Threshold Cryptography for Multiple Operators

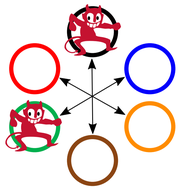
INFORMATION TECHNOLOGY LABORATORY

Cryptographic Technology Group, Computer Security Division

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

The threshold paradigm

Distribute trust over a secret key, via *secret-sharing*. Then, a key-based operation goes through without the key being in any one place.



Threshold: Secure even if f parties are malicious.

Focuses: signatures and encryption schemes.

Good news:

- Strong feasibility results (MPC)
- Well understood framework
- Expert stakeholders interested in standards

Challenges: many tradeoffs (e.g., various building blocks; crypto assumptions vs. efficiency) to consider; enable composability.

Webpage: https://csrc.nist.gov/projects/threshold-cryptography

Contact: threshold-MP@nist.gov

Poster produced by Luís T. A. N. Brandão (at NIST as a contractor from Strativia) for the NIST-ITL Science Day 2021 (October 28)

Towards guidelines

PAST (2019–2020)
- 2 reports
- 2 workshops

PRESENT **Call 2021a** for feedback **till Sep. 13**

UPCOMING **IR 8214B** Specify criteria

Call for feedback (2021a) on criteria:

Gadgets	**Interchangeability**	**Threshold profiles**
System model	**Games and UC**	**Adaptive security**

Looking forward:

- One "supplement" per primitive
- Public consultation with experts
- NISTIR on criteria
- Future guidance and recommendations

Acronyms. **AES**: Advanced Encryption Standard. **AHE**: Additively Homomorphic Encryption. **DSA**: Digital Signature Algorithm. **ECDSA**: Elliptic-curve DSA. **EdDSA**: Edwards-curve DSA. **MPC**: Secure Multiparty Computation. **RSA**: Rivest Shamir Adleman. **UC**: Universal Composability.

"Thresholdizations" in consideration

Legend: secret-shared (secret-key d, nonce k, primes p, q); clear view (message m, plaintext p, signature [component] s, modulus N).

Threshold EdDSA/Schnorr.
- $s = k + c \cdot d \pmod q$
- Linear in d and k: easy if k is random.

Threshold ECDSA.
- $s = k^{-1} \cdot (m + r \cdot d) \pmod q$
- Non-linear relation: MPC or AHE based.

Threshold RSA sign/decrypt.
- $s = m^d \pmod N$
- Easy to thresholdize using RSA.

Threshold AES.
- $c = \mathrm{Enc}_d(p)$. MPC for Boolean circuit.

Distributed RSA keygen.
- $p, q \leftarrow^{\$} \mathrm{Primes}[\lambda], N = p \cdot q$
- Pre-sieving, biprimality test (multi trials).