THE NIST PROJECT ON PRIVACY ENHANCING CRYPTOGRAPHY

Luís Brandão*, René Peralta, Angela Robinson

Presentation at ICMC20

International Cryptographic Module Conference

September 23, 2020 @ Virtual event

* At NIST as a Foreign Guest Researcher (Contractor, from Strativia)

Opinions expressed in this presentation are from the speaker and are not to be construed as official views of NIST.

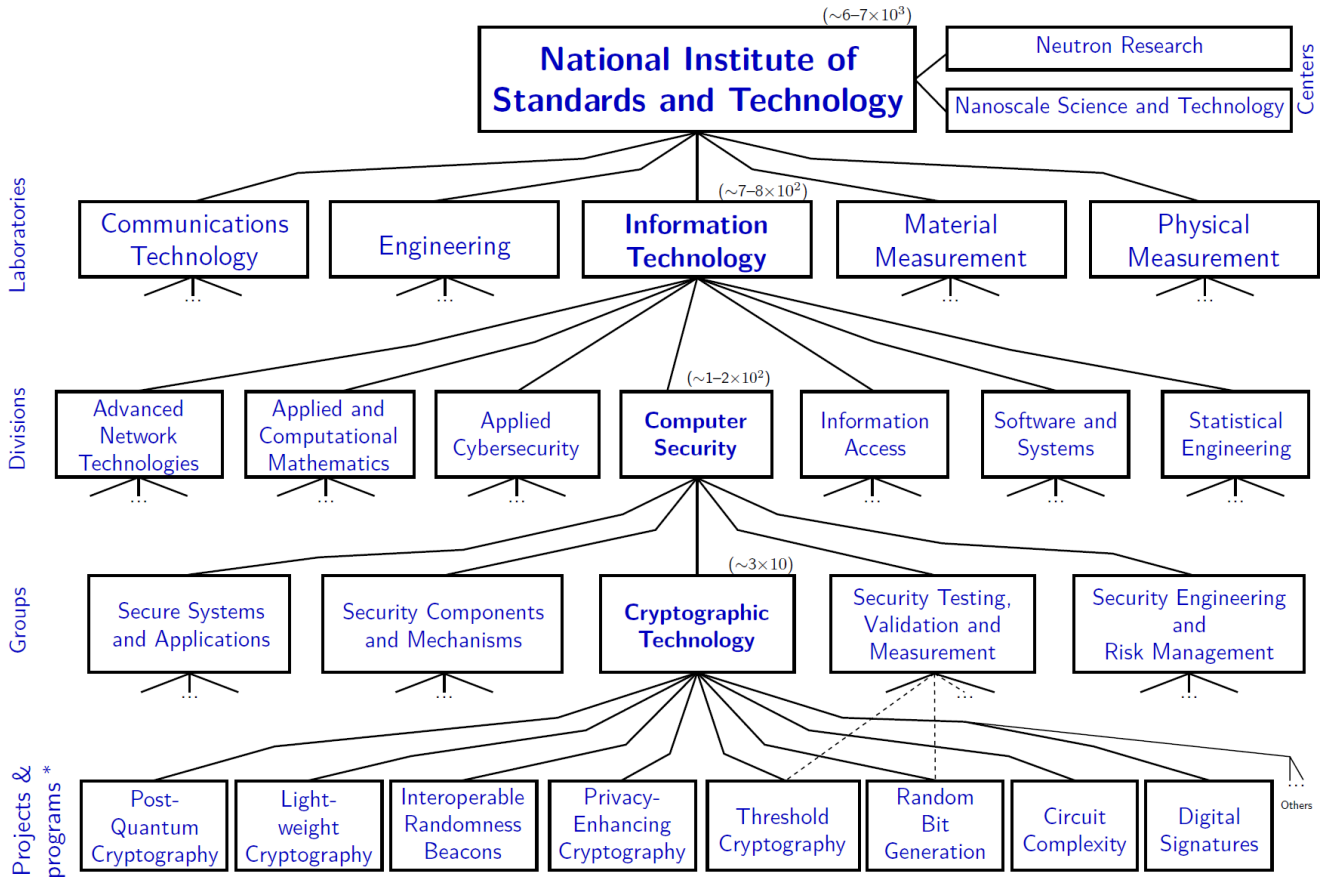
OUTLINE

1. The NIST PEC project
2. PEC techniques
3. Example applications of interest
4. PEC considerations

OUTLINE

1. The NIST PEC project
2. PEC techniques
3. Example applications of interest
4. PEC considerations

THE NIST CRYPTO GROUP



PRIVACY ENHANCING CRYPTO (PEC)

Goal: follow the progress of emerging technologies in the area of PEC and promote the use of cryptographic protocols that facilitate privacy goals

- Various primitives of interest:
  - Zero-knowledge proofs (ZKP)
  - Secure multiparty computation (SMPC)
  - Fully homomorphic encryption (FHE), identity-based encryption (IBE), etc.
- Development of reference material
- Privacy-enhancing applications

https://csrc.nist.gov/Projects/Privacy-Enhancing-Cryptography

REFERENCE MATERIAL

Assess the state of the art or research in a particular area

Motivate real-use applications or proofs of concept

Frame development of standards and future discussions

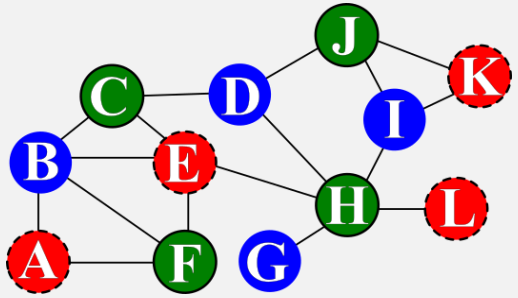
Promote interoperability for useful applications

OUTLINE

1. The NIST PEC project
2. PEC techniques
3. Example applications of interest
4. PEC considerations

ZERO-KNOWLEDGE PROOFS (ZKP)

Example [GMW91]: how to demonstrate the knowledge of a valid graph tri-coloration, without revealing any information about the solution?



Example: Consider this graph of

- 12 vertices: {A,B,C,D,E,F,G,H,I,J,K,L}
- 17 edges: {AB, AF, BC, BE, BF, CD, CE, DH, DJ, EF, EH, GH, HI, HL, IJ, IK, JK}

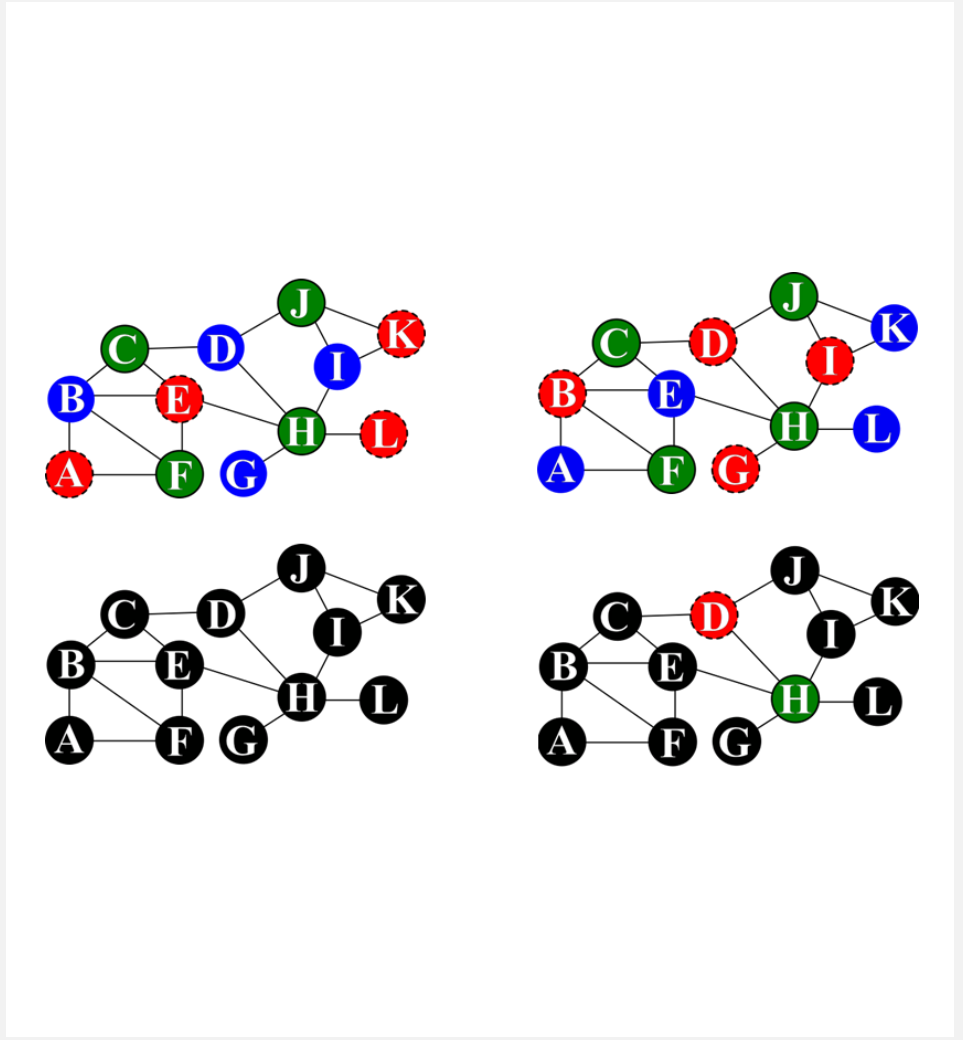
ZERO-KNOWLEDGE PROOFS (ZKP)

Example [GMW91]: how to demonstrate the knowledge of a valid tri-coloration, without revealing any information about the solution?

ZKP. Many iterations of the following:

1. Permute the colors
2. Commit to all permuted colors
3. Reveal an edge selected by the verifier

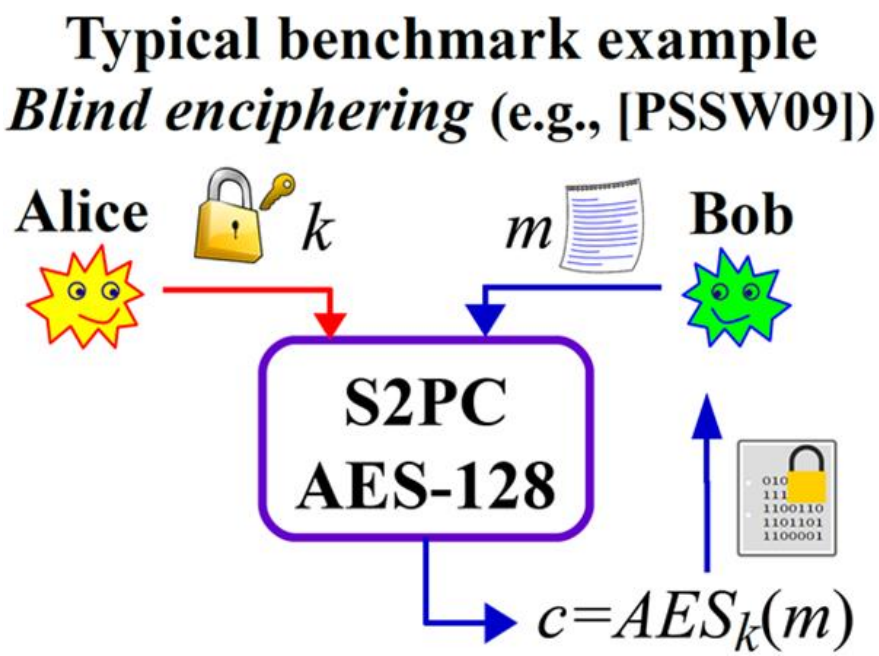
The verifier accepts if each revealed edge has two distinct colors



SECURE MULTIPARTY COMPUTATION (SMPC)

Since [Yao82]: allows multiple (distrustful) parties to jointly compute a function of their distributed inputs, while retaining privacy and correctness of each input and output

Secure two-party computation (S2PC) can be used for blind enciphering

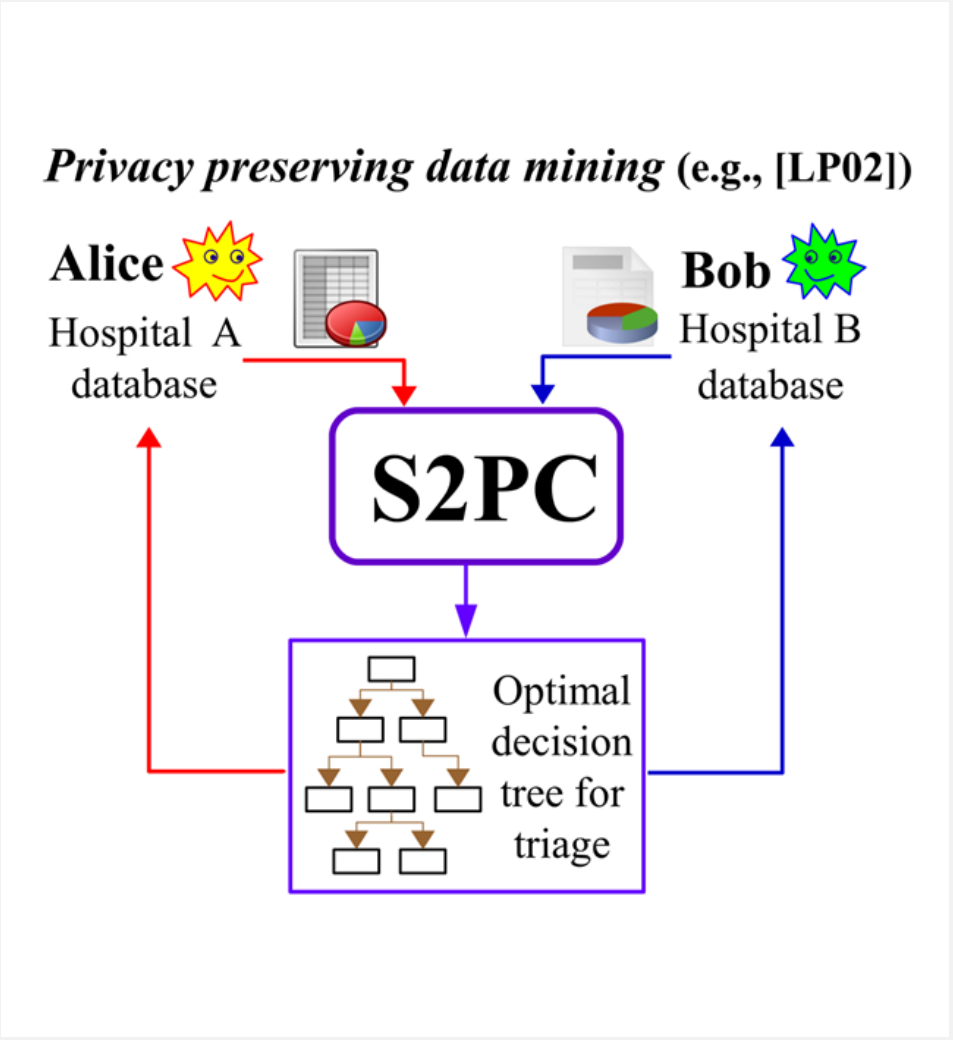


AES128: advanced encryption standard (a block-cipher) with 128 bits of key-size and plaintext-size.

SECURE MULTIPARTY COMPUTATION (SMPC)

Since [Yao82]: allows multiple (distrustful) parties to jointly compute a function of their distributed inputs, while retaining privacy and correctness of each input and output

Secure two-party computation (S2PC) can be used for privacy preserving data mining



OUTLINE

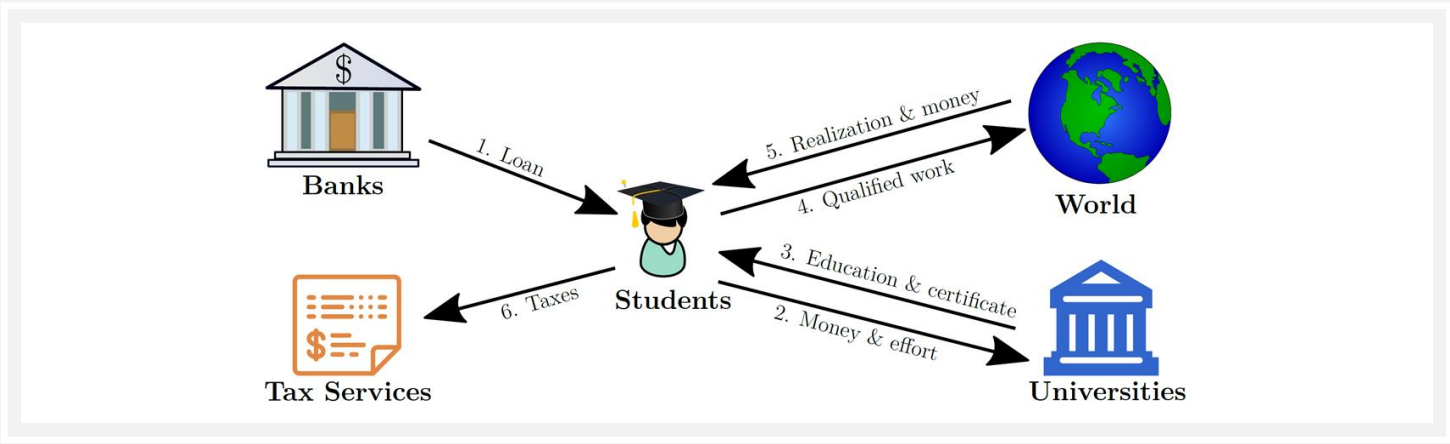
1. The NIST PEC project
2. PEC techniques
3. Example applications of interest
4. PEC considerations

USE CASE: STUDENTS' RIGHT TO KNOW

A U.S. Congress bill (2019) mandates the use of SMPC (or equivalent) to **estimate the return on investment by students on their college education**. *https://www.congress.gov/bill/116th-congress/house-bill/1565*

The data is distributed across several entities: SSA, Treasury, VA, Universities. Due to privacy concerns, these entities cannot share their data.

Approach: data holders encrypt the relevant data, then do SMPC to calculate aggregate statistics



USE CASE: ENCOUNTER METRICS

Goal: measure aggregate levels of encounters in a population while preserving the privacy of individuals

- Measurements useful for making informed decisions about occupancy rates and mobility rules
- We classify *encounters* according to distance between persons during and time of interaction

Application: privacy-preserving exposure notification

- Allows one to obtain a measure of their risk due to past encounters with self-reported COVID-19 positive people
- The precise engineering of a system for exposure notification should be targeted to particular environments

OUTLINE

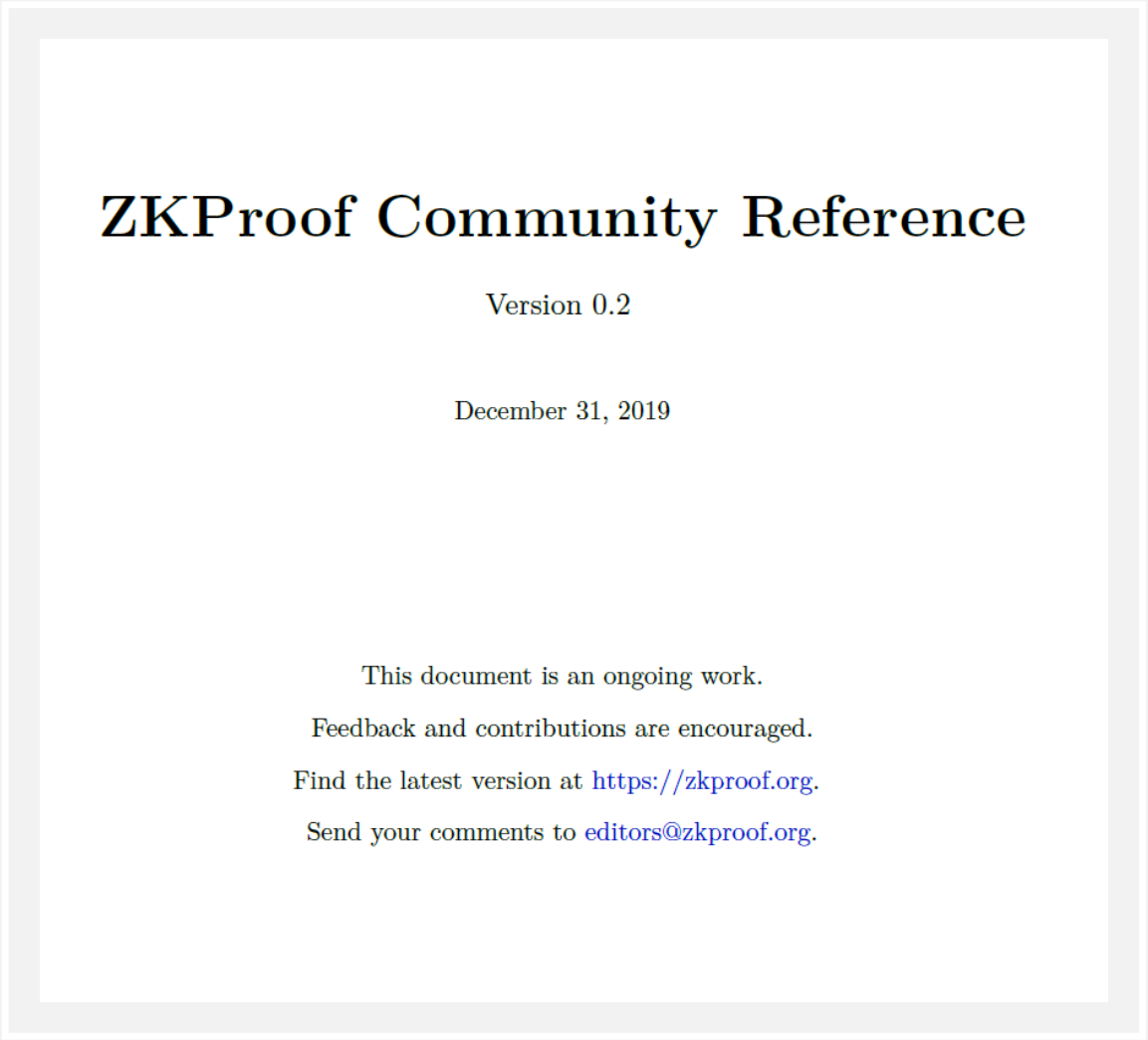
1. The NIST PEC project
2. PEC techniques
3. Example applications of interest
4. PEC considerations

CONSIDERATIONS

What kind of PEC could/should "Secure Cryptographic Modules" support?

- ZKPs about stored secret keys
- Private set intersection between two HSMs to determine a common subset (intersection), without revealing each others' private lists of data
- Participate in SMPC of key-generation (e.g., RSA or ECC), ending with a secret-share in each HSM
- Participate in a signature generation (e.g., RSA, ECDSA, EdDSA), without ever reconstructing the key

We welcome and encourage feedback from the community.



CURRENT ACTIVITIES

Collaboration with ZKProof initiative

- Open-industry academic initiative that seeks to mainstream (ZKP) cryptography
- ZKProof Community Reference
  - NIST PEC official comments
  - Involvement in editorial process

https://csrc.nist.gov/Projects/pec/zkproof

CURRENT ACTIVITIES

"Special Topics on Privacy and Public Auditability" speaker series, first event:

- *What math and physics can do to combat fake videos*
- *Differential Privacy at the US Census Bureau: Status Report*
- *De-Identification and Differential Privacy*
- *Randomness beacons as enablers of public auditability*

https://csrc.nist.gov/Projects/pec/stppa

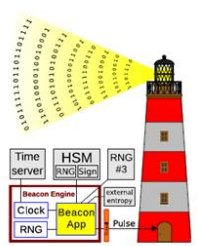
Privacy-preserving encounter metrics and exposure notification

- Approach to mitigate privacy concerns related to automated contact tracing efforts
- To appear

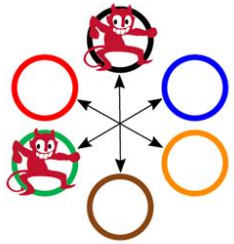
PEC AND OTHER CRYPTOGRAPHY

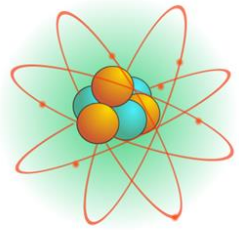
Foreseeable synergies with other projects:

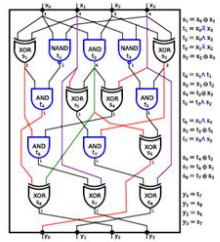
- Privacy preserving public auditability, as enabled by **randomness beacons**
- SMPC is useful for **threshold cryptography** (compute on secret-shared key)
- Some **post-quantum** cryptographic schemes are based on PEC (and vice-versa)
- Efficient ZKPs and SMPC depend strongly on good **circuits** with low **complexity**



Randomness Beacons


Threshold Cryptography


Post-Quantum Cryptography


Circuit Complexity

THANKS FOR YOUR ATTENTION

The NIST PEC team:

- Luís Brandão
- René Peralta
- Angela Robinson

Contact us at **crypto-privacy@nist.gov**