CYBERNETICA

Brief: On the need for threshold post-quantum (signature) schemes

Jan Willemson

November 4th, 2020

Threshold signatures

- Cryptocurrencies
- Server-assisted signature schemes
  - The reason of my interest in this area: SplitKey® digital signature product of Cybernetica

Threshold signatures

- Cryptocurrencies
- Server-assisted signature schemes
  - The reason of my interest in this area: SplitKey® digital signature product of Cybernetica
- In order to give standardized signatures, you can only use RSA or ECDSA
- When a sufficiently powerful quantum computer will be built, RSA and ECDSA will become weak, but the application scenarios requiring threshold signatures will still be there.

Two parallel standardization processes

- Threshold Schemes for Cryptographic Primitives (NISTIR 8214A)
- Post-Quantum Cryptography (NISTIR 8309)

Two parallel standardization processes

- Threshold Schemes for Cryptographic Primitives (NISTIR 8214A)
- Post-Quantum Cryptography (NISTIR 8309)
- Unfortunately, they do not overlap.
- NISTIR 8214A: "Although interesting, these cases are not considered in scope here for standardization, since the proposed conventional non-threshold primitives are still under security evaluation."

PQ schemes thresholdize poorly

- Daniele Cozzo and Nigel P. Smart. "*Sharing the LUOV: threshold post-quantum signatures.*" has mostly discouraging results.
- The same authors have also studied CSI-FiSh signature scheme that shows some promise, but currently only has a version with a specific short key length.

The need for threshold post-quantum schemes

- Classical asymmetric threshold schemes are not quantum-resistant.
- Thresholdizability is a property that rarely appears magically for the schemes that were not explicitly developed with this requirement in mind.
  - RSA and Schnorr schemes appear to be rare exceptions
- Thus we need a special effort to get schemes that would be quantum-resistant and have efficient threshold versions.

Thank you!

- For ideas, suggestions and discussions on threshold post-quantum (signature) schemes, contact `jan.willemson@cyber.ee`.