Introduction to MPTS 2023

Presented* on September 26th @ MPTS 2023 (Virtual)

NIST Workshop on **M**ulti-**P**arty **T**hreshold **S**chemes 2023

Hosted by the Cryptographic Technology Group @ NIST
National **I**nstitute of **S**tandards and **T**echnology

* Luís Brandão (NIST/Strativia: Foreign Guest Researcher [non-employee] at NIST, contractor from Strativia). Expressed opinions are those of the speaker/author and should not be construed as official views of NIST.

Outline

1. High-level context: MPTC, PEC, the Threshold Call

2. MPTS 2023 (schedule, topics, statistics)

3. Online resources

Outline

1. High-level context: MPTC, PEC, the Threshold Call

2. MPTS 2023 (schedule, topics, statistics)

3. Online resources

Two NIST-Crypto projects related to today's event

(i.e., projects in the Cryptographic Technology Group at NIST)

- **MPTC:** "**multi-party threshold cryptography**" (threshold schemes for crypto primitives)
- **PEC:** "**privacy-enhancing cryptography**" (advanced features/functionalities)

Two NIST-Crypto projects related to today's event

(i.e., projects in the Cryptographic Technology Group at NIST)

- **MPTC:** "**multi-party threshold cryptography**" (threshold schemes for crypto primitives)
- **PEC:** "**privacy-enhancing cryptography**" (advanced features/functionalities)

The "Threshold Call" (from MPTC+PEC):

NIST First Call for Multi-Party Threshold Schemes

[see NISTIR 8214C] to gather **reference material** for public analysis ...

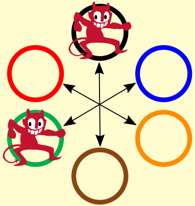
aiming for **recommendations** (in a 1st phase), including about PEC.

NIST Call for Multi-Party Threshold Schemes

- NISTIR 8214C: Initial public **draft** (**Jan 2023**) ⇒ Revised version (**late 2023**).
- Submission deadline (expected ≈ **2nd-half 2024**)

NIST Call for Multi-Party Threshold Schemes

- NISTIR 8214C: Initial public **draft** (**Jan 2023**) ⇒ Revised version (**late 2023**).
- Submission deadline (expected ≈ **2nd-half 2024**)

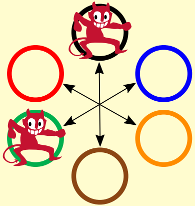


Calling for submissions of threshold schemes

(And gadgets for modular use)

NIST Call for Multi-Party Threshold Schemes

- NISTIR 8214C: Initial public **draft** (**Jan 2023**) ⇒ Revised version (**late 2023**).
- Submission deadline (expected ≈ **2nd-half 2024**)



Calling for submissions of threshold schemes for:

- **[Cat1] Selected NIST-standardized primitives**
- **[Cat2] Other primitives (including FHE, IBE/ABE, ZKP)**

  (And gadgets for modular use)

FHE = Fully-homomorphic encryption.

IBE/ABE = Identity/Attribute-based encryption.

ZKP = Zero-knowledge proof.

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

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

The revised version of the call will detail better each **component**.

A submission package can propose various **objects** (schemes/gadgets).

Each **component** will then map all such **objects**.

Selected notes about the "Threshold Call"

1. It has a **wide scope** of subcategories for submission (next slides)
2. Enables an **exploration** of advanced cryptography, before promising standards
3. The initial process will devise **recommendations** for subsequent processes
4. Both **post-and-pre quantum** primitives are in scope.
5. **Active security** is required, though open to diverse security formulations.
6. **Modularity** is strongly encoraged (gadgets)
7. Community **participation** is essential (feedback; submissions; analyses)

Category Cat1 of NIST Call for Multi-Party Threshold Schemes

Subcategory: Type	**Families of specifications**
C1.1: **Signing** (preQ)	EdDSA sign, ECDSA sign, RSADSA sign
C1.2: **PKE** (preQ)	RSA decrypt, RSA encrypt (a secret value)
C1.3: **2KA**	ECC-CDH, ECC-MQV
C1.4: **Symmetric**	AES encipher/decipher, KDM/KC (for 2KE)
C1.5: **Keygen**	ECC keygen, RSA keygen, bitstring keygen

Too many acronyms, we know. **Legend:** **2KA**: pair-wise key-agreement. **2KE**: pair-wise key-establisment. **AEAD** = Authenticated Encryption with Associated Data. **AES**: Advanced Encryption Standard. **CDH**: cofactor Diffie–Hellman. **DSA** = Digital Signature Algorithm. **ECC**: Elliptic-curve cryptography (or, if used as an adjective, EC-based). **ECDSA**: Elliptic-curve Digital Signature Algorithm. **EdDSA**: Edwards-curve Digital Signature Algorithm. Elliptic-curve based Key-Establishment. **KC**: Key-confirmtion. **KDM**: Key-derivation mechanism. **KEM**: Key-Encapsulation Mechanism. **Keygen**: Key-generation. **ML** = Module Lattice. **MQV**: Menezes-Qu-Vanstone. **PKE**: public-key encryption. **postQ**: Post-Quantum. **preQ**: Pre-Quantum. **RSA**: Rivest–Shamir–Adleman (signature and encryption schemes). **RSADSA**: RSA digital signature algorithm. **SLH** = StateLess hash. **XOF** = extendable Output Function. **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 Cat1 of NIST Call for Multi-Party Threshold Schemes

Subcategory: Type	**Families of specifications**
C1.1: **Signing** (preQ) (postQ)	EdDSA sign, ECDSA sign, RSADSA sign ML-DSA, SLH-DSA, FN-DSA
C1.2: **PKE** (preQ) (postQ)	RSA decrypt, RSA encrypt (a secret value) ML-KEM
C1.3: **2KA**	ECC-CDH, ECC-MQV
C1.4: **Symmetric**	AES encipher/decipher, KDM/KC (for 2KE) [upcoming] ("lightweight") ASCON-related AEAD and XOF
C1.5: **Keygen**	ECC keygen, RSA keygen, bitstring keygen

Too many acronyms, we know. **Legend:** **2KA**: pair-wise key-agreement. **2KE**: pair-wise key-establisment. **AEAD** = Authenticated Encryption with Associated Data. **AES**: Advanced Encryption Standard. **CDH**: cofactor Diffie–Hellman. **DSA** = Digital Signature Algorithm. **ECC**: Elliptic-curve cryptography (or, if used as an adjective, EC-based). **ECDSA**: Elliptic-curve Digital Signature Algorithm. **EdDSA**: Edwards-curve Digital Signature Algorithm. Elliptic-curve based Key-Establishment. **KC**: Key-confirmtion. **KDM**: Key-derivation mechanism. **KEM**: Key-Encapsulation Mechanism. **Keygen**: Key-generation. **ML** = Module Lattice. **MQV**: Menezes-Qu-Vanstone. **PKE**: public-key encryption. **postQ**: Post-Quantum. **preQ**: Pre-Quantum. **RSA**: Rivest–Shamir–Adleman (signature and encryption schemes). **RSADSA**: RSA digital signature algorithm. **SLH** = StateLess hash. **XOF** = extendable Output Function. **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 key-agreement	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

Note: While TF-QR is desired 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**seudo**r**andom **f**unction [family]. **PRP** = **p**seudo**r**andom **p**ermutation [family]. **QR** = **q**uantum **r**esistant. **TF** = **t**hreshold-**f**riendly. **ZKPoK** = **z**ero **k**nowledge **p**roof **o**f **k**nowledge.

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 key-agreement	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)	GC.generate; GC.evaluate

Note: While TF-QR is desired 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**seudo**r**andom **f**unction [family]. **PRP** = **p**seudo**r**andom **p**ermutation [family]. **QR** = **q**uantum **r**esistant. **TF** = **t**hreshold-**f**riendly. **ZKPoK** = **z**ero **k**nowledge **p**roof **o**f **k**nowledge.

Outline

1. High-level context: MPTC, PEC, the Threshold Call

2. MPTS 2023 (schedule, topics, statistics)

3. Online resources

Why this workshop (MPTS 2023)

Community feedback and participation are essential!

Thank you in particular (speakers and attendees) for joining MPTS 2023

Why this workshop (MPTS 2023)

Community feedback and participation are essential!

Thank you in particular (speakers and attendees) for joining MPTS 2023

MPTS 2023 is organized to:

1. obtain feedback and useful info for a better NIST Threshold Call/Process;
2. promote awareness/motivation of stakeholders (potential submitters, analyzers, ...)

Why this workshop (MPTS 2023)

Community feedback and participation are essential!

Thank you in particular (speakers and attendees) for joining MPTS 2023

MPTS 2023 is organized to:

1. obtain feedback and useful info for a better NIST Threshold Call/Process;
2. promote awareness/motivation of stakeholders (potential submitters, analyzers, ...)

What is MPTS 2023?

- "NIST Workshop on Multi-Party Threshold Schemes 2023"
- 3 half-days; ≈ 30 talks; ≈ 300 registered attendees

MPTS 2023 Schedule of Sessions

Date	Session	Time	Session title	# talks
Sep. 26th	—	10:00–10:20	Welcome/Intro to MPTS 2023	—
	1a	10:20–12:00	Generic considerations on MPC/MPTC	4
	1b	13:00–15:00	Threshold Signatures over Elliptic Curves	5
Sep. 27th	**2a**	10:00–12:00	FHE+ZKP+ABE	5
	2b	13:00–14:00	More on Threshold Signatures	3
	2c	14:00–15:00	NIST Standards	4
Sep. 28th	**3a**	10:00–11:40	Some Gadgets	4
	3b	11:40–12:00	Focused Feedback	—
	3c	13:00–14:50	More Gadgets	5
	—	14:50–15:00	Concluding remarks	—

Legend: ABE = **A**ttribute-**b**ased **e**ncryption. FHE = **F**ully-**h**omomorphic **e**ncryption. MPC = (Secure) **M**ulti**p**arty **C**omputation. MPTC = **M**ulti-**p**arty **t**hreshold **c**ryptography. MPTS = **M**ulti-**p**arty **t**hreshold **s**chemes. NIST = **N**ational **I**nstitute of **S**tandards and **T**echnology. Sep. = **Sep**tember. ZKP = **Z**ero-**k**nowledge **p**roof.

Event details: https://csrc.nist.gov/events/2023/mpts2023 **Contact email:** workshop-mpts2023@nist.gov

Suggested Topics in the Call for Presentations

1. **Scope of the Threshold Call:** refinements to the description of subcategories.
2. **Submission requirements** in the Threshold Call: needed clarifications.
3. **Expressions of interest:** intended concrete submissions (and possible submitter team).
4. **Need and adoptability:** special features and primitives useful for specific applications.
5. **Inspiration:** suggestions to the community, for submission of concrete threshold schemes.
6. **Frameworks:** pertinent system models, security formulations, and threshold parameters.
7. **Pre/post quantum:** concrete pre-quantum versus post-quantum cases worth focusing on.
8. **Technicalities:** challenges about concrete primitives / threshold schemes / assumptions.
9. **External efforts:** other processes developing related reference material or specifications.

Video-conference Webinar (registrations and logistics)

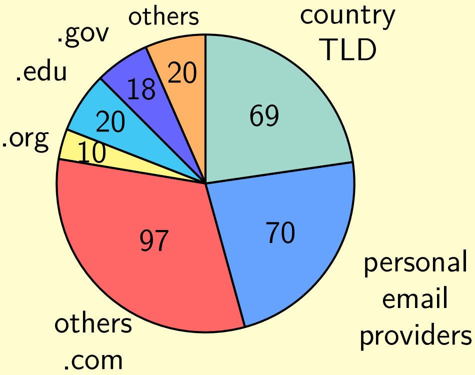
- **Virtual registrations:** 304*
  (Not counting speakers and hosts)

  Across 40 countries: US (124); IN (25); FR (17); CA (16), DE (11), UK (11), IL (9), CN (8), ...

- **Audio and video:** being recorded (posting will be announced in the PEC and MPTC forums)

- **Questions:** Attendees can use the virtual Q&A (to be considered as time permits)

Per registered email address:



*Registrations for 1st day of webinar, as of 8am EDT. Actual number is expected to increase until the workshop starts, and thereafter. Legend: CA = Canada; CN = China; DE = Germany; FR = France; IL = Israel; IN = India; Q&A = Questions and answers; TLD = top-level domain; UK = United Kingdom; US = United States.

Outline

1. High-level context: MPTC, PEC, the Threshold Call

2. MPTS 2023 (schedule, topics, statistics)

3. Online resources

Thank you for your attention!

Introduction to MPTS 2023:

September 26th @ Virtual

We appreciate followup comments: workshop-mpts2023@nist.gov

MPTS 2023
(Sept. 26–28)

Threshold Call
(Draft)

MPTC-Forum
(email list)

PEC-Forum
(email list)