NIST Call for Multi-Party Threshold Schemes

Brief Notes at RWC 2023

Presented* at the Real World Crypto (RWC) Symposium 2023

March 28, 2023 | Tokyo (Japan)

Suggested reading: NISTIR 8214C ipd

NIST First Call for Multi-Party Threshold Schemes

(Initial Public Draft) [2023-Jan-25]

Public comments due **2023-April-10**

* 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.

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

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.

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])

Legend: AEAD = **Auth**[enticated] **Enc**[ryption] w[ith] **Assoc**[iated] **Data**. **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.

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 = **Auth**[enticated] **Enc**[ryption] w[ith] **Assoc**[iated] **Data**. **CTG** = **C**ryptographic **T**echnology **G**roup. **LWC** = **L**ight**w**eight **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.

Updates on some NIST Crypto activities

- **Post-Quantum (PQC):** [Aim] Draft Standards of selected schemes (Summer 2023).
  – Public call (2022) for more PQ-signatures (submit by June 1st).

- **Lightweight (LWC):** Feb 2023, selected ASCON (**A**uth. **E**nc. w/ **A**ssoc. **D**ata; hash).
  – Workshop on June 21–22 (submit by May 1st). [Aim] Draft Standard (late 2023).

- **Threshold Call (MPTC/PEC):** Call Draft (Jan. 25th); comments due April 10th.
  – [Aim] Call finalized in 2023 2nd half; submissions deadline within 2024 1st half.

Legend: AEAD = **Auth**[enticated] **Enc**[ryption] w[ith] **Assoc**[iated] **D**ata. **EdDSA** = **Ed**wards-Curve **D**igital **S**ignature **A**lgorithm. **Feb** = **Feb**ruary. **FIPS** = **F**ederal **I**nformation **P**rocessing **S**tandards. **Jan** = **Jan**uary. **SP** = **S**pecial **P**ublication (800 series) [in Computer Security].

Updates on some NIST Crypto activities

- **Post-Quantum (PQC):** [Aim] Draft Standards of selected schemes (Summer 2023).
  – Public call (2022) for more PQ-signatures (submit by June 1st).

- **Lightweight (LWC):** Feb 2023, selected ASCON (**A**uth. **E**nc. w/ **A**ssoc. **D**ata; hash).
  – Workshop on June 21–22 (submit by May 1st). [Aim] Draft Standard (late 2023).

- **Threshold Call (MPTC/PEC):** Call Draft (Jan. 25th); comments due April 10th.
  – [Aim] Call finalized in 2023 2nd half; submissions deadline within 2024 1st half.

- **Crypto Publication Review:** Revising Standards (FIPS & SP) older than 5 years.

- **FIPS 186-5 (signatures, inc. EdDSA):** Standard (final) published Feb. 7th.

- **Other projects:** https://www.nist.gov/itl/csd/cryptographic-technology

Legend: AEAD = **Auth**[enticated] **Enc**[ryption] **w**[ith] **Assoc**[iated] **Data**. **EdDSA** = **Ed**wards-Curve **D**igital **S**ignature **A**lgorithm. **Feb** = **Feb**ruary. **FIPS** = **F**ederal **I**nformation **P**rocessing **S**tandards. **Jan** = **Jan**uary. **SP** = **S**pecial **P**ublication (800 series) [in Computer Security].

Updates on some NIST Crypto activities

- **Post-Quantum (PQC):** [Aim] Draft Standards of selected schemes (Summer 2023).
  – Public call (2022) for more PQ-signatures (submit by June 1st).

- **Lightweight (LWC):** Feb 2023, selected ASCON (**A**uth. **E**nc. w/ **A**ssoc. **D**ata; hash).
  – Workshop on June 21–22 (submit by May 1st). [Aim] Draft Standard (late 2023).

- **Threshold Call (MPTC/PEC):** Call Draft (Jan. 25th); comments due April 10th.
  – [Aim] Call finalized in 2023 2nd half; submissions deadline within 2024 1st half.

- **Crypto Publication Review:** Revising Standards (FIPS & SP) older than 5 years.

- **FIPS 186-5 (signatures, inc. EdDSA):** Standard (final) published Feb. 7th.

- **Other projects:** https://www.nist.gov/itl/csd/cryptographic-technology

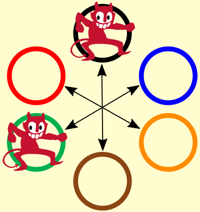
Legend: **AEAD** = **Auth**[enticated] **Enc**[ryption] **w**[ith] **Assoc**[iated] **Data**. **EdDSA** = **Ed**wards-Curve **D**igital **S**ignature **A**lgorithm. **Feb** = **Feb**ruary. **FIPS** = **F**ederal **I**nformation **P**rocessing **S**tandards. **Jan** = **Jan**uary. **SP** = **S**pecial **P**ublication (800 series) [in Computer Security].

The NIST Call for *Multi-Party Threshold Schemes*

NISTIR 8214C ipd (**i**nitial **p**ublic **d**raft)

Email public comments to nistir-8214C-comments@nist.gov, by **2023-April-10**.

Calling for threshold schemes for diverse primitives:

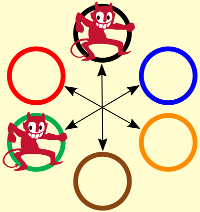


The NIST Call for *Multi-Party Threshold Schemes*

NISTIR 8214C ipd (**i**nitial **p**ublic **d**raft)

Email public comments to nistir-8214C-comments@nist.gov, by **2023-April-10**.

Calling for threshold schemes for diverse primitives:



- **Cat1: Selected NIST-standardized primitives**
  – In EdDSA, ECDSA, RSA, AES, ECC-KE, ...
- **Cat2: Primitives in schemes not standardized by NIST**
  – *Threshold friendly*, and possibly with advanced features (e.g., in FHE, IBE, ZKP)

Legend: AES = **A**dvanced **E**ncryption **S**tandard. EC = **E**lliptic **c**urve. ECC-KE = **EC c**ryptography (based) **k**ey-**e**xchange. FHE = **f**ully-**h**omomorphic **e**ncryption. EdDSA = **Ed**wards-Curve **d**igital **s**ignature **a**lgorithm. ECDSA = **EC d**igital **s**ignature **a**lgorithm. IBE = **i**dentity-**b**ased **e**ncryption. NIST = **N**ational **I**nstitute of **S**tandards and **T**echnology. RSA = **R**ivest–**S**hamir–**A**dleman. ZKP = **z**ero-**k**nowledge **p**roofs.

Category Cat1 of NIST Call for Multi-Party Threshold Schemes

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

Subcategory: Type
C1.1: **Signing**
C1.2: **PKE**
C1.3: **2KA**
C1.4: **Symmetric**
C1.5: **Keygen**

Legend: **2KA**: **pair**-wise **k**ey-**a**greement. **2KE**: **pair**-wise **k**ey-**e**stablisment. **AES**: **A**dvanced **E**ncryption **S**tandard. **CDH**: **c**ofactor **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-**c**urve 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**: **Key**-**gen**eration. **MQV**: Menezes-Qu-Vanstone. **PKE**: **p**ublic-**k**ey encryption. **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 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)

Legend: **2KA**: **pair**-wise **k**ey-**a**greement. **2KE**: **pair**-wise **k**ey-**e**stablisment. **AES**: **A**dvanced **E**ncryption **S**tandard. **CDH**: **c**ofactor **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-**c**urve 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**: **Key**-**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 Cat1 of NIST Call for Multi-Party Threshold Schemes

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

Subcategory: Type	Families of specifications	NIST references
C1.2: **PKE**	RSA decrypt, RSA encrypt (a secret value)	SP 800-56B Rev2

Legend: 2KA: **pair**-wise **k**ey-**a**greement. **2KE**: **pair**-wise **k**ey-**e**stablisment. **AES**: **A**dvanced **E**ncryption **S**tandard. **CDH**: **c**ofactor **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-**c**urve 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**: **Key**-**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 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**	ECC-CDH, ECC-MQV	SP 800-56A Rev3
C1.4: **Symmetric**	AES encipher/decipher, KDM/KC (for 2KE)	FIPS 197, SP 800-56C Rev2, ...
C1.5: **Keygen**	ECC keygen, RSA keygen, bitstring keygen	(corresponding references above)

Legend: **2KA**: pair-wise key-agreement. **2KE**: pair-wise key-establisment. **AES**: Advanced Encryption Standard. **CDH**: cofactor Diffie–Hellman. **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. **FIPS**: Federal Information Processing Standard. **KC**: Key-confirmtion. **KDM**: Key-derivation mechanism. **Keygen**: Key-generation. **MQV**: Menezes-Qu-Vanstone. **PKE**: public-key encryption. **RSA**: Rivest–Shamir–Adleman (signature and encryption schemes). **RSADSA**: RSA digital signature algorithm. **SP 800**: Special Publication (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

Subcategory: Type
C2.1: **Signing**
C2.2: **PKE**
C2.3: **Key-agreem.**
C2.4: **Symmetric**
C2.5: **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

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

Subcategory: Type
C2.6: **Advanced**
C2.7: **ZKPoK**
C2.8: **Gadgets**

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
C2.6: **Advanced**	TF-QR fully-homomorphic encryption	Decryption; Keygen
|	TF identity-based and attribute-based encryption	Decryption; Keygens

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

Subcategory: Type	Example types of schemes	Example primitives
C2.7: **ZKPoK**	**Z**ero-**k**nowledge **p**roof **o**f **k**nowledge of private key	ZKPoK.Generate

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

Subcategory: Type	Example types of schemes	Example primitives
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.

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.

Welcome/needed interaction with the community

1. **Feedback about the call:** [comments by **2023-Apr-10**]
   a. The structure and scope of the call (which primitives should be submitted)
   b. Notes on (in)compatibility between QR, TF and advanced features
   c. Security properties, cautionary recommendations / suggested requirements

Legend: QR = **q**uantum **r**esistance. **TF** = **t**hreshold **f**riendliness.

Welcome/needed interaction with the community

1. **Feedback about the call:** [comments by **2023-Apr-10**]
   a. The structure and scope of the call (which primitives should be submitted)
   b. Notes on (in)compatibility between QR, TF and advanced features
   c. Security properties, cautionary recommendations / suggested requirements

2. **Concrete submissions:**
   – Structured specification, open source implementation, evaluation, ...

3. **Public scrutiny of submitted schemes:**
   – Evaluation comments (can impact subsequent recommendations)

Legend: QR = **q**uantum **r**esistance. **TF** = **t**hreshold **f**riendliness.

Assorted notes about the “Threshold Call”

- Submission focuses
- Active security
- Synergies
- Reference material
- Clarification

Assorted notes about the “Threshold Call”

- **Submission focuses:** Can specify a family of schemes (in various subcategories).
- **Active security:** It is required; it is open to various security formulations.
- **Synergies:** Submissions of schemes in standardization development in other bodies and/or by **community efforts** are also very welcome!
- **Reference material:** The initial process is **not a competition** aiming to select a winner, but the public exposure is deemed useful.
- **Clarification:** The set of submissions and their analyses will clarify useful system models, security goals/requirements ... and **future processes**.

Assorted notes about the "Threshold Call"

- **Submission focuses:** Can specify a family of schemes (in various subcategories).
- **Active security:** It is required; it is open to various security formulations.
- **Synergies:** Submissions of schemes in standardization development in other bodies and/or by **community efforts** are also very welcome!
- **Reference material:** The initial process is **not a competition** aiming to select a winner, but the public exposure is deemed useful.
- **Clarification:** The set of submissions and their analyses will clarify useful system models, security goals/requirements ... and **future processes**.

Provide feedback (by 2023-Apr-10) ... will help improve the final call.

- ***NIST First Call for Multi-Party Threshold Schemes*** **(Initial Public Draft)**
  - **Publication: NISTIR 8214C ipd:** https://doi.org/10.6028/NIST.IR.8214C.ipd
  - **Public comments:** by email nistir-8214C-comments@nist.gov, till 2023-Apr-10

- ***NIST First Call for Multi-Party Threshold Schemes*** **(Initial Public Draft)**
  - **Publication: NISTIR 8214C ipd:** https://doi.org/10.6028/NIST.IR.8214C.ipd
  - **Public comments:** by email nistir-8214C-comments@nist.gov, till 2023-Apr-10
- **Multi-Party Threshold Cryptography (MPTC) Website and Forum:**

  https://csrc.nist.gov/projects/threshold-cryptography | https://list.nist.gov/MPTC-forum

- ***NIST First Call for Multi-Party Threshold Schemes*** **(Initial Public Draft)**
  - **Publication: NISTIR 8214C ipd:** https://doi.org/10.6028/NIST.IR.8214C.ipd
  - **Public comments:** by email nistir-8214C-comments@nist.gov, till 2023-Apr-10
- **Multi-Party Threshold Cryptography (MPTC) Website and Forum:**

  https://csrc.nist.gov/projects/threshold-cryptography | https://list.nist.gov/MPTC-forum
- **Privacy-Enhancing Cryptography (PEC) Website and Forum:**

  https://csrc.nist.gov/projects/pec | https://list.nist.gov/PEC-forum

Thank you for your attention! Questions?

NIST Call for Multi-Party Threshold Schemes: Brief Notes at RWC 2023

Presented at the Real World Crypto (RWC) Symposium 2023

March 28, 2023 @ Tokyo (Japan) — luis.brandao@nist.gov

- ***NIST First Call for Multi-Party Threshold Schemes*** **(Initial Public Draft)**
  - **Publication: NISTIR 8214C ipd:** https://doi.org/10.6028/NIST.IR.8214C.ipd
  - **Public comments:** by email nistir-8214C-comments@nist.gov, till 2023-Apr-10
- **Multi-Party Threshold Cryptography (MPTC) Website and Forum:**

  https://csrc.nist.gov/projects/threshold-cryptography | https://list.nist.gov/MPTC-forum
- **Privacy-Enhancing Cryptography (PEC) Website and Forum:**

  https://csrc.nist.gov/projects/pec | https://list.nist.gov/PEC-forum