Upcoming NIST Call for Threshold Schemes

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

Cryptographic Technology Group
National **I**nstitute of **S**tandards and **T**echnology

Presented at Crypto 2022 Rump Session
August 16, 2022 @ Santa Barbara, US

* Luís Brandão: At NIST as a Foreign Guest Researcher (non-employee), Contractor from Strativia. Expressed opinions are from the speaker, not to be construed as official NIST views.

Multi-Party Threshold Cryptography (MPTC) project

Scope: multi-party threshold schemes for (*interchangeable* with)
several NIST specified primitives (key-based; stateless)

ECDSA **EdDSA**

RSA **AES** **EC-KE**

(with secret-shared secret/private key)

AES: **A**dvanced **E**ncryption **S**tandard. **ECDSA**: **E**lliptic-**c**urve **D**igital **S**ignature **A**lgorithm. **EdDSA**: **Ed**wards-curve**D**igital **S**ignature **A**lgorithm. **EC-KE**: **E**lliptic-**c**urve based **K**ey-**E**stablishment. **RSA**: **R**ivest–**S**hamir–**A**dleman (signature and encryption schemes).

Upcoming: A call for threshold schemes

Intention:

- Create a basis for a period of public analysis
  - **System** model and **security** formulation
  - **Protocol** specification and **reference open-source** implementation
  - **Security** analysis
- Interest in modular descriptions/implementation ... and composability
- Support future *Guidelines and Recommendations*

Upcoming: A call for threshold schemes

Intention:

- Create a basis for a period of public analysis
  - **System** model and **security** formulation
  - **Protocol** specification and **reference open-source** implementation
  - **Security** analysis
- Interest in modular descriptions/implementation ... and composability
- Support future *Guidelines and Recommendations*

Not intending: a competition to select a protocol for standardization

Example technical considerations

Interchangeability

E.g., probabilistic signatures interchangeable w.r.t. standardized verification (check Draft IR 8214B "Notes on threshold EdDSA/Schnorr")

Criteria w.r.t.

adaptive corruptions

security formulations

simulatable / game-based

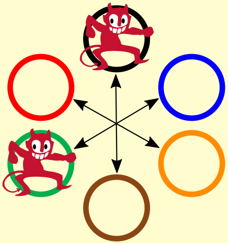
Strong threshold unforgeability for signatures

"Well behaved" parties with **bad randomness**

Agreeing on
session ids;
subset of participants;
input for operation

etc.

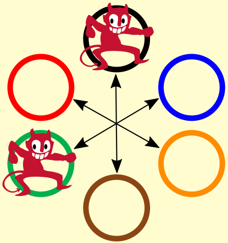
Aiming for Guidelines and Recommendations (G&R)



Various stakeholders can benefit from G&R:

- To-dos (best practices) and *to-don'ts* (pitfalls)
- Understanding of techniques and rationale
- Access to reference material / building blocks

Aiming for Guidelines and Recommendations (G&R)



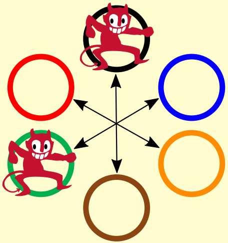
Various stakeholders can benefit from G&R:

- To-dos (best practices) and *to-don'ts* (pitfalls)
- Understanding of techniques and rationale
- Access to reference material / building blocks

Collaboration:

- Community participation is essential and highly appreciated!
- Stay tuned: we'll soon announce steps for feedback and participation

Aiming for Guidelines and Recommendations (G&R)



Various stakeholders can benefit from G&R:

- To-dos (best practices) and *to-don'ts* (pitfalls)
- Understanding of techniques and rationale
- Access to reference material / building blocks

Collaboration:

- Community participation is essential and highly appreciated!
- Stay tuned: we'll soon announce steps for feedback and participation

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

Thank you for your attention!