

MPTS 2026 and the NIST Threshold Call Introductory Notes

Presented* at MPTS 2026

NIST Workshop on Multi-Party Threshold Schemes

January 26, 2026 | Maryland (USA)

(Minor editorial updates on 2006-Feb-10)

* Luís Brandão: NIST Associate (Foreign Guest Researcher[†], Contractor via Strativia). Expressed opinions are from the speaker.

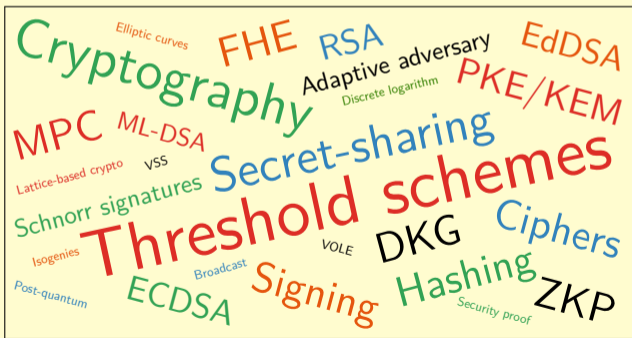
[†]Cryptographic Technology Group, Information Technology Laboratory, National Institute of Standards and Technology (NIST) © USA.

Based on [NIST IR 8214C](#) (joint work with René Peralta) and [NIST IR 8214B ipd](#) (joint work with Michael Davidson)

Welcome to MPTS 2026

The NIST Workshop on Multi-Party Threshold Schemes

We look forward to the sharing of insights



- 4 days
- 9 sessions
- 45 talks
- 26 “previews”
- \approx 200 co-authors

Outline

1. **The MPTC project**
2. **The NIST Threshold Call**
3. **The MPTS 2026 Workshop**

MPTC = Multi-Party Threshold Cryptography.
MPTS = Multi-Party Threshold Schemes.
NIST = National Institute of Standards and Technology.

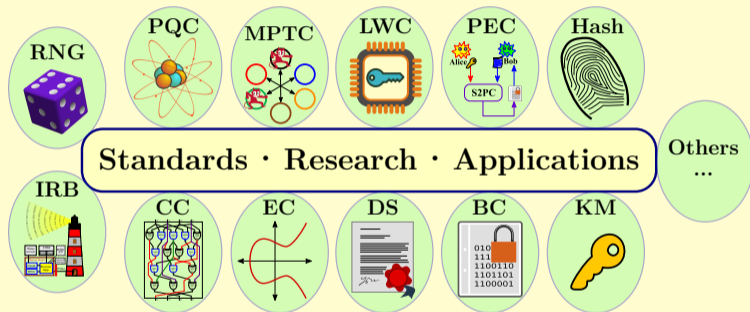
Outline

1. **The MPTC project**
2. The NIST Threshold Call
3. The MPTS 2026 Workshop

MPTC = Multi-Party Threshold Cryptography.
MPTS = Multi-Party Threshold Schemes.
NIST = National Institute of Standards and Technology.

Activities in the “Crypto” Group

<https://www.nist.gov/itl/csd/cryptographic-technology>

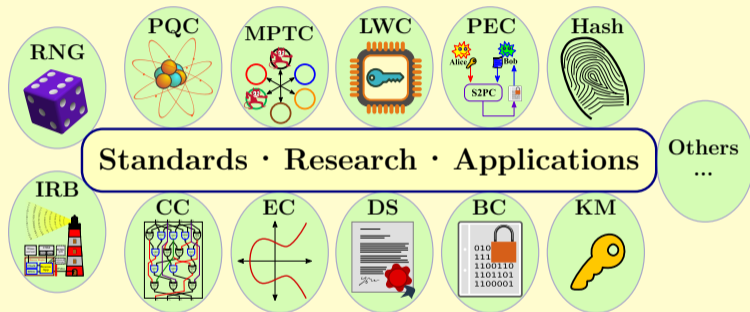


Legend:

- BC = Block Ciphers
- CC = Circuit Complexity
- **Crypto.** = **Cryptography**
- DS = Digital Signatures
- EC = Elliptic Curves
- IRB = Interop. Randomness Beacons
- KM = Key Management.
- LWC = Lightweight Crypto.
- PEC = Privacy-Enhancing Crypto.
- PQC = Post-Quantum Crypto.
- RNG = Random-Number Generation

Activities in the “Crypto” Group

<https://www.nist.gov/itl/csd/cryptographic-technology>



Legend:

- BC = Block Ciphers
- CC = Circuit Complexity
- **Crypto.** = Cryptography
- DS = Digital Signatures
- EC = Elliptic Curves
- IRB = Interop. Randomness Beacons
- KM = Key Management.
- LWC = Lightweight Crypto.
- PEC = Privacy-Enhancing Crypto.
- PQC = Post-Quantum Crypto.
- RNG = Random-Number Generation

Focus of this presentation and workshop:
MPTC = Multi-Party Threshold Cryptography

<https://csrc.nist.gov/projects/threshold-cryptography>



Multi-Party Threshold Cryptography: NIST Project

Cryptographic primitives:



Signing



Encryption



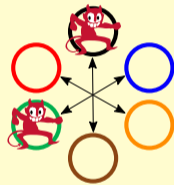
Hashing



KeyGen

etc.

Threshold schemes (for cryptographic primitives)



Multi-Party Threshold Cryptography: NIST Project

Cryptographic primitives:



Signing



Encryption



Hashing

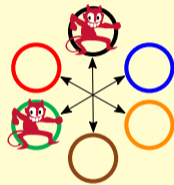


KeyGen

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")



Multi-Party Threshold Cryptography: NIST Project

Cryptographic primitives:



Signing



Encryption



Hashing

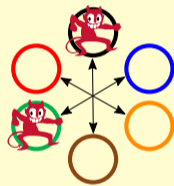


KeyGen

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")

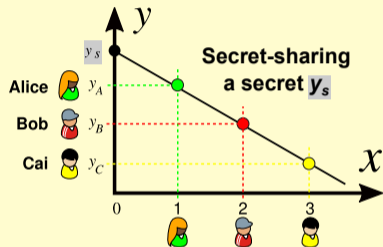


Threshold f Operation is secure if the number of corrupted parties is $\leq f$.

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

Basics of a Threshold Scheme

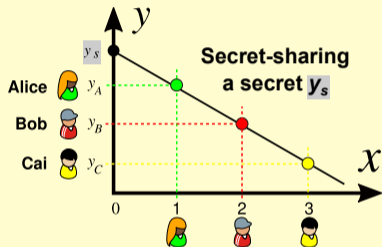
Secret-sharing:



1. Splits the key into secret shares

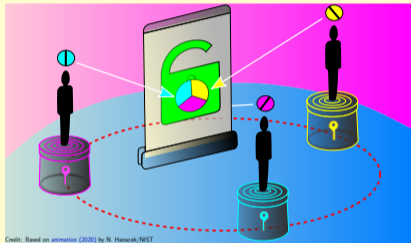
Basics of a Threshold Scheme

Secret-sharing:



1. Splits the key into secret shares

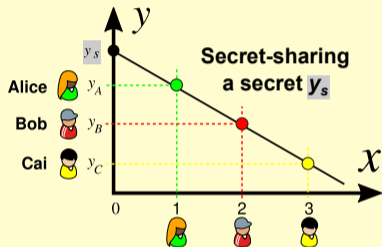
Multi-party computation (MPC)



2. Operates without recombining the key

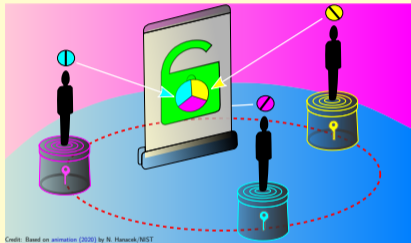
Basics of a Threshold Scheme

Secret-sharing:

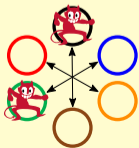


1. Splits the key into secret shares

Multi-party computation (MPC)



2. Operates without recombining the key



Participation threshold: the operation needs k parties in agreement

Corruption threshold: system secure even if f parties are malicious

Why Care about Threshold Schemes?

Why Care about Threshold Schemes?

Attraction

- Feasible decentralized paradigm for key-management.
- Also an entry point to discovering more general MPC.



Why Care about Threshold Schemes?

Attraction

- Feasible decentralized paradigm for key-management.
- Also an entry point to discovering more general MPC.



Goals

- Promote *good* **adoptability** (secure, interoperable, best practices; ...)
- Improving signal-to-noise (identifying sound crypto techniques)

Hesitation

- Many options (model, assumptions, parameters): which are useful?

Why Care about Threshold Schemes?

Attraction

- Feasible decentralized paradigm for key-management.
- Also an entry point to discovering more general MPC.



Goals

- Promote *good* **adoptability** (secure, interoperable, best practices; ...)
- Improving signal-to-noise (identifying sound crypto techniques)

Hesitation

- Many options (model, assumptions, parameters): which are useful?

Why Care about Threshold Schemes?

Attraction

- Feasible decentralized paradigm for key-management.
- Also an entry point to discovering more general MPC.



Goals

- Promote *good* **adoptability** (secure, interoperable, best practices; ...)
- Improving signal-to-noise (identifying sound crypto techniques)

Hesitation

- Many options (model, assumptions, parameters): which are useful?

**How to explore
the threshold space?**

Why Care about Threshold Schemes?

Attraction

- Feasible decentralized paradigm for key-management.
- Also an entry point to discovering more general MPC.



Goals

- Promote *good* **adoptability** (secure, interoperable, best practices; ...)
- Improving signal-to-noise (identifying sound crypto techniques)

Hesitation

- Many options (model, assumptions, parameters): which are useful?

**How to explore
the threshold space?**

**Next: A public Call for reference
material ... toward recommendations**

Outline

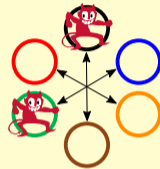
1. The MPTC project
2. **The NIST Threshold Call**
3. The MPTS 2026 Workshop

MPTC = Multi-Party Threshold Cryptography.
MPTS = Multi-Party Threshold Schemes.
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:

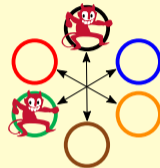
- It deals with **threshold** schemes
- It stands at the **threshold** of advanced cryptography



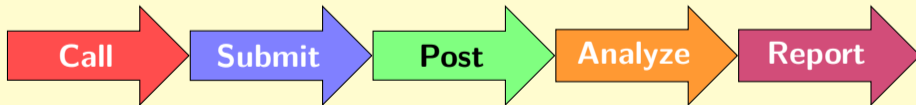
The NIST Call for *Multi-Party Threshold Schemes*

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



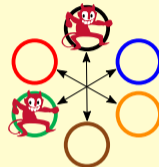
Establishes a process: (not a competition for selection of a standard)



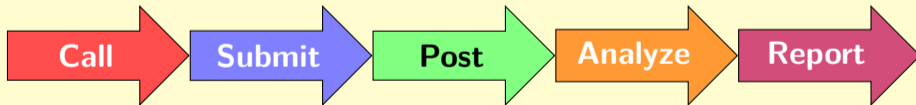
The NIST Call for *Multi-Party Threshold Schemes*

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

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

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](#))

Phases / Timeline

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

- Explain plan of upcoming package submissions
- Submit writeups by **Jan-12**, **Apr-20**, or **Jun-22**. (Then Preview talks)

Phases / Timeline

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

- Explain plan of upcoming package submissions
- Submit writeups by **Jan-12**, **Apr-20**, or **Jun-22**. (Then Preview talks)

Packages

- Tech. Specification, Ref. Implementation, Report Exp. Evaluation.
- Preliminary by **Jul-27–Sep-07** [for feedback]; complete by **Oct-19**.

Phases / Timeline

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

- Explain plan of upcoming package submissions
- Submit writeups by **Jan-12**, **Apr-20**, or **Jun-22**. (Then Preview talks)

Packages

- Tech. Specification, Ref. Implementation, Report Exp. Evaluation.
- Preliminary by **Jul-27–Sep-07** [for feedback]; complete by **Oct-19**.

Analysis

- Thorough presentations; MPTC report (\approx **2027**).

1st “Round” of Previews (January 2026)



Already posted: 26 Preview Writeups submitted by 23 teams.

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

| Team | . | Cat. | Team | . | Cat. | Team | . | Cat. |
|---------------|----|------|-------------|----|--------|-------------|----|---------|
| Amber | 4 | S2 | LEAST | 6 | S1/4 | RedETA | 6 | N1/4 |
| BBDL-tBLS | 4 | S1 | Mithril | 6 | N1/4 | Schmivitz | 8 | S6/7 |
| BDLR-Gargos | 4 | N1 | MPC-Minions | 14 | N1/4 | SmallWood | 2 | S6 |
| BICYCCLIST x2 | 4 | N1 | PANTHERIA | 26 | S5 | SplitForge | 10 | N1/4,S2 |
| Fireblocks x3 | 7 | N1/4 | PiVer | 10 | S7 | Symphony | 4 | N3,S7 |
| FROST | 12 | N1 | PQarrots | 30 | S1/2/4 | Tanuki | 12 | S1 |
| Haystack | 3 | N1 | Quorus | 5 | N1/4 | Vinaigrette | 9 | S1/4 |
| Hermine | 8 | S1/4 | | | | Zama | 13 | S4/5/6 |

Legend: Alphabetically ordered list of team names. |.| = Team size (number of members). Cat. = Categories. N1/S1 = Signing. N2/S2 = Public-Key Encryption/Decryption. N3/S3 = Symmetric (Ciphers and Hashing). N4 = KeyGen; S5 = FHE (Fully-Homomorphic Encryption). S6 = ZKPoK (Zero-Knowledge Proofs of Knowledge). S7 = Gadgets. N (prefix) = Class N (NIST specified primitives). S (prefix) = Class S (Other Special primitives).

Coverage of the First Set of Previews

NIST Signatures (N1)

- BDLR-Gargos
- BICYCCLIST
- Fireblocks
- Haystack
- FROST
- Mithril
- RedETA
- Quorus
- SplitForge

Symmetric (N3/S3)

- MPC MINlons
- Symphony

Non-NIST Signatures (S1)

- BBDL-tBLS
- Hermine
- LEAST
- PQarrots
- Tanuki
- Vinaigrette

Gadgets (S7)

- Fireblocks
- MPC MINlons
- PiVer
- Schmivitz
- Symphony
- Zama

PKE/KEM (S2)

- Amber
- Fireblocks
- PQarrots
- SplitForge

FHE (S5)

- PANTHERIA
- Zama

ZKP (S6)

- Schmivitz
- SmallWood
- Zama

(Not showing KeyGen categories N4/S4. Showing the team names, not the crypto-system names.)

Refined Coverage of Threshold Signatures

- **N1.1: EdDSA:** BDLR-Gargos; Fireblocks; FROST; RedETA
- **N1.2: ECDSA:** BICYCCLIST; Fireblocks; RedETA, SplitForge
- **N1.3: RSA:** SplitForge
- **S1: Non-NIST Sign:** BBDL-tBLS

Quantum
vulnerable

Refined Coverage of Threshold Signatures

- **N1.1: EdDSA:** BDLR-Gargos; Fireblocks; FROST; RedETA
- **N1.2: ECDSA:** BICYCCLIST; Fireblocks; RedETA, SplitForge
- **N1.3: RSA:** SplitForge
- **S1: Non-NIST Sign:** BBDL-tBLS

Quantum
vulnerable

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

Quantum
resistant

Refined Coverage of Threshold Signatures

- **N1.1: EdDSA:** BDLR-Gargos; Fireblocks; FROST; RedETA
- **N1.2: ECDSA:** BICYCCLIST; Fireblocks; RedETA, SplitForge
- **N1.3: RSA:** SplitForge
- **S1: Non-NIST Sign:** BBDL-tBLS

Quantum
vulnerable

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

Quantum
resistant

Signatures produced by N1.x schemes are verifiable with NIST-standardized verification

Main Components of a Submission Package

1. **Technical Specification:** Technical description; security analysis.
2. **Reference Implementation:** Open-source; distinguishes core-code from dependencies; includes execution and evaluation scripts.
3. **Experimental Evaluation:** Reports performance measurements (based on evaluation scripts), and interprets results.
4. **Notes on Patent Claims:** Lists known related patents, or claims none.

Note: The revised Call (i.e., since the 2pd) has an indexed list of requirements.

Selected Notes on Packages

Preparing a submission package

- Requires participating in a Preview phase.
- Teams can update their plans (e.g, combine crypto-systems, team composition).
- A LaTeX template will be available (February) for the written components.
- Preliminary submissions (Jul-27–Sep-07) for editorial-only feedback.

Selected Notes on Packages

Preparing a submission package

- Requires participating in a Preview phase.
- Teams can update their plans (e.g, combine crypto-systems, team composition).
- A LaTeX template will be available (February) for the written components.
- Preliminary submissions (Jul-27–Sep-07) for editorial-only feedback.

Analysis and discussion

- MPTC will hold a seminar series for thorough presentations by the teams.
- Comments about concrete submissions can be sent via the [MPTC-Forum](#).
- Expectation of MPTC-forum communication of newly found vulnerabilities.

Outline

1. The MPTC project
2. The NIST Threshold Call
3. **The MPTS 2026 Workshop**

MPTC = Multi-Party Threshold Cryptography.
MPTS = Multi-Party Threshold Schemes.
NIST = National Institute of Standards and Technology.

MPTS 2026 Sessions

| Day | Morning sessions | Afternoon sessions |
|-----------------|--|--|
| Jan-26 (Mon) | 1-0: Workshop Introduction 1a: Threshold Signatures: Schnorr/EdDSA | 1b: Threshold Signatures: BLS and Security |
| Jan-27 (Tue) | 2a: Threshold Signatures: ECDSA and others | 2b: Validation; FHE and Threshold FHE |
| Jan-28 (Wed) | 3a: Threshold Ciphers and Hashing | 3b: Threshold PQC Lattice-based Schemes |
| Jan-29 (Thu) | 4a: Threshold PQ Isogeny/Code-MV-based 4b: Misc. (RSA DKG, VSS, BB limitations) | 4c: Zero-Knowledge Proofs of Knowledge |

MPTS 2026 Brief Stats

A 4-day workshop

Many Talks

Time slots

Participants

MPTS 2026 Brief Stats

A 4-day workshop

Many talks

- 25 “Preview Talks”, 11 proposed/accepted talks, 4 invited talks
- And a few NIST-update talks

Time slots

Participants

MPTS 2026 Brief Stats

A 4-day workshop

Many talks

- 25 “Preview Talks”, 11 proposed/accepted talks, 4 invited talks
- And a few NIST-update talks

Time slots

- **Talk slots:** Most are **25 min** (some longer: T-FHE and T-Symmetric)
- **Breaks:** (5–10 min) within sessions; “lunch” break (≈ 1 h) between sessions

Participants

MPTS 2026 Brief Stats

A 4-day workshop

Many talks

- 25 “Preview Talks”, 11 proposed/accepted talks, 4 invited talks
- And a few NIST-update talks

Time slots

- **Talk slots:** Most are **25 min** (some longer: T-FHE and T-Symmetric)
- **Breaks:** (5–10 min) within sessions; “lunch” break (≈ 1 h) between sessions

Participants

- This morning: > 550 registered participants, from 50^+ indicated countries
- Stats will appear later on the webpage (more can register; fewer will join live)

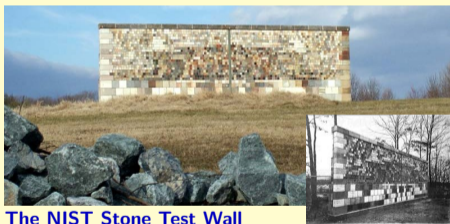
Guidelines for Virtual Participation

- **Code of Conduct:** Participation in [MPTS 2026](https://www.nist.gov/pao/code-conduct-nist-conferences) requires abiding to 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 workshop 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.



Thank You for Participating

NIST-MPTC wishes an insightful workshop to everyone.



The NIST Stone Test Wall

*Come place or study a new
“block” in the “wall” of
Crypto Reference Materials*

“Constructed [in 1948] to study the performance of stone subjected to weathering. It contains 2352 individual samples of stone, of which 2032 are domestic stone from 47 [U.S.] states, and 320 are stones from 16 foreign countries.”

Thank You for Your Attention!



**MPTS
2026**



**Threshold
Call**



**Submitted
Material**



**MPTC
Forum**

MPTS 2026 and the NIST Threshold Call: Introductory Notes

Presented at MPTS 2026 | @ Maryland (USA), January 26

luis.brandao@nist.gov