Brief notes on PEC (FHE+ZKP+ABE...) in the NIST Threshold Call

Presented* on September 27th @ MPTS 2023 (Virtual)

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

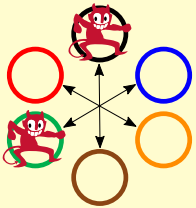
Hosted by the Cryptographic Technology Group @ NIST
National **I**nstitute of **S**tandards and **T**echnology

Legend:
ABE = Attribute-based encryption.
FHE = Fully-homomorphic encryption.
PEC = Privacy-enhancing cryptography.
ZKP = Zero-knowledge proof.

* 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.

PEC in the NIST Call for Multi-Party Threshold Schemes

The Threshold Call scope includes:



- C2.6: crypto schemes with advanced functional features
  (e.g., **FHE, IBE/ABE**)
- C2.7: **ZKP**s **o**f **k**nowledge useful to support the threshold setting
  (e.g., **ZKPoK** of secret-key corresponding to a public key)
- C2.8: **gadgets** useful to support the threshold setting
  (e.g., garbled circuit)

Legend: FHE = Fully-homomorphic encryption. IBE/ABE = Identity/Attribute-based encryption. PEC = privacy-enhancing cryptography. ZKP = Zero-knowledge proof.

Fully-homomorphic encryption (FHE) in the Threshold Call

- **Which primitives can be thresholdized?**
  - 1. **Decryption** (using secret-shared private key) [sufficient to call it a threshold scheme]
  - 2. **Keygen** [nice complement to threshold decryption]
  - 3. **Encryption** (of secret-shared secret value)
  - 4. **Homomorphic evaluation** (of secret gate/operation)
- We expect submitted solutions to already be **plausibly post-quantum secure**. Nice if security can be related to security levels defined by the NIST PQC process.
- To revise in the call: acknowledge **three mainstream approaches** for FHE
- **Benchmarking example** in the call: homomorphic evaluation of AES enciphering (To revise: acknowledge other benchmarking use-cases)

Legend: AES = Advanced encryption standard. FHE = Fully-homomorphic encryption. NIST = National Institute of Standards and Technology. PQC = Post-quantum cryptography.

Zero-Knowledge proofs (ZKP) in the Threshold Call

- **Non-threshold ZKPs** are of interest if relatable to other subcategories. Examples:
  1. ZKPoK of secret key corresponding to a (correct) public key [Section A.7, Table 12]
  2. ZKP of correct (FHE-related) homomorphic evaluation [Section A.6.1]
  3. Proof of determinism for the secret-nonce in an EdDSA or ECDSA signature
- **Distributed/threshold ZKPs** are also in scope. The set of parties holding secret-shares of a secret can produce a ZKP of distributed knowledge.
- **Examples to add in the call:** ZKPoKs related to Cat1-PQC&LWC, and to Cat2.
- **Within scope:**
  - Specialized ZKP systems, for specific types of proof
  - General ZKP systems, applicable to any statement (properly represented)

Legend: Cat1: Category [Cat]1. Cat2: Category [Cat]2. ECDSA = Elliptic-curve digital signature algorithm. EdDSA = Edwards-curve digital signature algorithm. FHE = Fully-homomorphic encryption. ZKP = Zero-knowledge proof. ZKPoK = ZKP of knowledge. LWC = Lightweight cryptography (project). PQC = Post-quantum cryptography (project).

Identity/Attribute Based Encryption (IBE/ABE)

To revise in the Call:

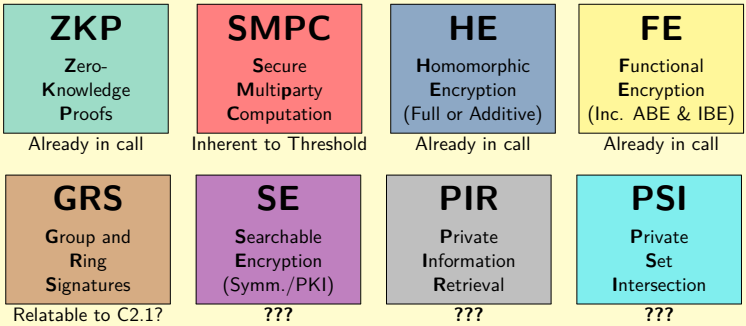
- **Refine description:** make subcategory for IBE/ABE, separate from FHE.
- **Differentiate "threshold" cases:**
  - operations over **secret-shared** private key (decryption, user-key gen, master-key gen)
  - system models with **multiple authorities**
- **Pre- vs. post-quantum:** both are in scope (e.g., pairings-based vs. lattice-based); submissions of pre-quantum solutions should argue well why it's worth consideration.

Legend: ABE = Attribute-based encryption. FHE = Fully-homomorphic encryption. IBE = Identity-based encryption.

Gadgets in the Threshold Call

The Threshold Call asks for gadgets useful for threshold schemes in scope.

For which other PEC tools or privacy-applications can the gadgets be useful?



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

Thank you for your attention!

Brief notes on PEC (FHE+ZKP+ABE...) in the NIST Threshold Call

September 27th @ 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)