NIST First Call for Multi-Party Threshold Schemes

Notes presented* at the TPMPC 2023 Workshop:

Theory and Practice of Multi-Party Computation

June 09, 2023 | Aarhus (Denmark)

Suggested reading: NISTIR 8214C ipd

NIST First Call for Multi-Party Threshold Schemes
(Initial Public Draft) [2023-Jan-25]

* Luís Brandão: At NIST as a Foreign Guest Researcher (non-employee), Contractor from Strativia. Expressed opinions are from the speaker and should not be construed as official NIST views. Joint work with René Peralta.
Outline

1. NIST Introduction

2. The “Threshold” Call

3. The Process

NIST = National Institute of Standards and Technology.
NIST: Laboratories → Divisions → Groups

- **Non-regulatory** federal agency (@ U.S. Dept. Commerce)
- **Mission:** ... innovation ... industrial competitiveness ... measurement science, standards, and technology ... economic security ... quality of life.

[Image: NIST name and address plate (source: nist.gov)]

→ **Computer Security Division (CSD):**

[Image: ITL INFORMATION TECHNOLOGY LABORATORY]

→ **Cryptographic Technology Group (CTG):** *research, develop, engineer, and produce guidelines, recommendations and best practices for cryptographic algorithms, methods, and protocols.*
Activities in the “Crypto” Group

- Public documentation: FIPS; Special Publications (SP 800); NIST Reports (IR).
- International cooperation: government, industry, academia, standardization bodies.


More details at https://www.nist.gov/itl/csd/cryptographic-technology
Intro: NIST has various Crypto Projects

- **PQC**: [standardization] “post-quantum” signatures and key-encapsulation
- **LWC**: [standardization] “lightweight” Auth. Enc. w/ Assoc. Data, and hashing
- **PEC**: [exploratory] “privacy-enhancing” (advanced) features/functionalities
- **MPTC**: [exploratory] “multi-party threshold” schemes for crypto primitives
- ... (various other projects in the NIST “Crypto group” [CTG])

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

On the PEC and MPTC projects

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

PEC: Privacy-Enhancing Cryptography

- Crypto (that can be) used to enhance privacy [emphasis on non-standardized tools].

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.
Outline

1. NIST Introduction
2. The “Threshold” Call
3. The Process

NIST = National Institute of Standards and Technology.
NIST Call for Multi-Party Threshold Schemes

▶ NISTIR 8214C ipd: initial public draft (Jan. 2023).
▶ Final version (by ≈ Nov. 2023) will specify submission deadline (≈ mid 2024))

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 “advanced” primitives from PEC: FHE, IBE, ZKP, ...

## Category Cat1 of NIST Call for Multi-Party Threshold Schemes

Too many acronyms, we know. *(Legend further below)*

<table>
<thead>
<tr>
<th>Subcategory: Type</th>
<th>Families of specifications</th>
<th>NIST references</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>C1.1: Signing</strong></td>
<td>EdDSA sign, ECDSA sign, RSADSA sign</td>
<td>FIPS 186-5 (see also NISTIR 8214B)</td>
</tr>
<tr>
<td><strong>C1.2: PKE</strong></td>
<td>RSA decrypt, RSA encrypt (a secret value)</td>
<td>SP 800-56B Rev2</td>
</tr>
<tr>
<td><strong>C1.3: 2KA</strong></td>
<td>EC-CDH, EC-MQV</td>
<td>SP 800-56A Rev3</td>
</tr>
<tr>
<td><strong>C1.4: Symmetric</strong></td>
<td>AES encipher/decipher, KDM/KC (for 2KE)</td>
<td>FIPS 197, SP 800-56C Rev2, ...</td>
</tr>
<tr>
<td><strong>C1.5: Keygen</strong></td>
<td>EC keygen, RSA keygen, bitstring keygen</td>
<td>(corresponding references above)</td>
</tr>
</tbody>
</table>

### Category Cat2 of the NIST “Threshold” Call

**TF** = threshold friendly. **QR** = quantum resistant.

<table>
<thead>
<tr>
<th>Subcategory: Type</th>
<th>Example types of schemes</th>
<th>Example primitives</th>
</tr>
</thead>
<tbody>
<tr>
<td>C2.1: <strong>Signing</strong></td>
<td>TF succinct &amp; verifiably-deterministic signatures</td>
<td>Sign</td>
</tr>
<tr>
<td></td>
<td>TF-QR signatures</td>
<td>Sign</td>
</tr>
<tr>
<td>C2.2: <strong>PKE</strong></td>
<td>TF-QR public-key encryption (PKE)</td>
<td>Decrypt/Encrypt (a secret value)</td>
</tr>
<tr>
<td>C2.3: <strong>Key agreem.</strong></td>
<td>TF Low-round multi-party key-agreement (KA)</td>
<td>Single-party primitives</td>
</tr>
<tr>
<td>C2.4: <strong>Symmetric</strong></td>
<td>TF blockcipher/PRP</td>
<td>Encipher/decipher</td>
</tr>
<tr>
<td></td>
<td>TF key-derivation / key-confirmation</td>
<td>PRF and hash function</td>
</tr>
<tr>
<td>C2.5: <strong>Keygen</strong></td>
<td>Any of the above</td>
<td>Keygen</td>
</tr>
<tr>
<td>C2.6: <strong>Advanced</strong></td>
<td>TF-QR fully-homomorphic encryption</td>
<td>Decryption; Keygen</td>
</tr>
<tr>
<td></td>
<td>TF identity-based and attribute-based encryption</td>
<td>Decryption; Keygens</td>
</tr>
<tr>
<td>C2.7: <strong>ZKPoK</strong></td>
<td>Zero-knowledge proof of knowledge of private key</td>
<td>ZKPoK.Generate</td>
</tr>
<tr>
<td>C2.8: <strong>Gadgets</strong></td>
<td>Garbled circuit (GC), broadcast, ...</td>
<td>GC.generate; GC.evaluate, ...</td>
</tr>
</tbody>
</table>

**Note:** While **TF-QR** is a desired combination for any type of scheme, some examples show just **TF** to highlight that it is welcome even if not **QR**.

**Legend:** agreem. = agreement. Keygen = key-generation. PKE = public-key encryption. PRF = pseudorandom function [family]. PRP = pseudorandom permutation [family]. QR = quantum resistant. TF = threshold-friendly. ZKPoK = zero knowledge proof of knowledge.
Main components of a submission package

<table>
<thead>
<tr>
<th>Check</th>
<th>#</th>
<th>Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>□</td>
<td>M1</td>
<td>Written specification (S1–S16)</td>
</tr>
<tr>
<td>□</td>
<td>M2</td>
<td>Reference implementation (Src1–Src4)</td>
</tr>
<tr>
<td>□</td>
<td>M3</td>
<td>Execution instructions (X1–X7)</td>
</tr>
<tr>
<td>□</td>
<td>M4</td>
<td>Experimental evaluation (Perf1–Perf5)</td>
</tr>
<tr>
<td>□</td>
<td>M5</td>
<td>Additional statements</td>
</tr>
</tbody>
</table>

- (Optional) early public abstract: \(\approx 3\) months after final call.
- (Optional) preliminary submission to check completeness: \(\approx 45\) days before deadline.
- Package-submission: by the submission deadline.

Tentative timeframes (subject to change)
Some technical notes

1. Submission focuses: can specify a family of schemes (in various subcategories).

2. Threshold profile: open to choice: number of parties; dishonest proportion; ...

3. Active security: it is required, though open to diverse security formulations.

4. Adaptive security: at least “argued for” for major safety properties,

5. Modularity: modularize gadgets; encouraged proactive resharing module; ...

6. Post-vs-Pre quantum crypto: both in scope; pre-QC requires justification.

7. Concrete implementation: e.g., including communication (e.g., broadcast? P2P?).
Expected revisions in the call

1. In Cat1, add subcategories for the NIST-selected PQC primitives

2. In Cat2, differentiate better some subcategories (e.g., FHE; what can be thresholdized)

3. Clarify scope of “gadgets” subcategory (and how to motivate them)

4. Detail better some logistic requirements (e.g., code licensing)

5. Include LaTeX template for submission
Outline

1. NIST Introduction

2. The “Threshold” Call

3. The Process

NIST = National Institute of Standards and Technology.
Tentative timeline

- **2023-Jul**: Revised version of the Call

- **2023-Sep**: Virtual workshop for feedback & awareness (TBA, likely Sep 26–28)

- **2023-Nov**: Final version of the call

- ≈ **Mid 2024**: Deadline for submissions

- **2024/2025**: Workshop(s) for characterization / analysis of submitted schemes

- ≥ **2025**: Initial recommendations (and new processes?)
Community participation

Various areas / possible synergies:

- Scope of the call is of interest to various crypto communities: MPC, ZKP, FHE, ...
- Work developed with other SDOs and in community efforts is also welcome.

(SDO = Standards Development Organization)

Some variables:

- How will the community compose teams? (How to avoid effort duplication?)
- How will the scope of the call be covered? (primitives / models / approaches)

Upcoming soon: Threshold Workshop (≈ Sep 26–28) [about revised call (≈ July)]
Welcome/needed interaction

1. **Feedback after the revised call (≥ July):**
   - Suggested improvements to the Call
   - What schemes should be submitted
   - Your possible intention to submit (what?)

2. **Concrete submissions (≈ Mid 2024):**
   - Structured specification, open source implementation, evaluation, ...

3. **Public scrutiny of submitted schemes (≥ 2024/2025):**
   - Evaluation comments (can impact subsequent recommendations)
Concluding remarks

▶ **Setup:** A gathering of reference material (not a competition for a selection).

▶ **Expected:** The process will clarify relevant system models, best practices, ...

▶ **Aim:** Devise recommendations about advanced cryptography (PEC + MPTC) (Will support future standardization processes.)

▶ **Ample room for participation:** Give feedback → Submit → Analyze

▶ **It’s time:** Consider starting to organize a future submission (team, scope, ...)
Thank you for your attention! Questions?

_NIST First Call for Multi-Party Threshold Schemes_

Notes presented at the TPMPC 2023 Workshop

June 09, 2023 @ Aarhus (Denmark) — 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