# NIST Threshold Call: Notes on the Upcoming Second Public Draft (2pd)

Presented<sup>\*</sup> at WPEC 2024:

NIST Workshop on Privacy-Enhancing Cryptography 2024 September 26, 2024 | Virtual (from Gaithersburg, USA)

Suggested reading: NISTIR 8214C ipd NIST First Call for Multi-Party Threshold Schemes (Initial Public Draft) [2023-Jan-25]



\* Luís Brandão (Foreign Guest Researcher (non-employee) at NIST, contractor from Strativia). Joint work with René Peralta.



1. Basics on the Threshold Call

2. Upcoming Second Public Draft

NIST = National Institute of Standards and Technology.



#### 1. Basics on the Threshold Call

2. Upcoming Second Public Draft

NIST = National Institute of Standards and Technology.

MPTC: Multi-Party Threshold Cryptography

**PEC:** Privacy-Enhancing Cryptography

Exploratory work to assess potential for recommendations, and standardization processes. Main approach: promote development of **reference material**.

MPTC: Multi-Party Threshold Cryptography

**PEC: Privacy-Enhancing Cryptography** 

Exploratory work to assess potential for recommendations, and standardization processes. Main approach: promote development of **reference material**.

#### MPTC: Multi-Party Threshold Cryptography

Threshold Schemes for diverse Cryptographic Primitives



PEC: Privacy-Enhancing Cryptography

Exploratory work to assess potential for recommendations, and standardization processes. Main approach: promote development of **reference material**.

#### MPTC: Multi-Party Threshold Cryptography

- Threshold Schemes for diverse 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., decrypt.

#### PEC: Privacy-Enhancing Cryptography



**MPC** = Secure **M**ulti**p**arty **C**omputation

Exploratory work to assess potential for recommendations, and standardization processes. Main approach: promote development of **reference material**.

#### MPTC: Multi-Party Threshold Cryptography

- Threshold Schemes for diverse 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., decrypt.

#### PEC: Privacy-Enhancing Cryptography

"Advanced crypto" usable to enhance privacy (See talk 1a1).



**MPC** = Secure **M**ulti**p**arty **C**omputation

Exploratory work to assess potential for recommendations, and standardization processes. Main approach: promote development of **reference material**.

#### MPTC: Multi-Party Threshold Cryptography

- Threshold Schemes for diverse 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., decrypt.

#### PEC: Privacy-Enhancing Cryptography



**MPC** = Secure **M**ulti**p**arty **C**omputation

"Advanced crypto" usable to enhance privacy (See talk 1a1).

The "Threshold Call" (from MPTC+PEC): to gather reference material for public analysis ... aiming for recommendations (in a 1st phase), including about PEC.

► NISTIR 8214C ipd: initial public **draft** (Jan. 2023).

- ► NISTIR 8214C ipd: initial public **draft** (Jan. 2023).
- Calling for submissions of threshold schemes for diverse primitives:



- ► NISTIR 8214C ipd: initial public **draft** (Jan. 2023).
- Calling for submissions of threshold schemes for diverse primitives:
- Cat1: Selected NIST-standardized primitives

Cat2: Primitives not specified by NIST



- ► NISTIR 8214C ipd: initial public **draft** (Jan. 2023).
- Calling for submissions of threshold schemes for diverse primitives:
- Cat1: Selected NIST-standardized primitives
  - EdDSA, ECDSA, RSA, AES, ECC-KE, ...
- Cat2: Primitives not specified by NIST



AES = Advanced Encryption Standard. EC = Elliptic curve. ECC-KE = EC cryptography (based) key-exchange. EdDSA = Edwards-Curve digital signature algorithm. ECDSA = EC digital signature algorithm. FHE = Fully-homomorphic encryption. IBE = Identity-based encryption. NIST = National institute of Standards and Technology. PEC = Privacy-enhancing cryptography. RSA = Rivest–Shamir–Adleman. ZKP = Zero-knowledge proof.

► NISTIR 8214C ipd: initial public **draft** (Jan. 2023).

Calling for submissions of threshold schemes for diverse primitives:

- ► Cat1: Selected NIST-standardized primitives
  - EdDSA, ECDSA, RSA, AES, ECC-KE, ...
- ► Cat2: Primitives not specified by NIST
  - Interest in threshold friendliness and quantum resistance
  - Interest in other primitives, including FHE, ZKP, and gadgets

AES = Advanced Encryption Standard. EC = Elliptic curve. ECC-KE = EC cryptography (based) key-exchange. EdDSA = Edwards-Curve digital signature algorithm. ECDSA = EC digital signature algorithm. FHE = Fully-homomorphic encryption. IBE = Identity-based encryption. NIST = National Institute of Standards and Technology. PEC = Privacy-enhancing cryptography. RSA = Rivest–Shamir–Adleman. ZKP = Zero-knowledge proof.

4/11



## Wide dissemination

- Publication of draft in Jan. 2023, open to public comments.
- ▶ Presented (10<sup>+</sup>) and socialized at a variety of crypto events/conferences
- Baseline positioning reports: NISTIR 8214 series
- Related workshops: MPTS 2020 & 2023, PEC STPPA #6
- Calls for public comments: Call 2021 about criteria, Call on IR 8214C ipd (2023)

## Wide dissemination

- Publication of draft in Jan. 2023, open to public comments.
- ▶ Presented (10<sup>+</sup>) and socialized at a variety of crypto events/conferences
- Baseline positioning reports: NISTIR 8214 series
- Related workshops: MPTS 2020 & 2023, PEC STPPA #6
- Calls for public comments: Call 2021 about criteria, Call on IR 8214C ipd (2023)

## Wide dissemination

- Publication of draft in Jan. 2023, open to public comments.
- ▶ Presented (10<sup>+</sup>) and socialized at a variety of crypto events/conferences
- Baseline positioning reports: NISTIR 8214 series
- Related workshops: MPTS 2020 & 2023, PEC STPPA #6
- Calls for public comments: Call 2021 about criteria, Call on IR 8214C ipd (2023)

Multiple expressions of interest / encoragement:

- to submit threshold schemes
- about the outcome of the process



**1. Basics on the Threshold Call** 

2. Upcoming Second Public Draft

NIST = National Institute of Standards and Technology.

# Soon upcoming Second Public Draft (2pd)

Open to a short period of public comments. Intended very close to the final version.

Related updates (compared with the ipd):

- Will indicate deadlines:
- **Specification**:
- **Reference implementation:**
- **Subcategories:**

# Soon upcoming Second Public Draft (2pd)

Open to a short period of public comments. Intended very close to the final version. Related updates (compared with the ipd):

- **Will indicate deadlines:**  $\geq$  2025-Jan for abstracts;  $\geq$  2025-June for packages.
- **Specification:** Allow multiple (related) "crypto-systems" by various sub-teams.
- **Reference implementation:** Allow external open-source dependencies.
- Subcategories: PQC primitives added to Cat1; "FHE" instead of "Advanced" in Cat2.

# Soon upcoming Second Public Draft (2pd)

Open to a short period of public comments. Intended very close to the final version. Related updates (compared with the ipd):

- **Will indicate deadlines:**  $\geq$  2025-Jan for abstracts;  $\geq$  2025-June for packages.
- **Specification:** Allow multiple (related) "crypto-systems" by various sub-teams.
- Reference implementation: Allow external open-source dependencies.
- Subcategories: PQC primitives added to Cat1; "FHE" instead of "Advanced" in Cat2.

Some related comments have been being posted in the MPTC-Forum

Subscribe to the MPTC forum for upcoming announcements.

## Category <u>Cat1</u> of the NIST Threshold Call

Subcategory: Type	Families of specifications
C1.1: Signing	[PreQ] <u>EdDSA</u> sign; <u>ECDSA</u> sign; <u>RSADSA</u> sign
	[QR stateless] <u>ML-DSA</u> sign; <u>SLH-DSA</u> sign; Falcon (to appear) sign
	[QR stateful]: <u>XMSS</u> sign; <u>LMS</u> sign
C1.2: PKE	[PreQ] <u>RSA</u> encryption & decryption
	[QR] <u>ML-KEM</u> encryption & decryption
C1.3: 2KA	ECC-CDH & ECC-MQV primitives
C1.4: Symmetric	Key-based: $\underline{AES}$ (blockcipher) & $\underline{ASCON}$ (AEAD) encipher and decipher; $\underline{C/H/K}$ -MAC
	Key-less: <u>SHA2</u> & <u>SHA3</u> hash; <u>Keccak</u> & <u>ASCON</u> XOF
C1.5: Keygen (aka DKG)	ECC keygen; RSA keygen; bitstring keygen; QR keygen for ML, SLH, Falcon, and stateful-HBS

Source: https://csrc.nist.gov/projects/threshold-cryptography

# Category Cat2 of the NIST Threshold Call

Subcategory: Type	Example scheme	Example primitive
C2.1: Signing	TF succinct & verifiable-deterministic signatures	Sign
	TF-QR signatures	Sign
C2.2: PKE	TF-QR <b>p</b> ublic- <b>k</b> ey <b>e</b> ncryption (PKE)	Decrypt; encrypt (a secret value)
C2.3: KA	Low-round multi-party <b>k</b> ey- <b>a</b> greement (KA)	Single-party primitives
C2.4: Symmetric	TF PRP (e.g., blockcipher) or PRF (e.g., for MAC or key-derivation)	Encipher, decipher, MAC
	Hash or XOF	Hash function, XOF
C2.5: Keygen	Any of the above or below	Keygen
C2.6: FHE	QR <b>F</b> ully- <b>h</b> omomorphic <b>e</b> ncryption (FHE)	Decryption; keygens
C2.7: ZKPoK	ZKPoK of private key	ZKPoK.Generate
C2.8: Gadgets	<b>G</b> arbled <b>c</b> ircuit (GC)	GC.generate; GC.evaluate

Source: https://csrc.nist.gov/projects/threshold-cryptography

### **General remarks**

- Wide scope: many primitives (including MPC, ZKP, FHE)
- Many possibilities: threshold profiles, network models, crypto assumptions Each submission will properly motivate its focus(es)
- Will form a body of reference material (not a "competition"), with high impact for future recommendation/processes
- ▶ Work developed with other SDOs and in community efforts is welcome.
- We'll start a "Threshold Crypto" Seminar series after the Abstracts are submitted
- It's been taking time since the draft: submissions will come in 2025.

Thank you for your attention! Questions?

NIST Threshold Call: Notes on the Upcoming Second Public Draft (2pd)

Presented at WPEC 104

September 26, 2024 @ Virtual (from Gaithersburg, USA) — luis.brandao@nist.gov

- NISTIR 8214C ipd: https://csrc.nist.gov/publications/detail/nistir/8214c/draft
- Send comments about the call to: nistir-8214C-comments@nist.gov
- MPTC Website: https://csrc.nist.gov/projects/threshold-cryptography
- Subscribe to the MPTC-Forum: https://list.nist.gov/MPTC-forum
- PEC Website: https://csrc.nist.gov/projects/pec
- Subscribe to the PEC-Forum: https://list.nist.gov/PEC-forum