NIST INFORMATION TECHNOLOGY LABORATORY

ITL Science Day 2023

The NIST Threshold Call

Cryptographic Technology Group, Computer Security Division

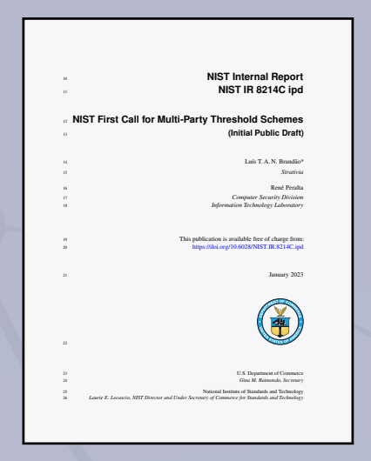
Updates at https://csrc.nist.gov/projects/threshold-cryptography

Crossing a "Threshold" …

- **What:** A door sill, crossed to enter a new space
- **Where:** into the **Advanced Cryptography** space (advanced features; secure data in use; multi-party protocols)
- **Whether:** are we ready? how should we cross it?

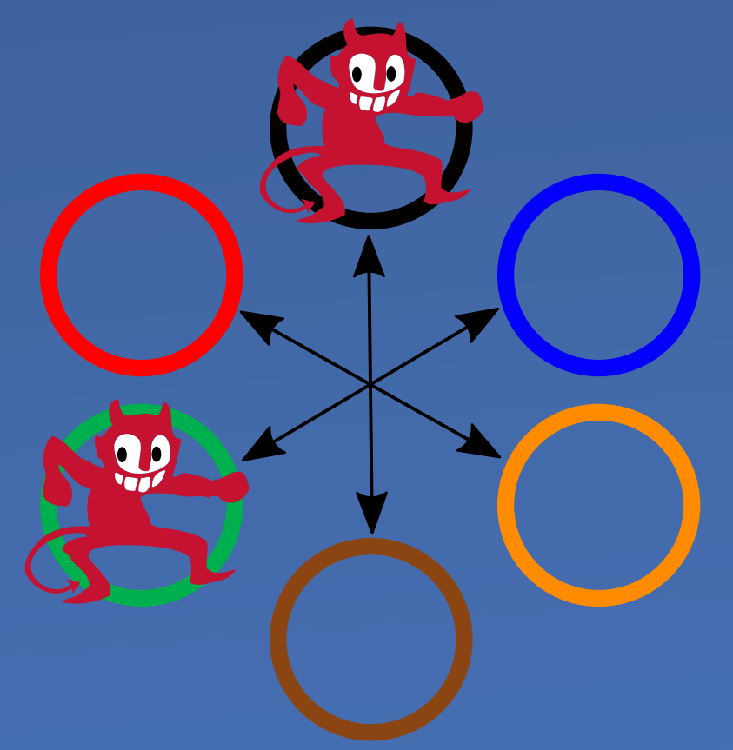
The "**NIST Threshold Call**" **process will:**

- gather a body of useful reference material
- help prepare for future recommendations



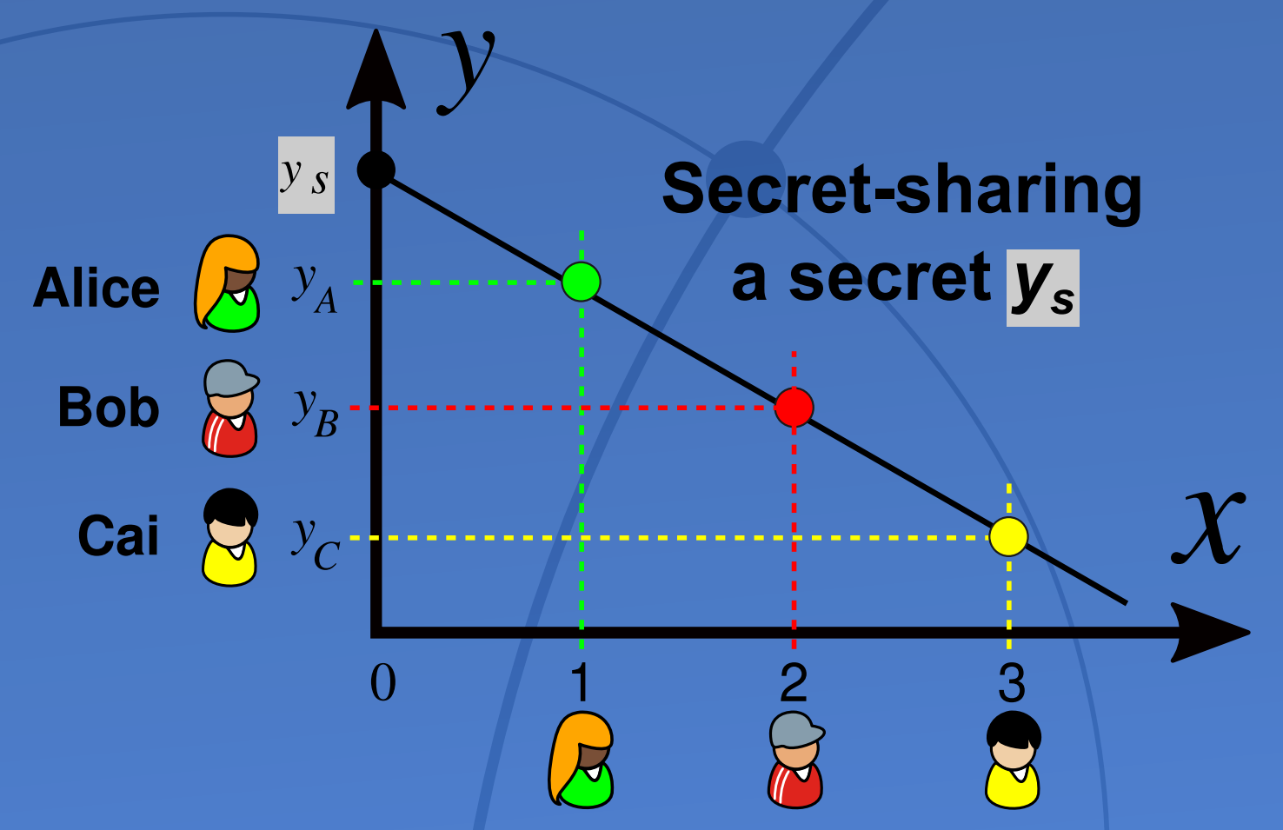
(NISTIR 8214C: NIST First Call for Multi-Party Threshold Schemes)

Threshold Schemes

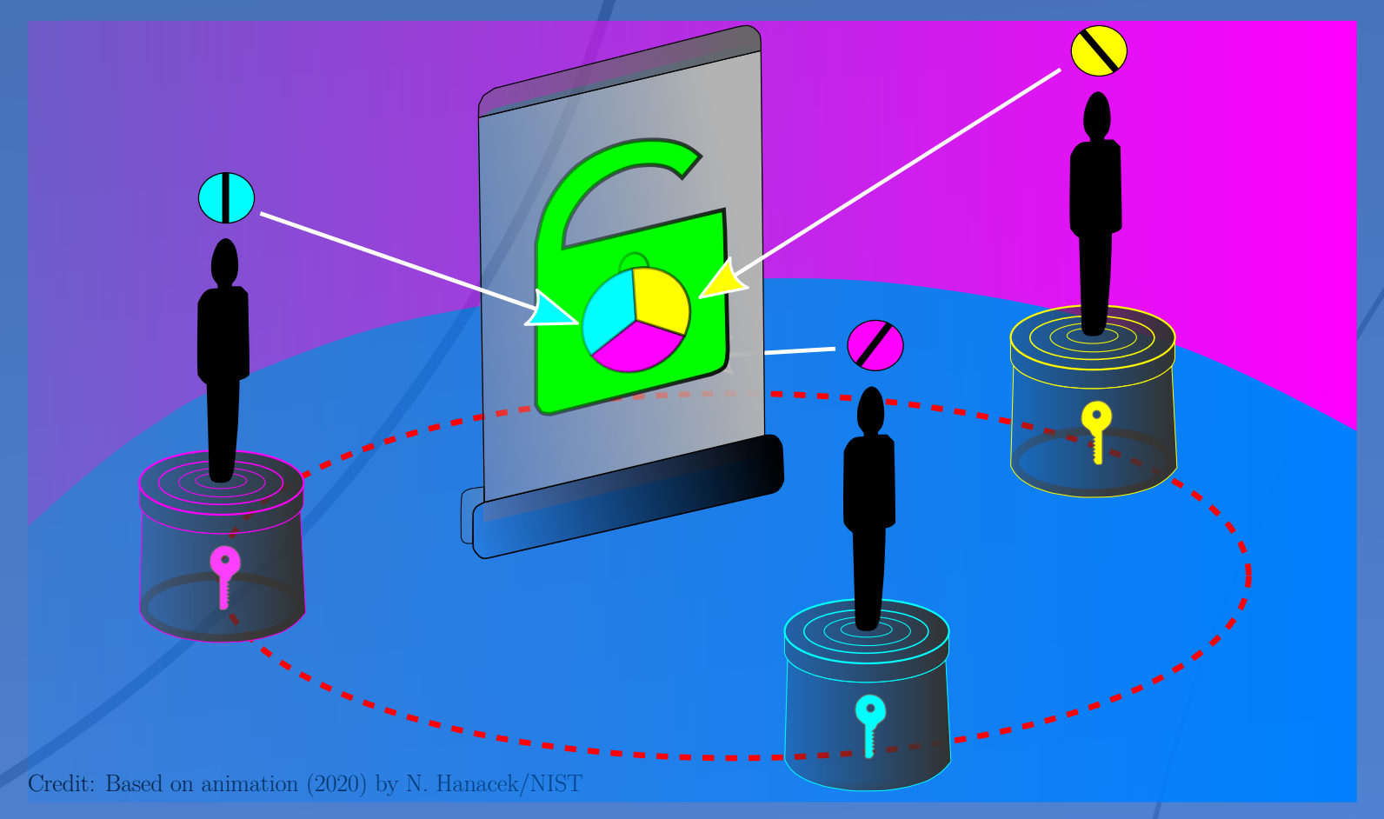


Corruption threshold: the system is secure even if f parties are malicious.

Participation threshold: the crypto operation needs k parties in agreement.



Secret-sharing stores the key in a distributed manner



Credit: Based on animation (2020) by N. Hanacek/NIST

Multi-party computation (MPC) performs operation without recombining the key

Calling for Threshold Schemes for:

- **Classic NIST-standardized crypto primitives**

Signing · Encryption · KeyGen · Hashing · RNG

- **Post-quantum (PQ) & lightweight primitives**

PQ signatures	PQ encryption	Lightweight AEAD

(AEAD = authenticated encryption with associated data)

- **Advanced cryptographic primitives:**
  - **Z**ero-**k**nowledge **p**roofs (ZKP)
  - **A**ttribute-**b**ased **e**ncryption (ABE)
  - **F**ully-**h**omomorphic **e**ncryption (FHE)
  - **M**ulti-**p**arty **c**omputation (MPC) building blocks

Adoption
Innov-ation
Standard

The MPTS 2023 Workshop

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

- Expressions of interest for future submissions
- Feedback useful for the threshold process
- Examples of techniques of interest

Trivia: 3 days (Sep. 26–28); 300+ registrations from ≈40 countries; 26 external talks; 9 NIST talks; 1 open session.

Also relevant: 3 PEC-STPPA events since Nov. 2022 (**S**pecial **T**opics on **P**rivacy and **P**ublic **A**uditability)

A Challenging & Pertinent Quest

- How *threshold-friendly* are the primitives?
- Assess the *quantum gap* (pre-quantum features not yet ready as post-quantum)
- Securely *compose* the building blocks

Threshold **Schemes are helping us cross the Advanced Cryptography "Threshold":**

- Toward technical recommendations / future processes
- Secure data in use (e.g., compute over encrypted data)
- Privacy-preserving collaborative computations

Led by the MPTC (**m**ulti-**p**arty **t**hreshold **c**rypto) & PEC (**p**rivacy-**e**nhancing **c**ryptography) projects

Upcoming

- Final version of NIST IR 8214B, on Threshold EdDSA (EdDSA = **Ed**wards-curve **D**igital **S**ignature **A**lgorithm)
- Final version of NIST IR 8214C, the Threshold Call
- Submissions deadline (2nd half of 2024)

Subscribe to the **MPTC** & **PEC** forums (mailing lists).

Poster produced by Luís Brandão[†] for the NIST-ITL Science Day 2023 (November 8th).
[†] Foreign Guest Researcher (non-employee) at NIST, contractor from Strativia.
The background and the header images were provided by the ITL Science Day Team.
Free-use cliparts were obtained (and/or adapted) from external sources, including clcker.com and iconpacks.net.