TCPT3 Welcome and Introduction

Presented* at NIST-TCPT3

Threshold Call Preview Talks #3

2026-Sep-30† | Virtual event (hosted from Maryland, USA)



* Luís Brandão: NIST Foreign Guest Researcher (Contractor). Scope: NIST-MPTC program.

† Note 2026-Oct-31: Edited post-event, combining notes about the four days: Sep 30 and Oct {6, 7, 13}.

Welcome to TCPT3

Threshold **C**all **P**review **T**alks **#3**

(Sep 30 and Oct {6, 7, 13}, 2026)

24 plans of upcoming submissions to the NIST Threshold Call



We look forward to hosting the 24 Preview Talks

Outline

1. **The NIST Threshold Call**

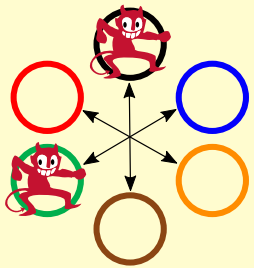
2. Submitted previews

3. The TCPT3 Event

TCPT3 = Threshold Call Preview Talks #3.
NIST = National Institute of Standards and Technology.

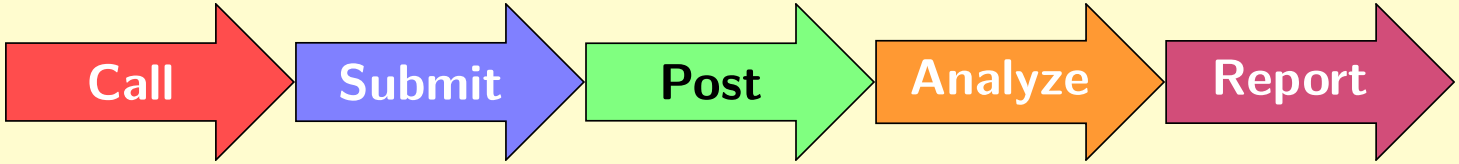
The NIST Call for *Multi-Party Threshold Schemes*

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

- Phase 1: 26 in January @ MPTS 2026
- Phase 2: 10 in July @ TCPT2
- Phase 3: 24 **in September/October @ TCPT3**

"Preview": A plan of package submission.

Packages

- Tech. Specification, Ref. Implementation, Report Exp. Evaluation.
- Optional: preliminary submission for editorial feedback: **Dec 01–31**
- Expected deadline: ($\geq$) **2027-Mar-01**

Selected Notes

Preparing a submission package

- Preview Writeups can still be updated.
- A LaTeX template will be available (using the Threshold Call description).
- Required disclosure of related patent claims (associated with team members).

Analysis and discussion (2027)

- Presentations by the teams.
- Experiment with open-source implementations.
- Public comments via the MPTC-Forum.

Outline

1. The NIST Threshold Call
2. **Submitted previews**
3. The TCPT3 Event

TCPT3 = Threshold Call Preview Talks #3.
NIST = National Institute of Standards and Technology.

36 Previews in Phases 1 & 2 (presented at MPTS & TCPT2)

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

Amber S2	BAM N1 N4	CGGMP N1 N4 S2 S7	Classic Schnorr N1 N4	Coord MPC S7	FaFROST N1	FROST N1	Gargos N1	Haystack N1
Hermine S1 S4	KU N1	LaZer S6	LEAST S1 S4	Lemur S1	LoTRS S1	Mithril N1 N4	MPC-MINIONS N1 N4	PANTHERIA S5
PiVer S7	PQarrots S1 S2 S4	Quorus N1 N4	RedETA N1 N4	Schmivitz S6 S7	SmallWood S6	SplitForge N1 N4 S2	Symphony N3 S7	TALUS N1 N4
Tanuki S1	tBLS S1	TECLA N1	THE-CLASH N1	Threshcon N3	Trout++ N1	Twig N1	Vinaigrette S1 S4	Zama S4 S5 S6

https://csrc.nist.gov/projects/threshold-cryptography/tcall-1

24 Previews in Phase 3 (presented at TCPT3)

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

Adamas S2	ark-pq S6	ATMACA N1	Axolotl N1 S7	(Threshold-)CL S2	DKLs N1 N4 S7
DUOV S1 S4	Holocron N2	Kettle S1	Kryptallage S4 S5	LaTSEC S1 S7	Menshen/(T)CL N1
MOZI S5 S7	Pilaf S1	Stoats N1 N4 S1 S4 S7	TALH N1 S1	TalonG/P-DualTS S1	TapTop/Robot S1
Teddy N1	Thimza S1	THQC N2	TORTL N4	TSitH S1	Tulva S5

https://csrc.nist.gov/projects/threshold-cryptography/tcall-1#Previews-3

24 Previews in Phase 3

Team/System	|.|	Cat.
Kryptallage	16	S5
MOZI	6	S5
Holocron	12	N2
ark-pq	4	S6
ATMACA	4	N1
Kettle	8	S1
DUOV	4	S1/S4
TALH	1	N1,S1
TalonG/P-DualTS	11	S1
LaTSEC	5	S1/S7
Thimza	2	S1
TSitH	4	S1
(Threshold-)CL	7	S2
Axolotl	3	N1,S7
Stoats	6	N1/N4,S7
DKLs	6	N1/N4,S7
Menshen/(T)CL	11	N1
TapTop/Robot	11	S1
Tulva	6	S5
Adamas	4	S2
THQC	4	N2
TORTL	4	N4
Teddy	11	N1
Pilaf	6	S1

Legend: Entries are in presentation order. |.| = Team size (number of members). Cat. = Categories. N (prefix) = Class N (NIST-specified primitives). S (prefix) = Class S (Other Special primitives).

24 Previews in Phase 3

	Team/System	|.|	Cat.
1st day	Kryptallage	16	S5
	MOZI	6	S5
	Holocron	12	N2
	ark-pq	4	S6
2nd day	ATMACA	4	N1
	Kettle	8	S1
	DUOV	4	S1/S4
	TALH	1	N1,S1

	Team/System	|.|	Cat.
2nd day	TalonG/P-DualTS	11	S1
	LaTSEC	5	S1/S7
	Thimza	2	S1
	TSitH	4	S1
3rd day	(Threshold-)CL	7	S2
	Axolotl	3	N1,S7
	Stoats	6	N1/N4,S7
	DKLs	6	N1/N4,S7

	Team/System	|.|	Cat.
3rd day	Menshen/(T)CL	11	N1
	TapTop/Robot	11	S1
4th day	Tulva	6	S5
	Adamas	4	S2
	THQC	4	N2
	TORTL	4	N4
	Teddy	11	N1
	Pilaf	6	S1

Legend: Entries are in presentation order. |.| = Team size (number of members). Cat. = Categories. N (prefix) = Class N (NIST-specified primitives). S (prefix) = Class S (Other Special primitives).

Phase 3 Previews per Category

- **Signatures N1 (7):** ATMACA, Axolotl, DKLs, Menshen/(T)CL, Stoats, TALH, Teddy
- **Signatures S1 (10):** DUOV, Kettle, LaTSEC, Pilaf, Stoats, TALH, TalonG/P-DualTS, TapTop/Robot, Thimza, TSitH
- **PKE N2 (2):** Holocron, THQC
- **PKE S2 (2):** Adamas, (Threshold-)CL
- **DKG N4/S4 (5):** DKLs, DUOV, Kryptallage, Stoats, TORTL
- **FHE S5 (3):** Kryptallage, MOZI, Tulva
- **ZKP S6 (1):** ark-pq

Systems may appear in more than one row.

Phase 3 Previews per Category

- **Signatures N1 (7):** ATMACA, Axolotl, DKLs, Menshen/(T)CL, Stoats, TALH, Teddy
- **Signatures S1 (10):** DUOV, Kettle, LaTSEC, Pilaf, Stoats, TALH, TalonG/P-DualTS, TapTop/Robot, Thimza, TSitH
- **PKE N2 (2):** Holocron, THQC
- **PKE S2 (2):** Adamas, (Threshold-)CL
- **DKG N4/S4 (5):** DKLs, DUOV, Kryptallage, Stoats, TORTL
- **FHE S5 (3):** Kryptallage, MOZI, Tulva
- **ZKP S6 (1):** ark-pq

Systems may appear in more than one row.

1st day 2nd day 3rd day 4th day

Coverage of FHE (S5)

Previous phases

- **PANTHERIA**: Threshold FHE for RLWE-based cryptosystems.
- **Zama**: TFHE (Torus FHE) and Nexus (Threshold-FHE).

TCPT3 1st day (Sep 30)

- **Kryptallage**: Thresholdized FHE scheme switching
- **MOZI**: Threshold FHE for many parties (S5, S7)
- **Holocron**: Threshold K-PKE via FHE (N2) [not S5]

TCPT3 4th day (Oct 13)

- **Tulva**: Practical asynchronous threshold FHE

Coverage of ZKP (S6)

Previous phases

- **Schmivitz: VOLE**-in-the-head-based ZK gadgets.
- **SmallWood: Hash**-based ZK arguments for relatively small instances.
- **LaZer: Lattice**-based ZK arguments for lattice relations.
- (ZKP **for FHE**: **Zama:** ZHEnith: ZKP of Correctness of TFHE Ciphertexts)

TCPT3 1st day (Sep 30)

- **ark-pq**: **Hash**-based post-quantum ZK arguments.
- (ZKP for FHE: **MOZI**, **Holocron**)

Coverage of PQC Threshold Signatures (N1, S1)

Previous phases

- **N1 (ML-DSA): Mithril**, **Quorus**, **SplitForge** (Trilithium), **TALUS**
- **N1 (LMS/XMSS): Haystack**
- **S1 (others): Hermine**, **LEAST**, **PQarrots** (Macaw), **Tanuki**, **Vinaigrette**, **Lemur**, **LoTRS**

TCPT3 2nd day (Oct 6)

- **ATMACA** (N1): Threshold FALCON signatures
- **Kettle** (S1): Threshold HAWK signatures
- **DUOV** (S1, S4): Threshold UOV with pre-signing
- **TALH and ASPEN** (N1, S1): Threshold hash-based signatures
- **TalonG and P-DualTS** (S1): Two-round lattice signatures
- **LaTSEC** (S1, S7): Lattice signatures via SEC secret sharing
- **Thimza** (S1): Stateless module-lattice signatures
- **TSitH** (S1): MPC-in-the-Head signatures

Coverage of Quantum-Vulnerable Threshold Signatures (N1, S1)

Previous phases

- **Schnorr/EdDSA (N1):** **FROST**, **Classic Schnorr**, **Gargos**, **RedETA**, **FaFROST**
- **ECDSA (N1):** **BAM and CGGMP**, **TECLA and THE-CLASH**, **RedETA**, **KU**
- **RSA/ECDSA (N1):** **SplitForge** (Split-RSA, Split-ECDSA)
- **BLS (S1):** **tBLS**
- **ECDSA/Schnorr (N1):** **Trout++**, **Twig**

TCPT3 3rd day (Oct 7)

- **Axolotl** (N1): Threshold Schnorr
- **Stoats** (N1, S1): Two-party ECDSA/Schnorr
- **DKLs** (N1): Threshold ECDSA
- **Menshen/(T)CL** (N1): Threshold ECDSA
- **TapTop/Robot** (S1): Threshold BBS

TCPT3 4th day (Oct 13)

- **Teddy** (N1): Threshold EdDSA
- **Pilaf** (S1): Schnorr-type signatures

Coverage of DKG (N4, S4)

Previous phases

- **N4, elliptic curves:** **Classic Schnorr**, **BAM and CGGMP**, **RedETA**
- **N4, ML-DSA:** **Mithril**, **Quorus**, **TALUS**
- **N4, several primitives:** **SplitForge** (RSA, ECDSA, ML-DSA)
- **S4:** **Hermine**, **LEAST**, **PQarrots** (Kakapo), **Vinaigrette**, **Zama** (Nexus)

TCPT3

- **1st day (Sep 30):** **Kryptallage** (S4): Distributed key generation for FHE
- **2nd day (Oct 6):** **DUOV** (S4): Key generation for threshold UOV
- **3rd day (Oct 7):** **Stoats** (N4/S4), **DKLs** (N4): Key generation alongside threshold signing
- **4th day (Oct 13):** **TORTL** (N4): Elliptic-curve and module-lattice DKG

Coverage of PKE/KEM (N2/S2) and Symmetric Primitives (N3/S3)

Previous phases

PKE/KEM (S2)

- **Amber**: Lattice-based threshold KEMs
- **CGGMP**: Paillier encryption (building block)
- **PQarrots** (Kea): Isogeny-based PKE
- **SplitForge**: Server-assisted ElGamal decryption

Symmetric (N3/S3)

- **MPC MINIons** (N3/S3): Authenticated garbling
- **Symphony** (N3): AES, hashing, MACs
- **Threshcon** (N3): Ascon encryption/hashing

TCPT3: PKE/KEM (N2/S2)

- **1st day (Sep 30): Holocron** (N2): Threshold K-PKE via FHE
- **3rd day (Oct 7): (Threshold-)CL** (S2): Class-group homomorphic PKE
- **4th day (Oct 13): Adamas** (S2): Lattice KEM/PKE; one-round decryption
- **4th day (Oct 13): THQC** (N2): Code-based threshold PKE decryption

No N3/S3 previews at TCPT3.

Outline

1. The NIST Threshold Call

2. Submitted previews

3. **The TCPT3 Event**

TCPT3 = Threshold Call Preview Talks #3.
NIST = National Institute of Standards and Technology.

Guidelines for Virtual Participation

- **Code of Conduct:** Participation in TCPT3 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.

TCPT3 Sessions

Day	Morning session (starts 10:00)	Afternoon session (starts 13:00)
Sep-30 (Wed)	**Session 1a:** FHE and ZKP	—
Oct-06 (Tue)	**Session 2a:** PQ threshold signatures	**Session 2b:** PQ threshold signatures
Oct-07 (Wed)	**Session 3a:** QV threshold schemes	**Session 3b:** QV threshold signatures
Oct-13 (Tue)	**Session 4a:** PQ PKE (including FHE)	**Session 4b:** DKG and QV signatures

TCPT3 Schedule of 1st day (2026-Sep-30)

Session 1a: FHE and ZKP

- **Talk 101:** 10:00–10:10: **TCPT3:** Welcome and Introduction
- **Talk 1a1:** 10:10–10:35: **Kryptallage:** Unified FHE scheme and threshold protocol layer
- **Talk 1a2:** 10:35–11:00: **MOZI:** Scalable threshold FHE
- **Break**
- **Talk 1a3:** 11:15–11:40: **Holocron:** Ciphertext-interchangeable threshold K-PKE via FHE
- **Talk 1a4:** 11:40–12:05: **ark-pq:** Post-quantum zero-knowledge arguments of knowledge

TCPT3 Schedule of 2nd day (2026-Oct-06)

Session 2a: Morning: post-quantum threshold signatures

- **Talk 2a1:** 10:10–10:35: **ATMACA:** Lattice-Based Threshold Signing for FALCON
- **Talk 2a2:** 10:35–11:00: **Kettle:** Short Threshold HAWK Signatures
- Break
- **Talk 2a3:** 11:15–11:40: **DUOV:** A Dressing in Advance for Threshold UOV with Pre-signing
- **Talk 2a4:** 11:40–12:05: **TALH:** Threshold Authentication via Leaf-sharing in Hash-based Signatures

---

Session 2b: Afternoon: post-quantum threshold signatures

- **Talk 2b1:** 13:00–13:25: **TalonG and P-DualTS:** 2-round Lattice-based Threshold Signatures
- **Talk 2b2:** 13:25–13:50: **LaTSEC:** Lattice-Based Threshold Signature from Expander Codes
- Break
- **Talk 2b3:** 14:05–14:30: **Thimza:** Lattice-Based Stateless Threshold Signatures at Optimal Bandwidth
- **Talk 2b4:** 14:30–14:55: **TSitH:** Threshold Signatures in the Head

All times are in EDT (UTC–4).

TCPT3 Schedule of 3rd day (2026-Oct-07)

Session 3a: Morning: QV threshold schemes

- **Talk 3a1:** 10:10–10:35: **(Threshold-)CL:** (Threshold) Linearly Homomorphic PKE from Class Groups
- **Talk 3a2:** 10:35–11:00: **Axolotl:** Robust Asynchronous Threshold Schnorr
- **Talk 3a3:** 11:00–11:25: **Stoats:** Short Two-round vOle-bAsed Threshold Signatures

---

Session 3b: Afternoon: QV threshold schemes

- **Talk 3b1:** 13:00–13:25: **DKLs:** Threshold ECDSA from VOLE and Commitments
- **Talk 3b2:** 13:25–13:50: **Menshen and (T)CL:** 3-round threshold ECDSA schemes
- **Talk 3b3:** 13:50–14:15: **TapTop & Robot:** 2-party threshold BBS schemes

All times are in EDT (UTC–4).

TCPT3 Schedule of 4th day (2026-Oct-13)

Session 4a: Morning: post-quantum PKE (inc. FHE)

- **Talk 4a1:** 10:10–10:35: **Tulva:** Practical Asynchronous Threshold FHE
- **Talk 4a2:** 10:35–11:00: **Adamas:** 1-Round Lattice-Based Threshold KEM/PKE vs Adaptive Corruptions
- **Talk 4a3:** 11:00–11:25: **THQC:** Threshold Hamming Quasi-Cyclic (KEM decryption)

Session 4b: Afternoon: DKG and QV signatures

- **Talk 4b1:** 13:00–13:25: **TORTL** DKG
- **Talk 4b2:** 13:25–13:50: **Teddy:** Threshold EdDSA Schemes
- **Talk 4b3:** 13:50–14:15: **Pilaf:** Fully Tight Two-Round Threshold Signatures

All times are in EDT (UTC–4).

Thank You for Your Attention!

TCPT3 Event

MPTC Project

Threshold Call

Preview Materials

MPTC Forum

TCPT3 Welcome and Introduction

Presented at TCPT3 | Virtual event (hosted from Maryland, USA), 2026-Sep-30[†]

luis.brandao@nist.gov

[†] Note 2026-Oct-31: Edited post-event, combining notes about the four days: Sep 30 and Oct {6, 7, 13}.

Index of Slides

1. Cover
2. Welcome to TCPT3
3. Outline: The NIST Threshold Call
4. The NIST Call for Multi-Party Threshold Schemes
5. A Scope Organized into Two Classes
6. Phases / Timeline (2026)
7. Selected Notes
8. Outline: Submitted previews
9. 36 Previews in Phases 1 & 2 (presented at MPTS & TCPT2)
10. 24 Previews in Phase 3 (presented at TCPT3)
11. 24 Previews in Phase 3
12. Phase 3 Previews per Category
13. Coverage of FHE (S5)
14. Coverage of ZKP (S6)
15. Coverage of PQC Threshold Signatures (N1, S1)
16. Coverage of Quantum-Vulnerable Threshold Signatures (N1, S1)
17. Coverage of DKG (N4, S4)
18. Coverage of PKE/KEM (N2/S2) and Symmetric Primitives (N3/S3)
19. Outline: The TCPT3 Event
20. Guidelines for Virtual Participation
21. TCPT3 Sessions
22. TCPT3 Schedule of 1st day (2026-Sep-30)
23. TCPT3 Schedule of 2nd day (2026-Oct-06)
24. TCPT3 Schedule of 3rd day (2026-Oct-07)
25. TCPT3 Schedule of 4th day (2026-Oct-13)
26. Thank You for Your Attention!
27. Index of Slides