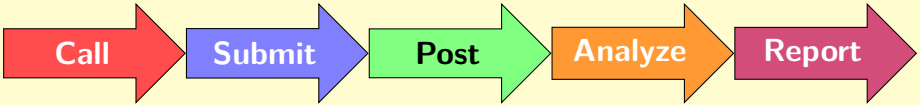
The NIST Call for *Multi-Party Threshold Schemes*

A public call for input, to form a body of reference material:

- It deals with **threshold** schemes
- It stands at the **threshold** of advanced cryptography



Establishes a process: (not a competition for selection of a standard)



Fits the exploratory **"Reference Materials"** approach of the MPTC project.

A Scope Organized into Two Classes

- **Class N: NIST-standardized primitives** (Sign, PKE, Symm, KeyGen)

  KeyGen = Key Generation; PKE = Public-Key Encryption; Symm = Symmetric

- **Class S: Special others** (those above; FHE, ZKPoK, Gadgets)

  FHE = Fully-Homomorphic Encryption; ZKPoK = Zero-Knowledge Proof of Knowledge

Each class is organized into various categories

	Sign	PKE	Symmetric	KeyGen	**FHE**	**ZKPoK**	**Gadgets**
NIST specified	N1	N2	N3	N4			
Special others	S1	S2	S3	S4	**S5**	**S6**	**S7**

Phases / Timeline (2026)

T-Call

- NIST First Call for Multi-Party Threshold Schemes (NIST IR 8214C)
- Published on **Jan-20**, after two public drafts (ipd in 2023; 2pd in 2025)

Previews

- A "preview" explains a plan of upcoming package submission.
- Phase 1: January (26 previews).
- Phase 2: May/**July (10 previews)**.
- Phase 3: July/August: writeups by **July 31**; talks TBA.

Packages

- Tech. Specification, Ref. Implementation, Report Exp. Evaluation.
- Not before ($\geq$) **Nov-30** (deadline TBA after Previews Phase 3).

Delays: the latex-template and talk-videos will still to be posted.

Outline

1. The MPTC project
2. The NIST Threshold Call
3. **Submitted previews**
4. The TCPT2 Event

MPTC = Multi-Party Threshold Cryptography.
TCPT2 = Threshold Call Preview Talks, 2nd Phase.
NIST = National Institute of Standards and Technology.

Previews Phase #2: 10 new Preview Writeups

Category	System	Hint
N1.2: T. ECDSA	**Trout++**	Robust, asynchronous, 2-round
	Twig	2-round, via non-interactive multiplication
	KU	Honest-majority
N1.1: T. EdDSA/Schnorr	**FaFROST**	Fully adaptive, 1-round online
N1.4: T. ML-DSA	**TALUS**	1-round online
N3: T. Symmetric	**Threshcon**	Threshold Ascon primitives
S1: T. Signing	**Lemur**	Lattice-based synchronized multi-signature
	LoTRS	Lattice-based threshold ring signatures
S6: ZKP	**LaZer**	Lattice-based ZK arguments
S7: Gadgets	**CoordMsg**	Coordinated message-delivery layer

Cat. = [Sub]Category. N (prefix) = Class N (NIST-specified primitives). S (prefix) = Class S (Other Special primitives).

Coverage of the Previews

- **N1.1: EdDSA/Schnorr:** Fireblocks-3MI; Gargos; FROST; RedETA; ▶ FaFROST
- **N1.2: ECDSA:** BICYCCLIST; Fireblocks-3MI; RedETA; SplitForge; ▶ Trout++; ▶ Twig; ▶ KU
- **N1.3: RSA:** SplitForge
- **S1: Non-NIST Sign:** tBLS

Quantum vulnerable signatures

- **N1.4: ML-DSA:** Mithril, Quorus, SplitForge; ▶ TALUS
- **N1.5: LMS/XMSS:** Haystack
- **S1: Non-NIST:** Hermine, LEAST, PQarrots, Tanuki, Vinaigrette; ▶ Lemur; ▶ LoTRS

Quantum resistant signatures

- **S2: PKE/KEM:** Amber, Fireblocks-3MI, PQarrots, SplitForge
- **N3/S3: Symmetric:** MPC MINIons, Symphony; ▶ Threshcon
- **S5: FHE:** PANTHERIA, Zama
- **S6: ZKP:** Schmivitz, SmallWood, Zama; ▶ LaZer
- **S7: Gadgets:** Fireblocks-3MI, MPC MINIons, PiVer, Schmivitz, Symphony, Zama; ▶ CoordMsg

Other categories

▶ = submitted in the 2nd Preview phase.

Selected Notes

Preparing a submission package

- Requires an earlier "preview" (in phase 1, 2 or 3).
- Teams can still update their presented plans (e.g, combine crypto-systems).
- A LaTeX template will be available (following the Threshold Call description).
- Disclosure of related patent claims (associated with team members) is required.

Analysis and discussion (2027)

- MPTC will hold a seminar series for thorough presentations by the teams.
- Expect technical comments via the MPTC-Forum.

Outline

1. The MPTC project
2. The NIST Threshold Call
3. Submitted previews
4. **The TCPT2 Event**

MPTC = Multi-Party Threshold Cryptography.
TCPT2 = Threshold Call Preview Talks, 2nd Phase.
NIST = National Institute of Standards and Technology.

Guidelines for Virtual Participation

- **Code of Conduct:** Participation in TCPT2 requires abiding by the Code of Conduct for NIST conferences: https://www.nist.gov/pao/code-conduct-nist-conferences

- **Recording:** Audio-visual recording is allowed only by the hosts, for later posting on the webpage. Slide-decks (PDF) will also be posted.
- **Text/chat:** Limited to topics related to the event and crypto.
- **Q&A:** For each talk, we may relay a few comments / questions from the audience. Speakers can also follow up in the chat, after their talk.
- **Audio:** Oral question/comment implies consent for audio recording/posting.

TCPT2 Sessions

Day	Morning sessions	Afternoon sessions
Jul-07 (Tue)	• Introduction • **Session 1a:** ECDSA	• **Session 1b:** Messaging and EdDSA • 6–7pm: Two talks of session 2a
Jul-08 (Wed)	• **Session 2a:** Lattice-based signatures (including replay of 2 recorded talks)	• **Session 2b:** ZKP and Ascon

Note: due to timezone differences, talks 2a2 and 2a3 are presented-and-recorded live on July 7, 6–7pm EDT, and retransmitted on July 8 in the morning.

TCPT2 Schedule

Day 1: July 07

Session 1a: ECDSA

- Talk 1a1: 10:40–11:05: **Trout++:** Robust Asynchronous Two-Round ECDSA for Arbitrary Thresholds
- Talk 1a2: 11:05–11:20: **Twig:** Two-Round Threshold ECDSA from Non-Interactive Multiplication
- Talk 1a3: 11:20–11:55: **KU25:** Honest-Majority Threshold ECDSA

Session 1b: Messaging and EdDSA

- Talk 1b1: 13:05–13:30: **Coordinated MPC:** Transport Layer for Multi-Party Protocols
- Talk 1b2: 13:30–13:55: **FaFROST:** Fully Adaptive FROST with Identifiable Aborts from AOMDL

Day 2: July 08

Session 2a: Lattice-based signatures

- Talk 2a1: 10:40–11:05: **TALUS:** Threshold ML-DSA with One-Round Online Signing
- Talk 2a2: 11:05–11:30: **Lemur:** Scalable Post-Quantum Synchronized Multi-Signatures
- Talk 2a3: 11:30–11:55: **LoTRS:** Practical Post-Quantum Structured Threshold Ring Signatures from Lattices

Session 2b: Others: ZKP and Ascon

- Talk 2b1: 13:30–13:55: **LaZer:** Lattice-Based Zero-Knowledge Arguments for Lattice Relations
- Talk 2b2: 13:55–14:20: **Threshcon:** Multi-Party Threshold Ascon

Talks 2a2 and 2a3 are recorded live on July 7, 6–7pm EDT, and retransmitted on July 8 in session 2a.

Thank You for Your Attention!

TCPT2 Event

MPTC Project

Threshold Call

Preview Materials

MPTC Forum

TCPT2 Welcome and Introduction

Presented at TCPT2 | Virtual event (hosted from Maryland, USA), July 7, 2026

luis.brandao@nist.gov

Index of Slides

1. Cover
2. Welcome to TCPT2
3. Outline: The MPTC project
4. Multi-Party Threshold Cryptography: NIST Project
5. Outline: The NIST Threshold Call
6. The NIST Call for Multi-Party Threshold Schemes
7. A Scope Organized into Two Classes
8. Phases / Timeline (2026)
9. Outline: Submitted previews
10. Previews Phase #2: 10 new Preview Writeups
11. Coverage of the Previews
12. Selected Notes
13. Outline: The TCPT2 Event
14. Guidelines for Virtual Participation
15. TCPT2 Sessions
16. TCPT2 Schedule
17. Thank You for Your Attention!
18. Index of Slides