Updates on the NIST Threshold Call

(The 2nd Public Draft and the FHE Category)

HES8: 8th HomomorphicEncryption.org Standards Meeting

2025-Mar-23 @ Istambul, Turkey

Presented virtually from Maryland, USA, by Luís Brandão, NIST Foreign Associate (Guest Researcher, non-employee), Contractor from Strativia. Expressed opinions are from the speaker. The Threshold Call is joint work with René Peralta.

Preamble

1. **Thank you** for the invite
2. **Presentation goals:**
   - A preview of the Threshold Call 2nd public draft
   - Motivate engagement with the envisioned process
3. **Disclaimer:** Details may change until the final version is published

Outline

1. **The Threshold Call**

2. **Upcoming 2nd Public draft (2pd)**

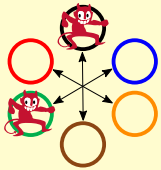
3. **Notes on FHE**

Outline

1. **The Threshold Call**
2. **Upcoming 2nd Public draft (2pd)**
3. **Notes on FHE**

The NIST Call for *Multi-Party Threshold Schemes*

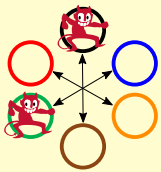
A public call for input, to form a body of reference material:



- 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:

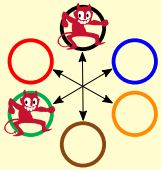


- It deals with **threshold** schemes
- It stands at the **threshold** of advanced cryptography

Fits within the **exploratory "Reference Materials" approach** of the NIST projects on Privacy-Enhancing Cryptography (PEC) and Multi-Party Threshold Cryptpgraphy (MPTC).

The NIST Call for *Multi-Party Threshold Schemes*

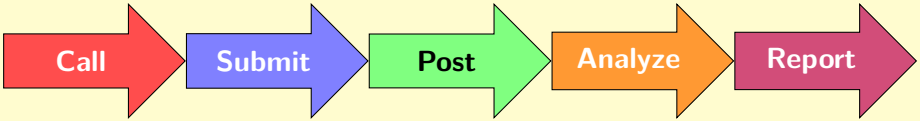
A public call for input, to form a body of reference material:



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

Fits within the **exploratory "Reference Materials" approach** of the NIST projects on Privacy-Enhancing Cryptography (PEC) and Multi-Party Threshold Cryptpgraphy (MPTC).

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



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-Homomoprhic Encryption; ZKP = Zero-Knolwedge Proof

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-Homomoprhic Encryption; ZKP = Zero-Knolwedge Proof

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

Using notation of upcoming 2nd public draft (different from initial public draft)

Outline

1. The Threshold Call
2. **Upcoming 2nd Public draft (2pd)**
3. Notes on FHE

Phases and Deadlines

Phase	Subphase	Required?	Deadline
1. Previews	1.1: Preview 1	No	≈**X+2**
	1.2: Preview 2	No	≈**X+5**
2. Packages	2.1: Preliminary submission	No	≈**X+6**
	2.2: Regular submission	**Yes**	≈**X+8**
3. Analysis	3.1: Public presentations	**Yes**	(2026)
	3.2: Package updates	—	—
	3.3: NIST-MPTC report	**Yes**	(≈ 2027)

Tentative deadlines are relative (unit in months) to the publication date (X) of the final version of the Call.

Phases and Deadlines

Phase	Subphase	Required?	Deadline
1. Previews	1.1: Preview 1	No	≈**X+2**
	1.2: Preview 2	No	≈**X+5**
2. Packages	2.1: Preliminary submission	No	≈**X+6**
	2.2: Regular submission	**Yes**	≈**X+8**
3. Analysis	3.1: Public presentations	**Yes**	(2026)
	3.2: Package updates	—	—
	3.3: NIST-MPTC report	**Yes**	(≈ 2027)

Tentative deadlines are relative (unit in months) to the publication date (X) of the final version of the Call.

- **Preview:** abstract of a planned submission, followed by public presentation
- **Package:** specification, implementation, experimental evaluation
- **Analysis:** including seminar series

Submission of Packages (3 main components)

- **Written specification:**
- **Reference implementation:**
- **Experimental evaluation:**

Submission of Packages (3 main components)

- **Written specification:** (PDF file, with description and security analysis)
  - The conventional scheme (e.g, FHE) can be specified thoroughly or by reference.
  - The threshold scheme (e.g., for decryption) must be specified.
- **Reference implementation:**
- **Experimental evaluation:**

Submission of Packages (3 main components)

- **Written specification:** (PDF file, with description and security analysis)
  - The conventional scheme (e.g, FHE) can be specified thoroughly or by reference.
  - The threshold scheme (e.g., for decryption) must be specified.
- **Reference implementation:** (Link/commitment to Git-compatible repository)
  - **Open source**; can rely on open-source external dependencies.
  - Including **scripts** to compile/install and execute (on Ubuntu).
- **Experimental evaluation:**

Submission of Packages (3 main components)

- **Written specification:** (PDF file, with description and security analysis)
  - The conventional scheme (e.g, FHE) can be specified thoroughly or by reference.
  - The threshold scheme (e.g., for decryption) must be specified.
- **Reference implementation:** (Link/commitment to Git-compatible repository)
  - **Open source**; can rely on open-source external dependencies.
  - Including **scripts** to compile/install and execute (on Ubuntu).
- **Experimental evaluation:** (PDF file with report)
  - Measurements / interpretation of results from running the execution script.
  - Metrics (whole and per party): memory, time, communication (bytes and rounds).

Submission of Packages (3 main components)

- **Written specification:** (PDF file, with description and security analysis)
  - The conventional scheme (e.g, FHE) can be specified thoroughly or by reference.
  - The threshold scheme (e.g., for decryption) must be specified.
- **Reference implementation:** (Link/commitment to Git-compatible repository)
  - **Open source**; can rely on open-source external dependencies.
  - Including **scripts** to compile/install and execute (on Ubuntu).
- **Experimental evaluation:** (PDF file with report)
  - Measurements / interpretation of results from running the execution script.
  - Metrics (whole and per party): memory, time, communication (bytes and rounds).

Note: A submission can propose multiple crypto-systems. Each can be attributed to a distinct subteam.

Implied agreement; License; Disclosure

- **Specification and evaluation report:**
- **Implementation:**
- **Patents:**

(Text/format under internal review)

Implied agreement; License; Disclosure

- **Specification and evaluation report:**
  - — Freely available worldwide for review and evaluation
  - — Allow NIST to post; encouraged CC BY 4.0 license for redistributability
- **Implementation:**
- **Patents:**

(Text/format under internal review)

Implied agreement; License; Disclosure

- **Specification and evaluation report:**
  - — Freely available worldwide for review and evaluation
  - — Allow NIST to post; encouraged CC BY 4.0 license for redistributability
- **Implementation:** Code licensed as Open-source (per Open Source Initiative)
- **Patents:**

(Text/format under internal review)

Implied agreement; License; Disclosure

- **Specification and evaluation report:**
  - — Freely available worldwide for review and evaluation
  - — Allow NIST to post; encouraged CC BY 4.0 license for redistributability
- **Implementation:** Code licensed as Open-source (per Open Source Initiative)
- **Patents:** Required disclosure (in a section of the specification) of known related patents associated with any submitter

(Text/format under internal review)

Outline

FHE in the Threshold Call

Category S5 (FHE), adapted from old "C2.6. Advanced"

- **FHE scheme specification:**
- **Threshold scheme:**
- **One instantiation:**
- **Performance evaluation:**

FHE in the Threshold Call

Category S5 (FHE), adapted from old "C2.6. Advanced"

- **FHE scheme specification:** Thoroughly as a proposed crypto-system, or at a high-level (interface, terminology, properties) in a preliminaries section (and reference a free spec).
- **Threshold scheme:**
- **One instantiation:**
- **Performance evaluation:**

FHE in the Threshold Call

Category S5 (FHE), adapted from old "C2.6. Advanced"

- **FHE scheme specification:** Thoroughly as a proposed crypto-system, or at a high-level (interface, terminology, properties) in a preliminaries section (and reference a free spec).
- **Threshold scheme:** At least for decryption, or encryption of a secret-shared value.
- **One instantiation:**
- **Performance evaluation:**

FHE in the Threshold Call

Category S5 (FHE), adapted from old "C2.6. Advanced"

- **FHE scheme specification:** Thoroughly as a proposed crypto-system, or at a high-level (interface, terminology, properties) in a preliminaries section (and reference a free spec).
- **Threshold scheme:** At least for decryption, or encryption of a secret-shared value.
- **One instantiation:** Aim for security level $\kappa \gtrsim 128$ (classic) or $\theta \geq 1$ (quantum)
- **Performance evaluation:**

FHE in the Threshold Call

Category S5 (FHE), adapted from old "C2.6. Advanced"

- **FHE scheme specification:** Thoroughly as a proposed crypto-system, or at a high-level (interface, terminology, properties) in a preliminaries section (and reference a free spec).
- **Threshold scheme:** At least for decryption, or encryption of a secret-shared value.
- **One instantiation:** Aim for security level $\kappa \gtrsim 128$ (classic) or $\theta \geq 1$ (quantum)
- **Performance evaluation:** At least the threshold scheme. **Also encouraged:** conventional (non-threshold) FHE scheme, with actual homomorphic evaluation.

  Note: use cases are not prescribed; suggestions from HES will be useful for future comparisons.

Concluding remarks

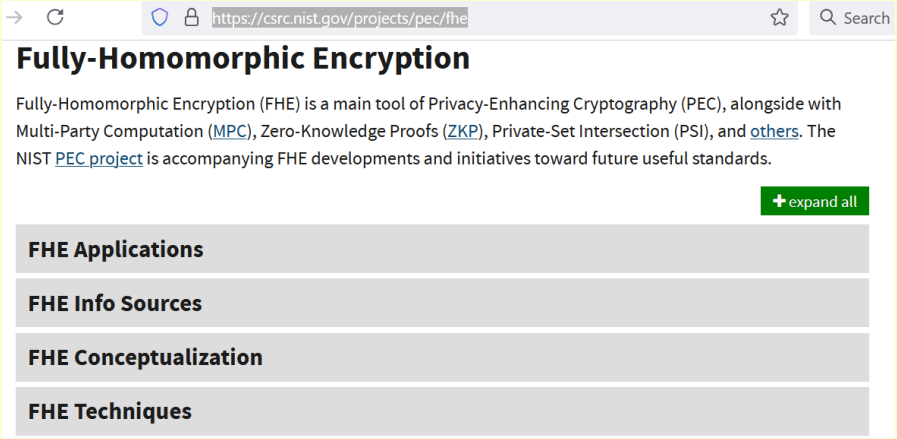
- **The Threshold Call acknowledges the HE community drive**
  - Corresponding FHE submissions are welcome.
  - The analysis will also rely on community contributions.

Concluding remarks

- **The Threshold Call acknowledges the HE community drive**
  - Corresponding FHE submissions are welcome.
  - The analysis will also rely on community contributions.
- **The process is tapping into advanced cryptography**
  - Including FHE in the Threshold Call allows a robust exploratory process.
  - The results will support a future report (recommendations, ...).

A PEC/FHE webpage

The PEC project website includes an FHE page (feedback welcome)



Thank you for your attention!

Updates on the NIST Threshold Call

(The 2nd Public Draft and the FHE Category)

luis.brandao@nist.gov

Presented (virtually from Maryland, USA) on March 23, 2025
HES8: 8th HomomorphicEncryption.org Standards Meeting

Useful links:

- **MPTC Website:** https://csrc.nist.gov/projects/threshold-cryptography
- **Subscribe to the MPTC-Forum:** https://csrc.nist.gov/projects/mptc/email-list
- **Upcoming second public draft:** https://csrc.nist.gov/pubs/ir/8214/c/2pd