National Institute of Standards and Technology
U.S. Department of Commerce

Multi-Party Threshold Schemes

Computer Security Division (NIST-ITL)

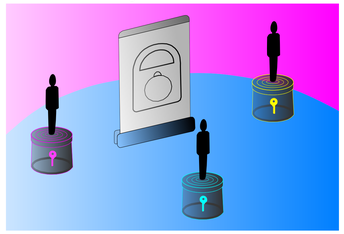
NIST Threshold Cryptography Project — Multi-Party Track

INFORMATION TECHNOLOGY LABORATORY

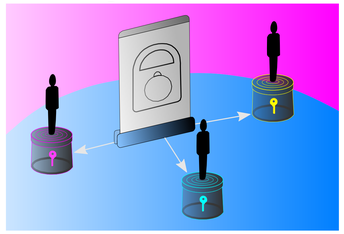
Threshold cryptographic operations

Distributed crypto operations without exposing the key to single-points of failure. Threshold decryption example:

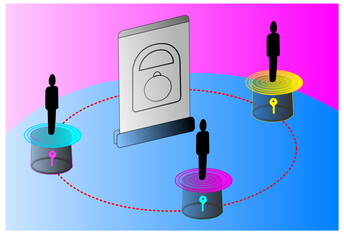
1. The key is secret-shared



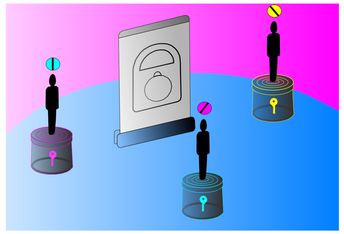
2. The ciphertext is sent to all



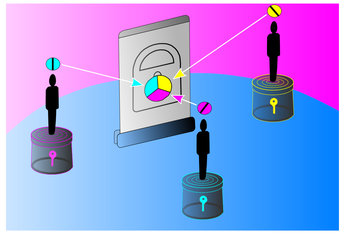
3. The parties can interact, but not reveal their secret-shares



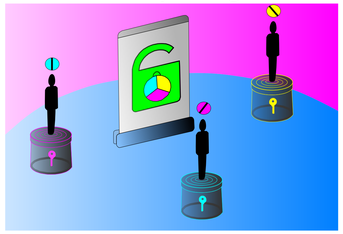
4. At some point, the parties obtain a "signature-share"



5. The signature-shares can be safely combined



6. The ciphertext is decrypted without the key being revealed



Adapted from animation (2020/July/7) by N. Hanacek/NIST.

Eliminate single-points of failure

- Attacks that exploit vulnerabilities in implementations
- Rogue operators that misuse secret keys

Potential new threshold standards

Key-generation (e.g., RSA, ECC, AES)

Signing (e.g., RSA, ECDSA, EdDSA)

Enciphering (e.g., AES, lightweight ciphers)

Decryption (e.g., RSA)

Random number generation

Post-Quantum Crypto (emerging standards)

Potential impact areas (examples):

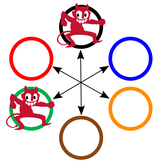
- Threshold signing → financial transactions
  (rogue insiders in institutions; hackers of blockchain wallets)
- Distributed key-gen → certification authorities
- Secret-sharing → store secrets at rest

External cliparts obtained/adapted from clker.com: key, signing pen, ciphertext, lock, dice, atom, dancing devil.

A standardization initiative

To improve the implementation security of our crypto standards.

NISTIR 8214A (July 2020):
NIST Roadmap Toward Criteria for
Threshold Schemes for Cryptographic Primitives



1. Devise **criteria** — **We are here now!**
2. **Call** for contributions (proposals, . . .)
3. **Evaluate** proposed threshold schemes
4. **Publish** new guidelines/standards (e.g., SP 800)

Upcoming workshop: MPTS 2020 (Nov 4–6)

NIST Workshop on **Multi-Party** Threshold Schemes

Will collect feedback from world-renowned experts in the area.

https://csrc.nist.gov/events/2020/mpts2020

More info at: https://csrc.nist.gov/Projects/Threshold-Cryptography
Poster presented at: NIST-ITL Virtual Science Day 2020 (October 29)
Poster prepared by: Luís T.A.N. Brandão, Michael Davidson, Apostol Vassilev

The first author is a Foreign Guest Researcher at NIST (Contractor via Strativia)