NIST First Call for Multi-Party Threshold Schemes

Notes presented* at the TPMPC 2023 Workshop:

Theory and **P**ractice of **M**ulti-**P**arty **C**omputation

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

NIST = National Institute of Standards and Technology.

NIST: Laboratories → Divisions → Groups

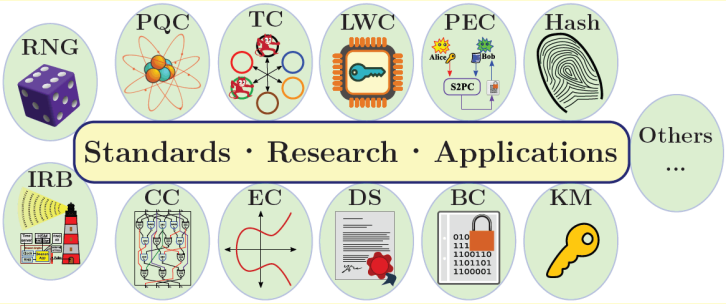
- **Non-regulatory** federal agency (@ U.S. Dept. Commerce)
- **Mission:** ... innovation ... industrial competitiveness ... measurement science, standards, and technology ... economic security ... quality of life.

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

INFORMATION TECHNOLOGY LABORATORY → **Computer Security Division (CSD):**

→ **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.

Legend: **BC** = **B**lock **C**iphers. **CC** = **C**ircuit **C**omplexity. **Crypto** = **Crypto**graphy. **DS** = **D**igital **S**ignatures. **EC** = **E**lliptic **C**urves. **FIPS** = **F**ederal **I**nformation **P**rocessing **S**tandards. **IR** = **I**nternal or **I**nteragency (denoting that the public NIST report was developed internally at NIST or in an interagency collaboration, respectively. **IRB** = **I**nteroperable **R**andomness **B**eacons. **KM** = **K**ey **M**anagement. **LWC** = **L**ightweight **C**rypto. **PEC** = **P**rivacy-**E**nhancing **C**rypto. **PQC** = **P**ost-**Q**uantum **C**rypto. **RNG** = **R**andom-**N**umber **G**eneration. **SP 800** = **S**pecial **P**ublications in Computer Security. **TC** = [Multi-Party] **T**hreshold **C**rypto).

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**" **A**uth. **E**nc. w/ **A**ssoc. **D**ata, 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.

Legend: AEAD = **A**uth[enticated] **E**nc[ryption] w[ith] **A**ssoc[iated] **D**ata. **CTG** = **C**ryptographic **T**echnology **G**roup. **LWC** = **L**ightweight **C**ryptography. **MPTC** = **M**ulti-**P**arty **T**hreshold **C**ryptography. **NIST** = **N**ational **I**nstitute of **S**tandards and **T**echnology. **PEC** = **P**rivacy-**E**nhancing **C**ryptography. **PQC** = **P**ost-**Q**uantum **C**ryptography.

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

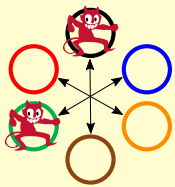
- Crypto (that can be) used to enhance privacy [emphasis on non-standardized tools].

ZKP	MPC	FHE	PSI	GRS	FnE	PIR	StE
Zero- **K**nowledge **P**roofs	(**S**ecure) **M**ulti**p**arty **C**omputation	**F**ully **H**omomorphic **E**ncryption	**P**rivate **S**et **I**ntersection	**G**roup and **R**ing **S**ignatures	**Fn**ctional **E**ncryption (Inc. ABE & IBE)	**P**rivate **I**nformation **R**etrieval	**St**ructured **E**ncryption (Symm./Pub.)

Legend: ABE: attribute-based encryption. IBE: identity-based encryption. Symm./pub.: symmetric-key or public-key based.

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**

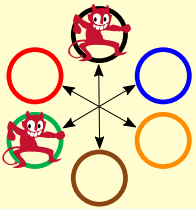
NIST = National Institute of Standards and Technology.

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, ...



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.

Category Cat1 of NIST Call for Multi-Party Threshold Schemes

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

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

Legend: 2KA: **pair**-wise **k**ey-agreement. **2KE**: **pair**-wise **k**ey-establisment. **AES**: **A**dvanced **E**ncryption **S**tandard. **CDH**: cofactor **D**iffie–**H**ellman. **ECC**: **E**lliptic-**c**urve **c**ryptography (or, if used as an adjective, **EC**-based). **ECDSA**: **E**lliptic-**c**urve **D**igital **S**ignature **A**lgorithm. **EdDSA**: **Ed**wards-curve **D**igital **S**ignature **A**lgorithm. **E**lliptic-curve based **K**ey-**E**stablishment. **FIPS**: **F**ederal **I**nformation **P**rocessing **S**tandard. **KC**: **K**ey-**c**onfirmtion. **KDM**: **K**ey-**d**erivation **m**echanism. **Keygen**: **K**ey-**gen**eration. **MQV**: Menezes-Qu-Vanstone. **PKE**: **p**ublic-**k**ey **e**ncryption. **RSA**: **R**ivest–**S**hamir–**A**dleman (signature and encryption schemes). **RSADSA**: **RSA** digital signature algorithm. **SP 800**: **S**pecial **P**ublication (in Computer Security). **Note:** In the 2nd column, each item within a subcategory is itself called a family of specifications, since it may include diverse primitives or modes/variants.

Category Cat2 of the NIST "Threshold" Call

TF = **t**hreshold **f**riendly. QR = **q**uantum **r**esistant.

Subcategory: Type	Example types of schemes	Example primitives
C2.1: **Signing**	TF succinct & verifiably-deterministic signatures	Sign
|	TF-QR signatures	Sign
C2.2: **PKE**	TF-QR **p**ublic-**k**ey **e**ncryption (PKE)	Decrypt/Encrypt (a secret value)
C2.3: **Key agreem.**	TF Low-round multi-party **k**ey-**a**greement (KA)	Single-party primitives
C2.4: **Symmetric**	TF blockcipher/PRP	Encipher/decipher
|	TF key-derivation / key-confirmation	PRF and hash function
C2.5: **Keygen**	Any of the above	Keygen
C2.6: **Advanced**	TF-QR fully-homomorphic encryption	Decryption; Keygen
|	TF identity-based and attribute-based encryption	Decryption; Keygens
C2.7: **ZKPoK**	**Z**ero-**k**nowledge **p**roof **o**f **k**nowledge of private key	ZKPoK.Generate
C2.8: **Gadgets**	Garbled circuit (GC), broadcast, ...	GC.generate; GC.evaluate, ...

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. = **agreem**ent. **Keygen** = **key-gen**eration. **PKE** = **p**ublic-**k**ey **e**ncryption. **PRF** = **p**seudorandom **f**unction [family]. **PRP** = **p**seudorandom **p**ermutation [family]. **QR** = **q**uantum **r**esistant. **TF** = **t**hreshold-**f**riendly. **ZKPoK** = **z**ero **k**nowledge **p**roof **o**f **k**nowledge.

Main components of a submission package

Check	#	Item
☐	M1	Written specification (S1–S16)
☐	M2	Reference implementation (Src1–Src4)
☐	M3	Execution instructions (X1–X7)
☐	M4	Experimental evaluation (Perf1–Perf5)
☐	M5	Additional statements

- (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
- $\approx$ **Mid 2024:** Deadline for **submissions**
- **2024/2025: Workshop(s)** for characterization / analysis of submitted schemes
- $\geq$ **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 ($\approx$ Sep 26–28) [about revised call ($\approx$ July)]

Welcome/needed interaction

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

2. **Concrete submissions ($\approx$ Mid 2024):**
   – Structured specification, open source implementation, evaluation, ...

3. **Public scrutiny of submitted schemes ($\geq$ 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 $\rightarrow$ Submit $\rightarrow$ 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