Open Discussion

- share recovery
- module validation
- (verifiable) secret sharing
- static vs. adaptive
- diversity
- composability
- passive vs. active
- pseudorandomness
- post-quantum security
- setup assumptions
- single vs. multiple devices
- pitfalls
- API
- robustness
- proofs of security
- intellectual property
- SMPC
- communication interfaces
- RSA
- detectable vs. undetectable
- ECDSA
- reliability
- asynchrony
- test harness
- k-out-of-n
- key generation
- dealer
- zero-knowledge proofs
- Curve25519
- deterministic vs. randomized
- Schnorr
- non-interactive
- applications
- roadmap
- reference implementation
- garbled circuits
- HSM
- intended outcome
- AES
- reactive vs. proactive
- rounds of communication
- availability
- side-channel attacks