Threshold signatures on smartcards

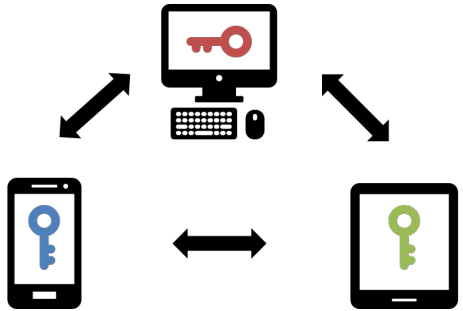
CHESS Brokerage Event 2025

Antonín Dufka
dufkan@mail.muni.cz
Masaryk University, Brno, Czech Republic

Threshold cryptography

- Secret key protection by distributed computation
  - the secret key is split into multiple shares
  - the shares are used in distributed computation
  - the secret key is never reconstructed
- Properties
  - eliminates single point of failure
  - introduces resilience against key loss
  - compatible with standard cryptographic structures

Single-party computation



Threshold cryptography

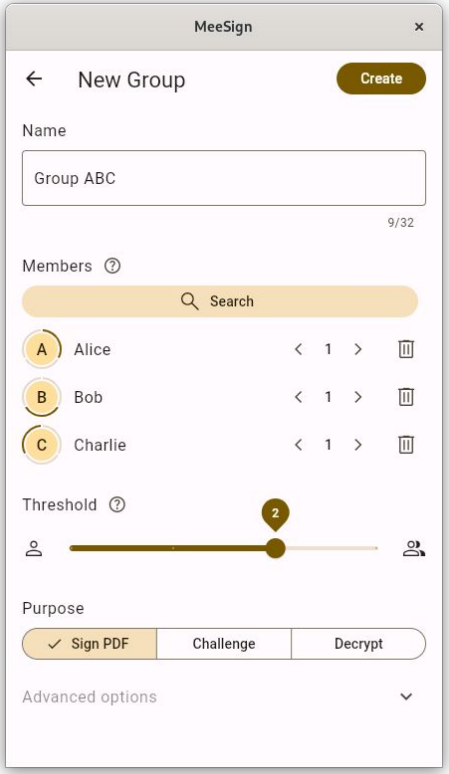
Threshold computation with smartcards

- Smartcards
  - provide secure storage
  - have standalone computing capabilities
  - are convenient for use with smartphones (NFC interface)

- k-of-n Schnorr
  - EdDSA, ECSCHNORR, BIP-Schnorr
  - https://github.com/crocs-muni/JCFROST
- two-party ECDSA
  - https://github.com/crocs-muni/JC2pECDSA

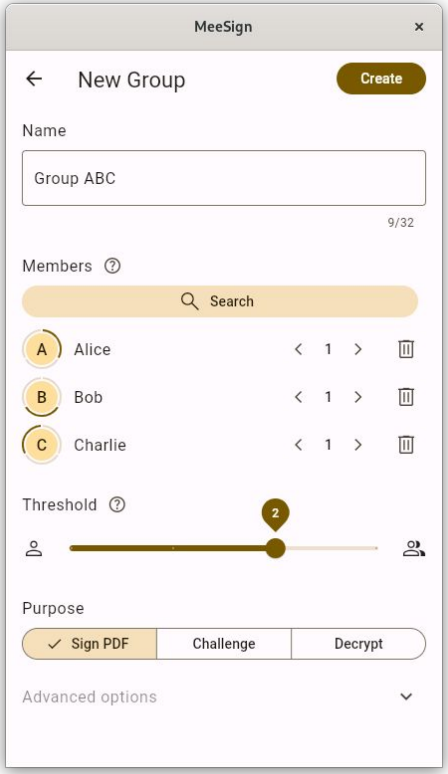
Threshold cryptography platform

- A platform demonstrating threshold cryptography
  - client application (Android, Windows, Linux, MacOS)
  - server facilitating communication (Linux)
- Features
  - k-of-n signing / decryption
  - smartcard support
  - share weighting
  - automated policies
  - integration via crypto-interfaces (PKCS#11, FIDO2, Web eID)



Threshold cryptography platform

- A platform demonstrating threshold cryptography
  - client application (Android, Windows, Linux, MacOS)
  - server facilitating communication (Linux)
- Features
  - k-of-n signing / decryption
  - smartcard support
  - share weighting
  - automated policies
  - integration via crypto-interfaces (PKCS#11, FIDO2, Web eID)



Thank you for your attention!