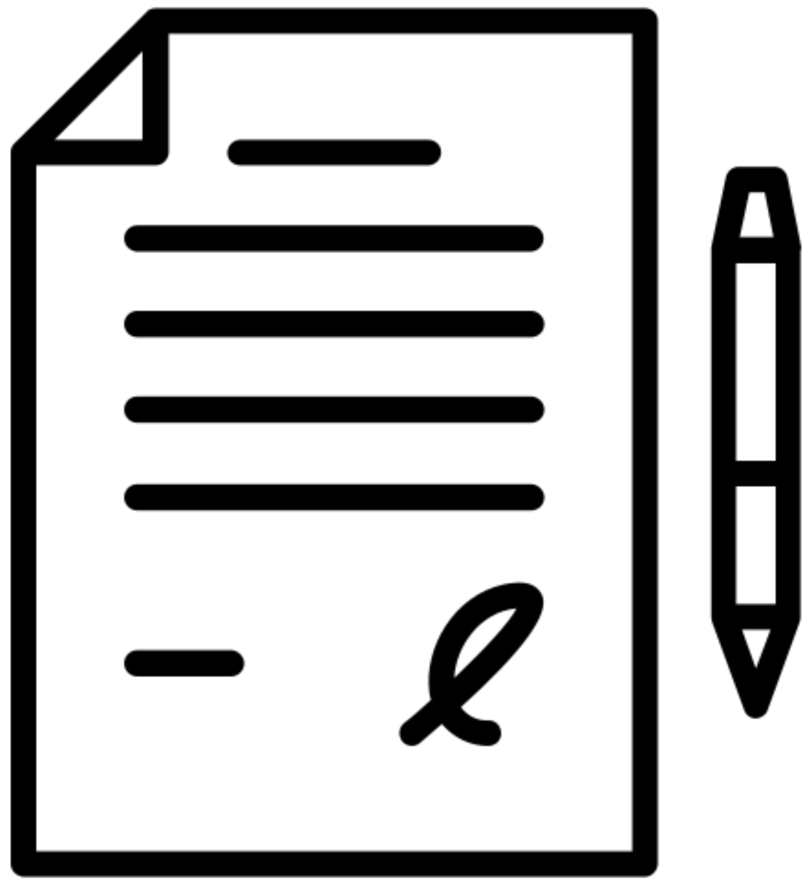
Multi-Party Schnorr Signatures

Elizabeth Crites
University of Edinburgh

April 23, 2023

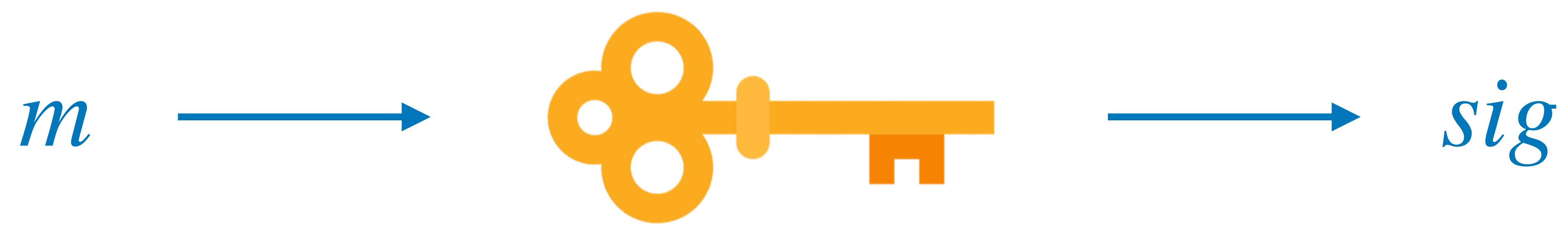
What is a Cryptographic Signature?

- used to verify that a message comes from a particular person
    - signer holds secret signing key
- main security property: unforgeability



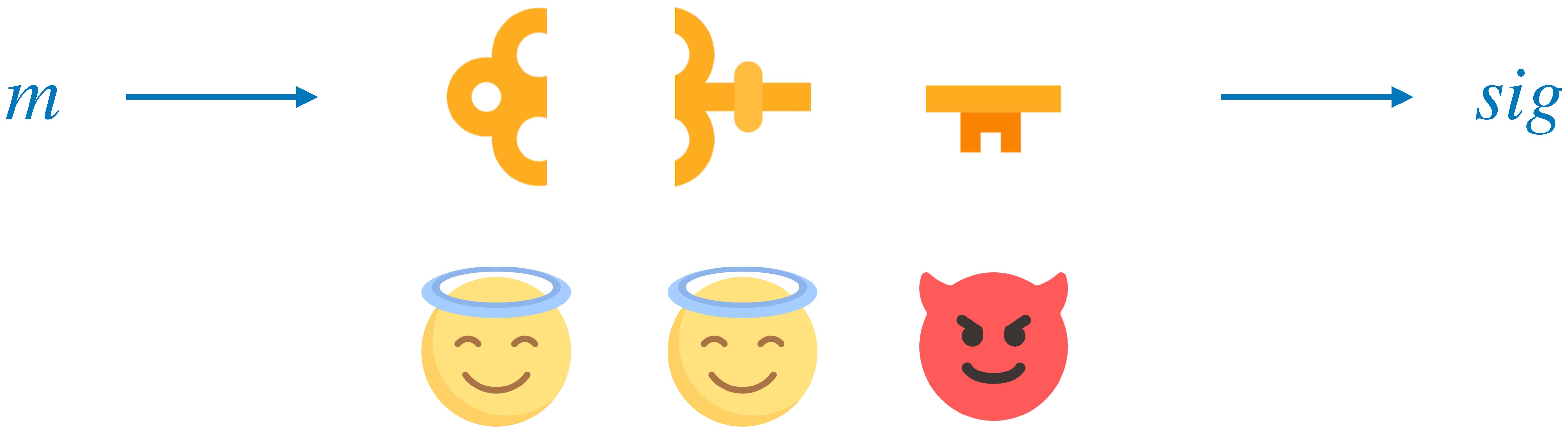
Threshold Cryptography

- introduced by Desmedt & Frankel [D87, DF89]
- secret key enables signatures, decryption, etc.
    - single point of failure
- idea: distribute the secret key among several parties
    - some fraction may be corrupt

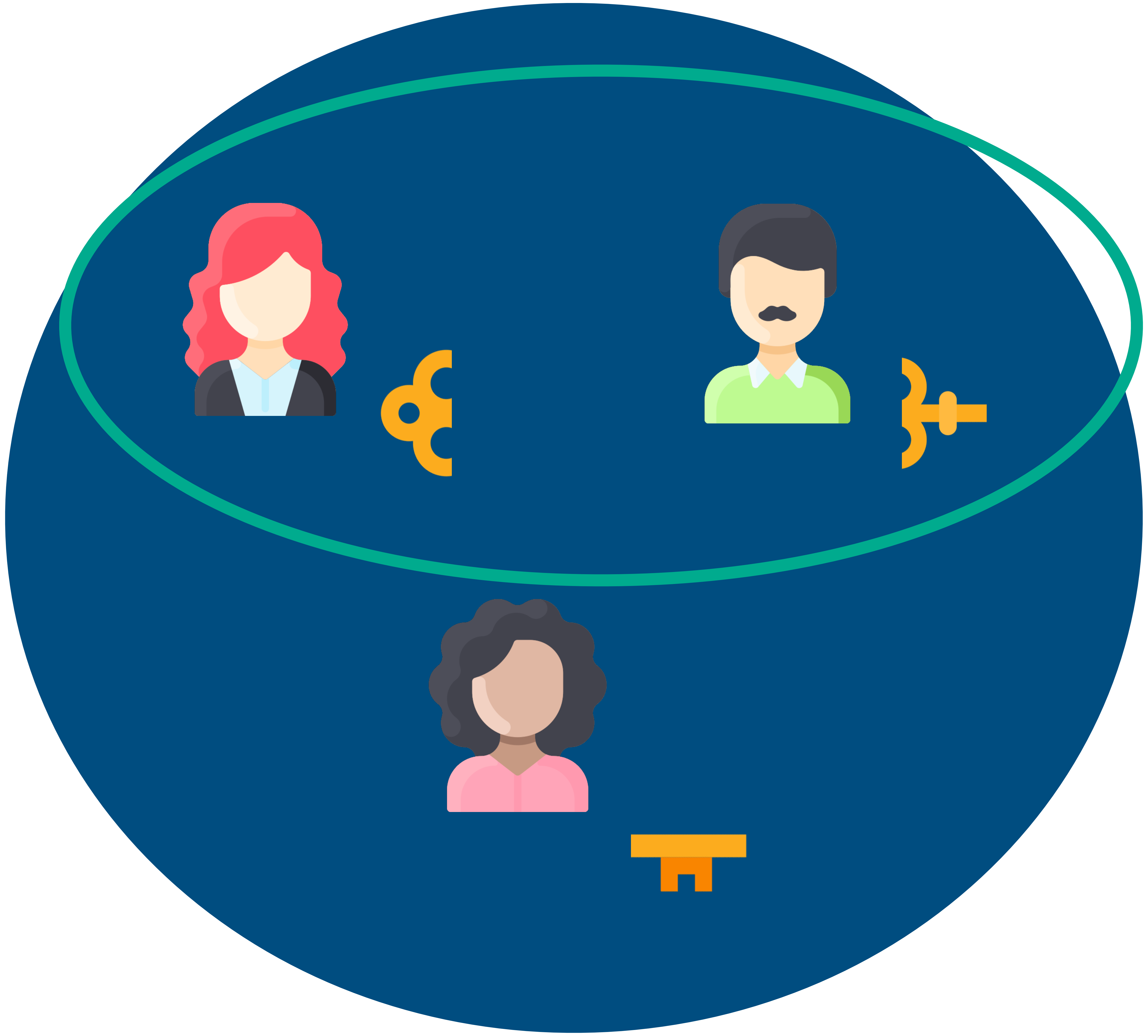


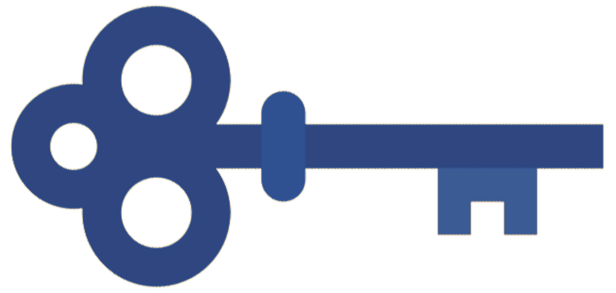
Threshold Cryptography

- distribute the secret key via:
  - trusted key generation *algorithm* (Shamir secret sharing [Sha79])
  - distributed key generation *protocol* (DKG)



What are Threshold Signatures?



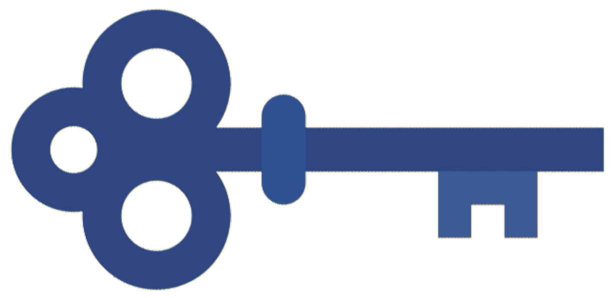


Public Key PK

- t-out-of-n
- trusted key generation or DKG to produce PK

$(2,3)$ Example

What are Multi-Signatures?



Public Key PK

- n-out-of-n
- key aggregation to produce PK
- set of signers can be spontaneous

$(3,3)$ Example

Why Multi-Party Schnorr Signatures? Why Now?

(Single-Party) Schnorr Signature Scheme [Sch91]

To generate a key pair:

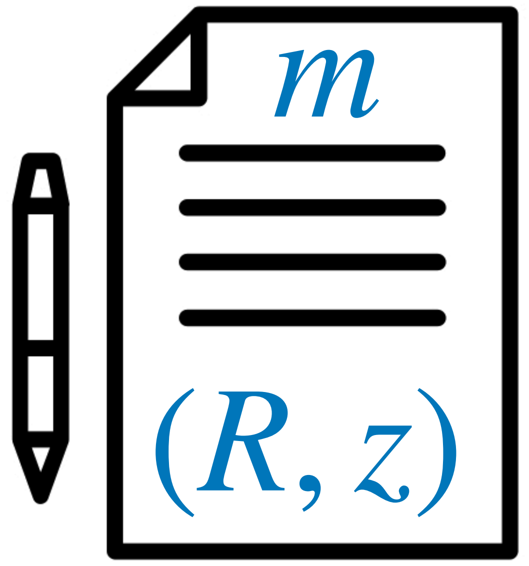
$$sk \leftarrow \mathbb{F};\ \ PK \leftarrow g^{sk}$$

To sign a message m:

$$r \leftarrow \mathbb{F};\ \ R \leftarrow g^{r}$$
$$c \leftarrow H(PK, m, R)$$
$$z \leftarrow r + c \cdot sk$$

$$\xrightarrow{\quad (R, z) \quad}$$

(sk, r)



Verify:

$$c \leftarrow H(PK, m, R)$$
$$R \cdot PK^{c} = g^{z}$$ ✓

Multi-Party Schnorr Signature Scheme

Key Generation: PK

sk_1 $\quad$ sk_2

$R_1 \leftarrow g^{r_1}$ $\quad$ $R_2 \leftarrow g^{r_2}$

$$R = R_1 R_2$$

$$c \leftarrow H(PK, m, R)$$

$$z_1 \leftarrow r_1 + c \cdot sk_1 \quad z_2 \leftarrow r_2 + c \cdot sk_2$$

Round 1:

R_1, R_2 $\longrightarrow$

Round 2:

z_1, z_2 $\longrightarrow$

(sk_1, r_1)

(sk_2, r_2)

m

(R, z)

Combine / Verify:

$$z \leftarrow z_1 + z_2$$

$$c \leftarrow H(PK, m, R)$$

$$R \cdot PK^c = g^z \checkmark$$

NOT concurrently secure ✗

	Scheme	Secure Under	Signing Rounds
Multi-Signatures	MuSig [MPSW18, BDN18] SimpleMuSig [BDN18, CKM21]	DL+ROM	3
	MuSig2 [NRS21] DWMS [AB21] SpeedyMuSig [CKM21]	OMDL+ROM	2
Threshold Signatures	Lindell22 Sparkle [CKM23]	Schnorr DL+ROM	3
	FROST [KG20, BCKMTZ22] FROST2 [CKM21]	OMDL+ROM	2

All are concurrently secure ✓

One-More Discrete Logarithm (OMDL):

- stronger assumption

+ essentially non-interactive signing

MuSig2: Simple Two-Round Schnorr Multi-Signatures

Jonas Nick[1], Tim Ruffing[1], and Yannick Seurin[2]

FROST: Flexible Round-Optimized Schnorr Threshold Signatures

Chelsea Komlo
University of Waterloo, Zcash Foundation
ckomlo@uwaterloo.ca

Ian Goldberg
University of Waterloo
iang@uwaterloo.ca

How to Prove Schnorr Assuming Schnorr: Security of Multi- and Threshold Signatures

Elizabeth Crites[1], Chelsea Komlo[2], and Mary Maller[3]

Better than Advertised Security for Non-interactive Threshold Signatures

Mihir Bellare[1], Elizabeth Crites[2], Chelsea Komlo[3], Mary Maller[4], Stefano Tessaro[5], and Chenzhi Zhu[5](✉)

Fully Adaptive Schnorr Threshold Signatures

Elizabeth Crites[1], Chelsea Komlo[2], and Mary Maller[3]

Deployment and Standardization

Multi-Party Schnorr Signatures in Practice

FROST

firo

AMIS

CHAINFLIP

toposware

serai-dex/**serai**

9 Contributors · 2 Used by · 94 Stars · 18 Forks

PENUMBRA

DFNS

jesseposner/
FROST-BIP340

BIP340 compatible implementation of Flexible Round-Optimized Schnorr Threshold Signatures (FROST). This work is made possible with the support of Brink.

2 Contributors · 2 Issues · 20 Stars · 3 Forks

CRYPTOSAT
TRUST IN SPACE

MuSig2

Blockstream

BlockstreamResearch / **secp256k1-zkp**

LLFourn / **secp256kfun**

bitcoin/bips
#1372 **Add BIP MuSig2**

input-output-hk / **musig2**

BlockstreamResearch/secp256k1-zkp
#223 **musig: Update to BIP v1.0.0-rc.4 (Check pubnonce in NonceGe...**

0 comments · 3 reviews · 3 files · +15 −7

real-or-random • March 3, 2023 · 1 commit

muun
Self-custodial wallet for bitcoin and lightning.

Standardization

NIST | COMPUTER SECURITY RESOURCE CENTER CSRC

NISTIR 8214C (Draft)

NIST First Call for Multi-Party Threshold Schemes

Date Published: January 25, 2023

Comments Due: April 10, 2023

Email Comments to: nistir-8214C-comments@nist.gov

Author(s)

Luís T. A. N. Brandão (Strativia), Rene Peralta (NIST)

https://csrc.nist.gov/publications/detail/nistir/8214c/draft

Thank you!

References

[AB21] H. K. Alper, J. Burdges. Two-Round Trip Schnorr Multi-signatures via Delinearized Witnesses. CRYPTO 2021.

[BCKMTZ22] M. Bellare, E. Crites, C. Komlo, M. Maller, S. Tessaro, and C. Zhu. Better than advertised security for non-interactive threshold signatures. CRYPTO 2022.

[BP23] L. Brandao and R. Peralta. NIST First Call for Multi-Party Threshold Schemes. https://csrc.nist.gov/publications/detail/nistir/8214c/draft. 2023.

[BDN18] D. Boneh, M. Drijvers, G. Neven. Compact Multi-signatures for Smaller Blockchains. ASIACRYPT 2018.

[CKGW22] D. Connolly, C. Komlo, I. Goldberg, and C. Wood. Two-Round Threshold Schnorr Signatures with FROST. 2022. url: https://datatracker.ietf.org/doc/draft- irtf-cfrg-frost/.

[CKM21] E. Crites, C. Komlo, and M. Maller. How to prove Schnorr assuming Schnorr: Security of multi- and threshold signatures. ePrint: https://eprint.iacr.org/2021/1375.

[CKM23] E. Crites, C. Komlo, and M. Maller. Fully Adaptive Schnorr Threshold Signatures. ePrint: https://eprint.iacr.org/2023/445.

[D87] Y. Desmedt. Society and group oriented cryptography: A new concept. CRYPTO 1987.

[DF89] Y. Desmedt and Y. Frankel. Threshold cryptosystems. CRYPTO 1989.

[KG20] C. Komlo and I. Goldberg. Frost: flexible round-optimized schnorr threshold signatures. SAC 2020.

[MPSW18] G. Maxwell, A. Poelstra, Y. Seurin, P. Wuille. Simple Schnorr multi-signatures with applications to Bitcoin. DESI 2019.

[NRS21] J. Nick, T. Ruffing, and Y. Seurin. MuSig2: Simple Two-Round Schnorr Multi- signatures. CRYPTO 2021.

[Sch91] C.-P. Schnorr. Efficient Signature Generation by Smart Cards. JoC 1991.

[Sha79] A. Shamir. How to Share a Secret. Commun. ACM 1979.

[SS01] D. R. Stinson and R. Strobl. Provably Secure Distributed Schnorr Signatures and a (t, n) Threshold Scheme for Implicit Certificates. ACISP 2001.