# Quantum-Resistance in the Upcoming NIST Call for Threshold Schemes

Presented* at Real-World PQC

March 26, 2023 | Tokyo (Japan)

Suggested reading: NISTIR 8214C ipd: *NIST First Call for Multi-Party Threshold Schemes (Initial Public Draft)* [Jan. 2023]

* 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**" secure signatures and KEM/PKE
- **LWC:** [standardization] "**lightweight**" AEAD and hashing
- **PEC:** [exploratory] "**privacy-enhancing**" (advanced) features/functionalities
- **MPTC:** [exploratory] "**multi-party threshold**" schemes for crypto primitives
- **...** (various other projects in the "Crypto group" [CTG])

**Legend: AEAD** = **A**uthenticated **E**ncryption with **A**ssociated **D**ata. **CTG** = **C**ryptographic **T**echnology **G**roup. **L**aboratory. **KEM** = **K**ey **E**ncapsulation **M**echanism. **LWC** = **L**ightweight **C**ryptography. **MPTC** = **M**ulti-**P**arty **T**hreshold **C**ryptography. **NIST** = **N**ational **I**n-sti-tute of **S**tandards and **T**echnology. **PEC** = **P**rivacy-**E**nhancing **C**ryptography. **PKE** = **p**ublic-**k**ey **e**ncryption. **PQC** = **P**ost-**Q**uantum **C**ryptography.

# Intro: NIST has various Crypto Projects

- **PQC:** [standardization] "**post-quantum**" secure signatures and KEM/PKE
- **LWC:** [standardization] "**lightweight**" AEAD and hashing
- **PEC:** [exploratory] "**privacy-enhancing**" (advanced) features/functionalities
- **MPTC:** [exploratory] "**multi-party threshold**" schemes for crypto primitives
- **...** (various other projects in the "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.

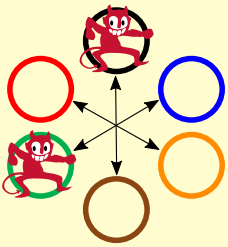
Legend: AEAD = Authenticated Encryption with Associated Data. CTG = Cryptographic Technology Group. Laboratory. KEM = Key Encapsulation Mechanism. LWC = Lightweight Cryptography. MPTC = Multi-Party Threshold Cryptography. NIST = National In-sti-tute of Standards and Technology. PEC = Privacy-Enhancing Cryptography. PKE = public-key encryption. PQC = Post-Quantum Cryptography.

# The NIST Call for *Multi-Party Threshold Schemes*

NISTIR 8214C ipd (**i**nitial **p**ublic **d**raft) — public comments till **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 specified by NIST**
  - Interest in *threshold friendliness* and **quantum resistance**
  - Including from schemes with advanced features (e.g., 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 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 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-key **e**ncryption. **PRF** = **p**seudorandom **f**unction [family]. **PRP** = **p**seudorandom **p**ermutation [family]. **QR** = **q**uantum resistant. **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 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.

# Category Cat2 of the NIST “Threshold” Call

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

**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-key **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.

# 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 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.

# 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 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.

# 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 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.

# 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 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.

# Welcome/needed interaction by the PQC 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. **PQC** = **P**ost-**Q**uantum **C**ryptography.

# Welcome/needed interaction by the PQC 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:**
   – Specification, implementation (open source), reproducible, ...

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



**Legend:** **QR** = **q**uantum **r**esistance. **TF** = **t**hreshold **f**riendliness. **PQC** = **P**ost-**Q**uantum **C**ryptography.

# Thank you for your attention! Questions?

***Quantum-Resistance in the Upcoming NIST Call for Threshold Schemes***

Presented at the Real-World PQC

March 26, 2023 @ Tokyo (Japan) — luis.brandao@nist.gov

- **NISTIR 8214C ipd:** *NIST First Call for Multi-Party Threshold Schemes (Initial Public Draft)*
- **Public comments:** by email nistir-8214C-comments@nist.gov, till 2023-Apr-10
- **PEC Website:** https://csrc.nist.gov/projects/pec
- **PEC-Forum:** https://list.nist.gov/PEC-forum
- **MPTC Website:** https://csrc.nist.gov/projects/threshold-cryptography
- **MPTC-Forum:** https://list.nist.gov/MPTC-forum