Recent Developments on Multi-Party Schnorr Signatures

Elizabeth Crites
Web3 Foundation

Roadmap

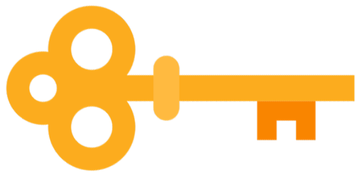
- What is a digital signature?
- Why Schnorr signatures?
- Why multi-party signatures?
- Recent developments on multi-party Schnorr signatures
- New directions

Roadmap

- What is a digital signature?
- Why Schnorr signatures?
- Why multi-party signatures?
- Recent developments on multi-party Schnorr signatures
- New directions

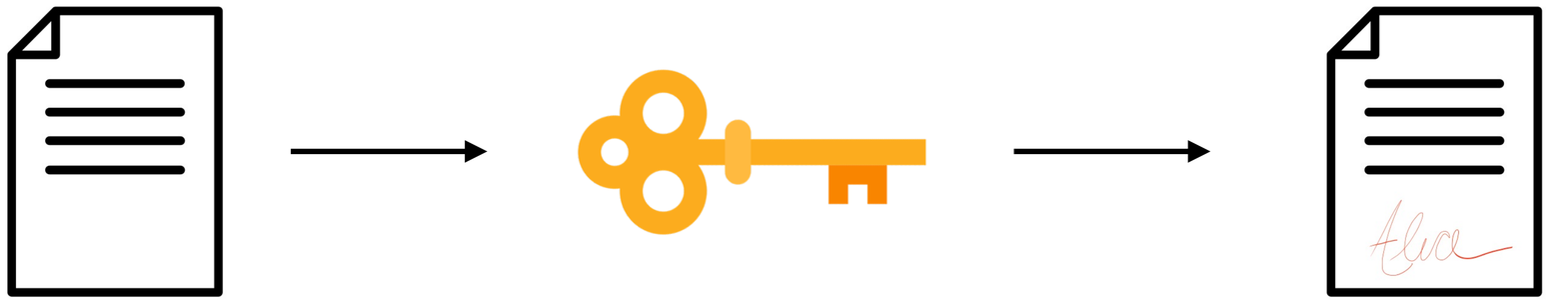
What is a cryptographic secret key?

- a piece of information (i.e., a string of numbers/letters) used to secure digital communication
- secret key enables signatures, decryption, etc.
    - single point of attack or failure



What is a digital signature?

- used to verify that a message comes from a particular person
    - signer holds secret signing key
- digital signatures are ubiquitous

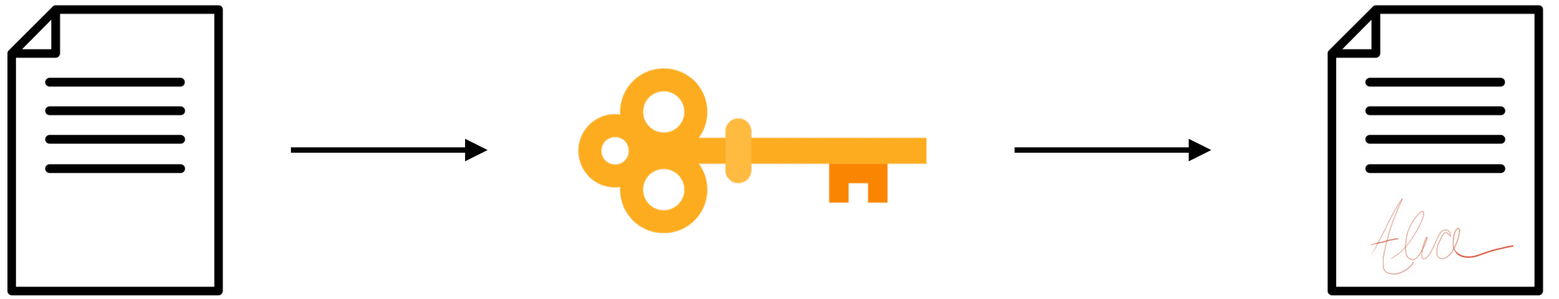


message secret key signature

Unforgeability:

Attacker cannot forge signatures.

What is a Schnorr signature?



message

m

(string)

secret key

sk

(field element)

r_m

(field element, per message)

signature

(R, z)

(group element, field element)

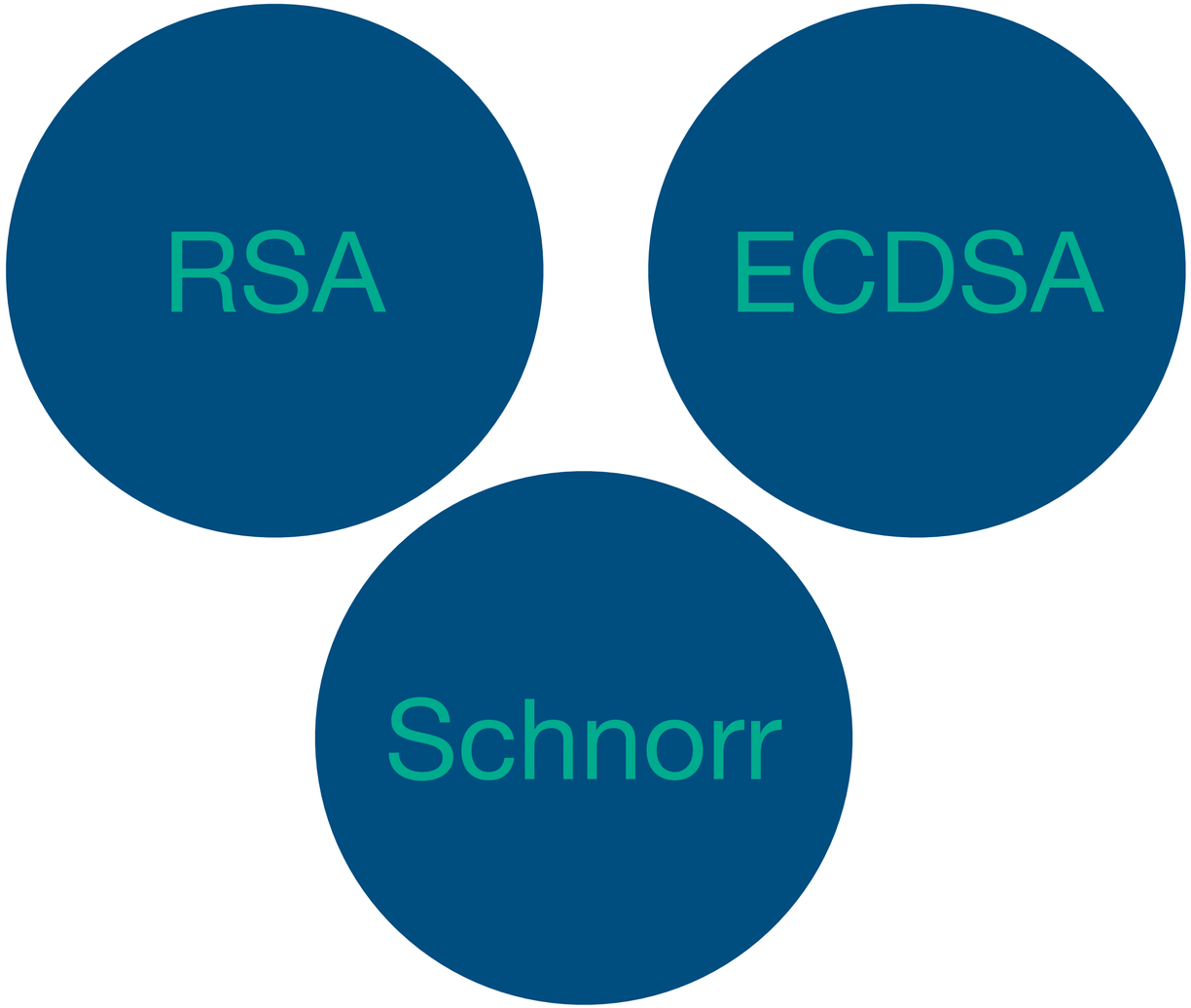
$g^z = R \cdot PK^{\text{Hash}(PK,\, m,\, R)}$

(signature verification)

Roadmap

- What is a digital signature?
- Why Schnorr signatures?
- Why multi-party signatures?
- Recent developments on multi-party Schnorr signatures
- New directions

NIST Standardized Signatures



NIST COMPUTER SECURITY RESOURCE CENTER CSRC

NIST Standardized Signatures

- signatures and keys are large
- 6 times the size of Schnorr/ECDSA signatures
- still used in legacy systems

NIST Standardized Signatures

- designed to get around the patent for Schnorr signatures (1991-2008)
- 2000: NIST standardized
- complex (especially multi-party ECDSA)

NIST Standardized Signatures

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

- 1991: paper by Claus Peter Schnorr
- clean, efficient scheme, straightforward security proof
- 2008: patent expires
- 2021: Bitcoin moved from ECDSA to Schnorr (BIP 340)
- 2023: NIST standardized

NIST Standardized Signatures

RSA

ECDSA

Schnorr

Honourable Mention

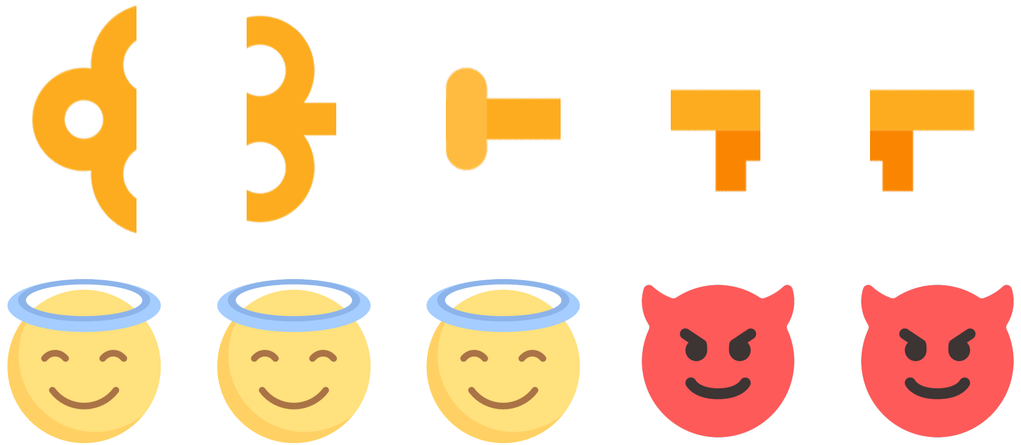
- used everywhere (e.g., for generating public randomness used on blockchains)
- verification is slow

Roadmap

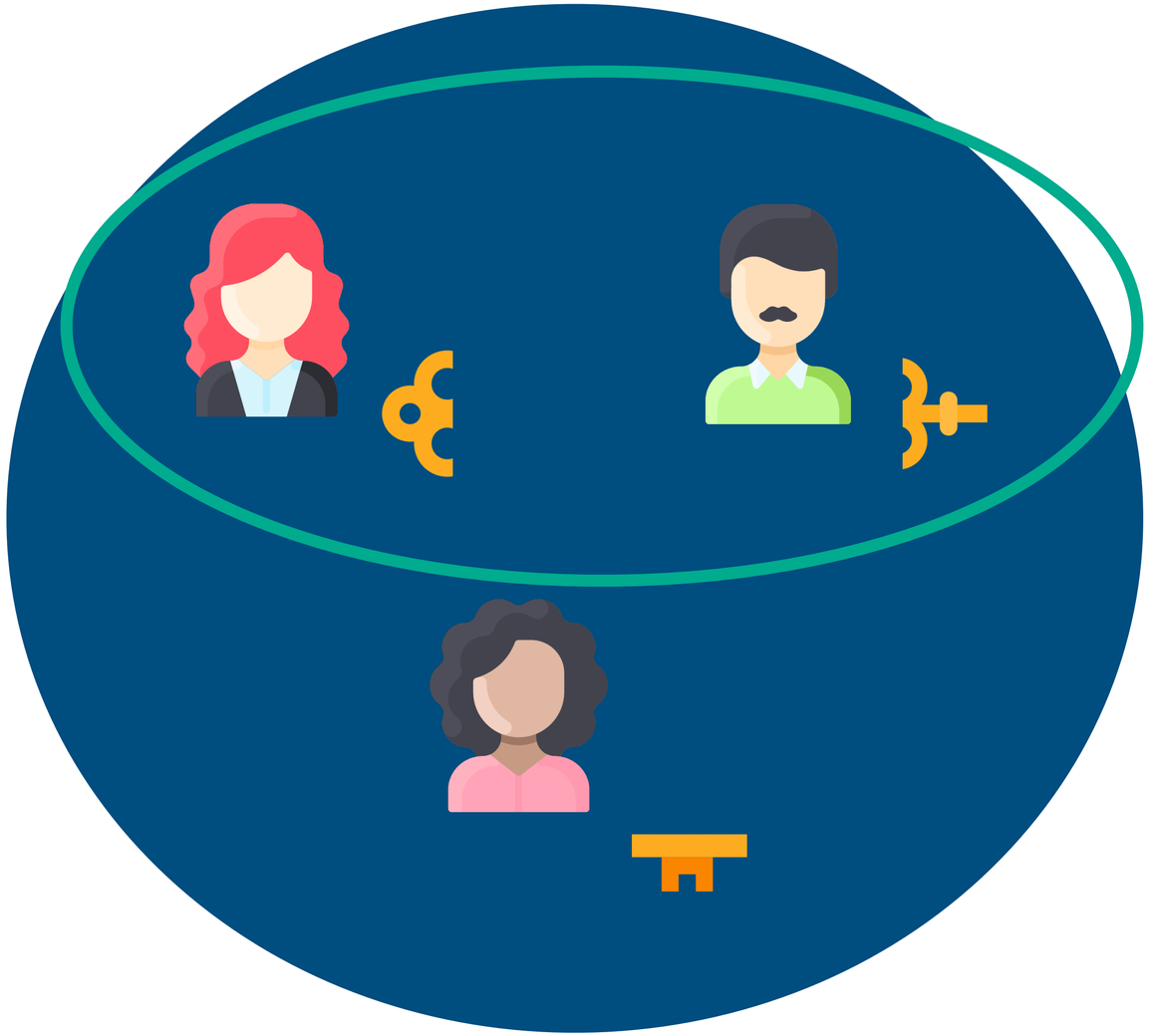
- What is a digital signature?
- Why Schnorr signatures?
- Why multi-party signatures?
- Recent developments on multi-party Schnorr signatures
- New directions

Secret key is single point of failure

- secret key enables signatures, decryption, etc.
    - attractive target for misuse or forgery
    - loss or theft can be catastrophic
- solution: distribute the secret key among several parties (some corrupt)



What are threshold signatures?



public key PK

- t-out-of-n
- public key PK representing all n parties

$(2,3)$ Example

What are multi-signatures?

public key PK

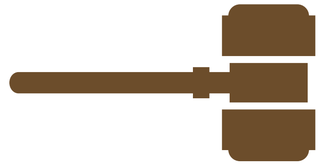
- n-out-of-n
- does not require secret sharing to produce PK
- n signers can be spontaneous

$(3,3)$ Example

Use-cases for multi-party signatures

Cryptocurrency wallets

- allow multiple parties to authorize a spend transaction
- distributed storage of secret key



Certification authorities (CAs)

- distribute trust

Desiderata for multi-party Schnorr signing

- produce a single signature
  - Bitcoin Multisig addresses were previously n signatures
  - off-chain signing, one signature on chain
- produce a Schnorr signature
  - backwards compatible with every system using Schnorr signatures
- 2-3 signing rounds

Roadmap

- What is a digital signature?
- Why Schnorr signatures?
- Why multi-party signatures?
- Recent developments on multi-party Schnorr signatures
- New directions

Concurrent Security:
Attacker cannot forge signatures, even if they open multiple signing sessions in parallel.

Prior broken attempts (and a secure one)

- [NKDM03, DEFKLNS19, BLLOR21] show how to break unforgeability in concurrent setting (“ROS” attack)
- Affected many Schnorr schemes:
    - multi-signature MuSig (2-round) [MPSW18a]
    - threshold signature FROST [KG20a]
    - blind signatures [PS00, Sch01]
    - and more!
- Most did not claim concurrent security
- Stinson & Strobl [SS01] secure (but unfortunately many signing rounds)

Schnorr Multi-Signatures (n-out-of-n)

3-Round:

- **MuSig** [MPSW18, BDN18]
- **SimpleMuSig** [BDN18, **C**KM21]

2-Round:

- **MuSig2** [NRS21]
- **DWMS** [AB21]
- **SpeedyMuSig** [**C**KM21]

Schnorr Threshold Signatures

3-Round:

- **SimpleTSig** [**C**KM21]
- **Classic/Zero Schnorr** [Makriyannis22]
- **Lindell22** [Lindell22]
- **Sparkle** [**C**KM23]

2-Round:

- **FROST** [KG20b, B**C**KMTZ22]
- **FROST2** [**C**KM21]
- **FROST3** [RRJSS22, CGRS23]
- all are partially non-interactive (1 offline round, 1 online)

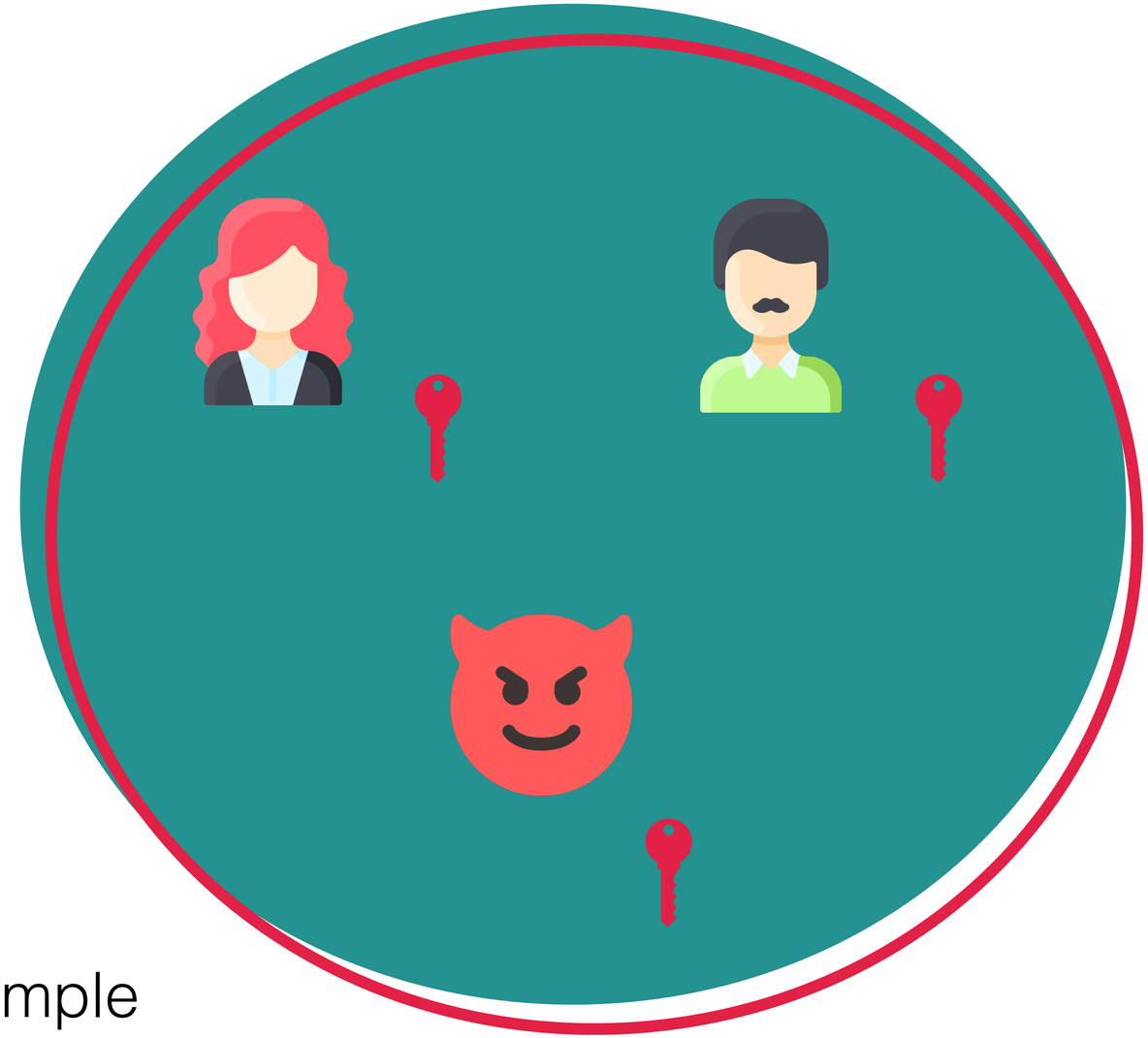
Unforgeability:

Attacker cannot forge signatures,
even in the concurrent setting.

Liveness:

System can always create signatures.

Multi-signatures do not guarantee liveness

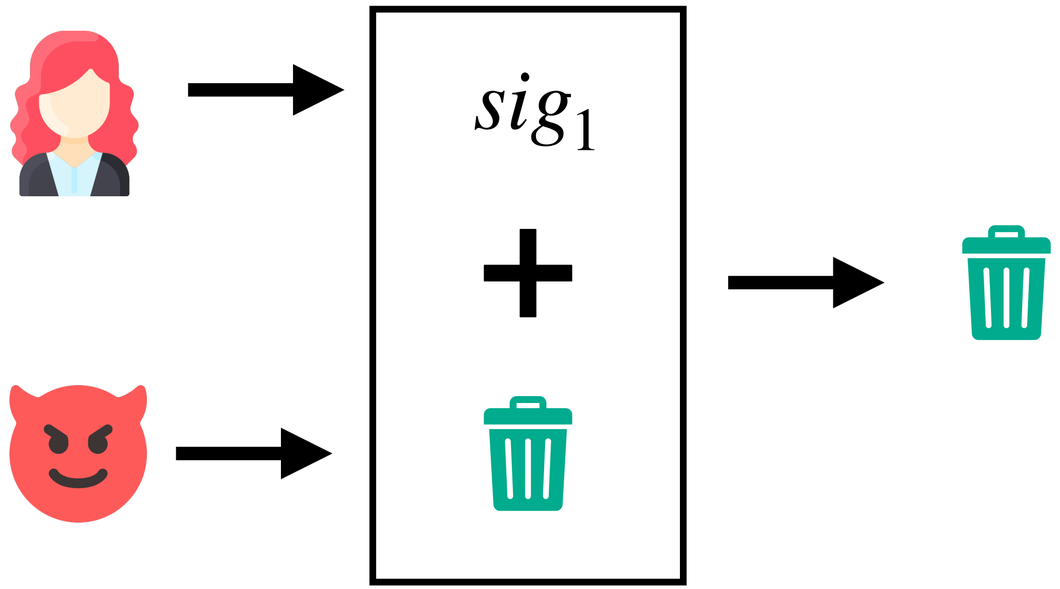


- if even one signer is unavailable, signing is not possible

(3,3) Example

FROST is not robust

- if even one signer outputs garbage, the resulting signature is garbage
- the protocol must be re-run with a different subset of signers



(2,3) Example

Robustness:

The protocol succeeds so long as at least t players participate honestly.

(Required for liveness!)

Robust Schnorr Threshold Signatures

- **ROAST** [RRJSS22]
- **Groth-Shoup'23** [GS23]
- **SPRINT** [BHKMR23]
- **HARTS** [BLSW24]
- constant number of signing rounds

Bitcoin MuSig2 Standardization

```
BIP: 327
Title: MuSig2 for BIP340-compatible Multi-Signatures
Author: Jonas Nick <jonasd.nick@gmail.com>
        Tim Ruffing <crypto@timruffing.de>
        Elliott Jin <elliott.jin@gmail.com>
Status: Draft
License: BSD-3-Clause
Type: Informational
Created: 2022-03-22
```

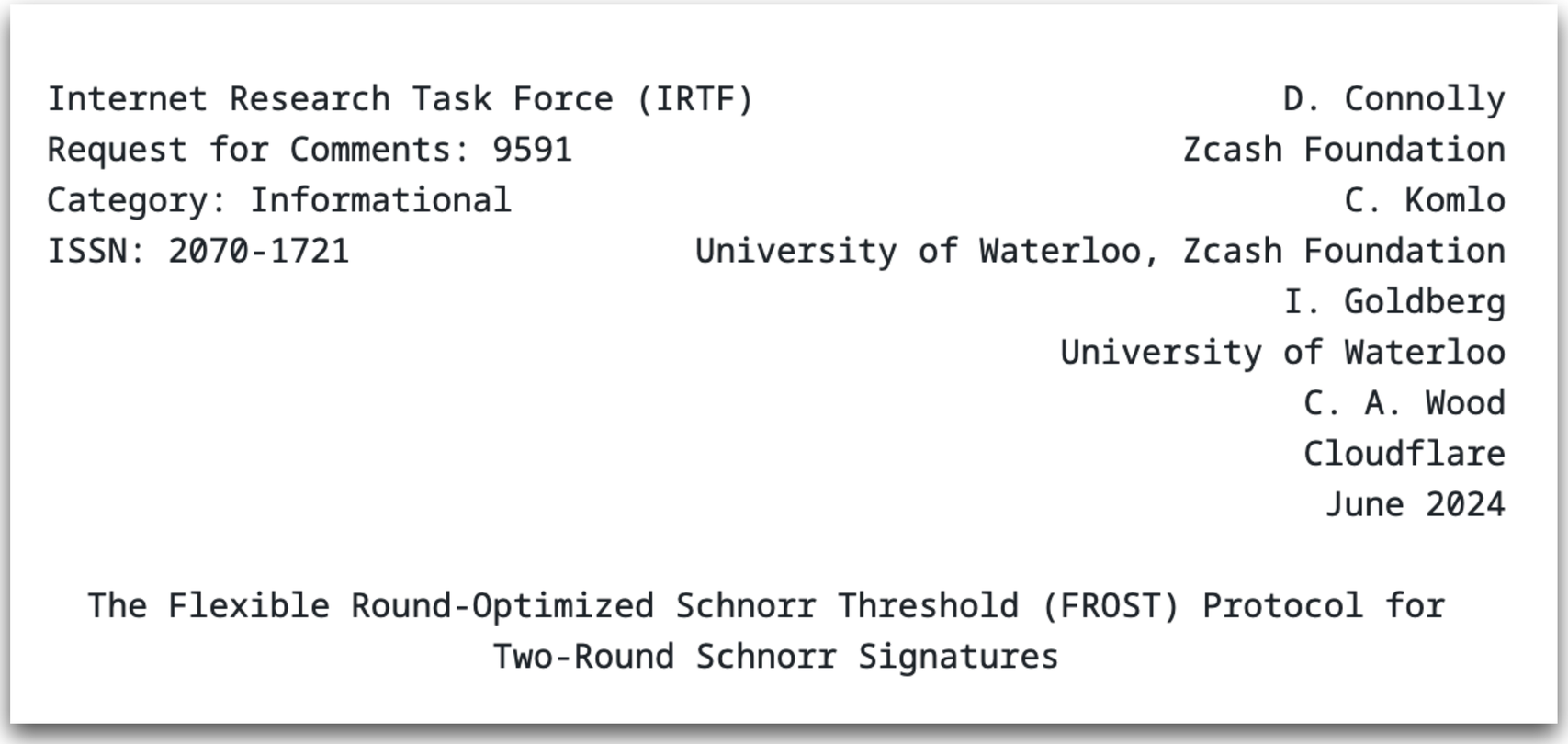
https://github.com/bitcoin/bips/blob/master/bip-0327.mediawiki

Zcash FROST Standardization

```
ZIP: 312
Title: FROST for Spend Authorization Signatures
Owners: Conrado Gouvea <conrado@zfnd.org>
        Chelsea Komlo <ckomlo@uwaterloo.ca>
        Deirdre Connolly <deirdre@zfnd.org>
Status: Draft
Category: Wallet
Created: 2022-08-dd
License: MIT
Discussions-To: <https://github.com/zcash/zips/issues/382>
Pull-Request: <https://github.com/zcash/zips/pull/662>
```

https://github.com/ZcashFoundation/zips/blob/zip-frost/zip-0312.rst

IRTF FROST Standardization



Internet Research Task Force (IRTF)
Request for Comments: 9591
Category: Informational
ISSN: 2070-1721

D. Connolly
Zcash Foundation
C. Komlo
University of Waterloo, Zcash Foundation
I. Goldberg
University of Waterloo
C. A. Wood
Cloudflare

June 2024

The Flexible Round-Optimized Schnorr Threshold (FROST) Protocol for Two-Round Schnorr Signatures

https://datatracker.ietf.org/doc/draft-irtf-cfrg-frost/

Multi-party Schnorr signatures in use today

FROST 1/2/3

firo

toposware

PENUMBRA

CRYPTOSAT
TRUST IN SPACE

AMIS

CHAINFLIP

serai-dex/**serai**

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

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

MuSig2 / DWMS

Blockstream

BlockstreamResearch / **secp256k1-zkp**

LLFourn / **secp256kfun**

input-output-hk / **musig2**

bitcoin/bips
#1372 **Add BIP 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.

Roadmap

- What is a digital signature?
- Why Schnorr signatures?
- Why multi-party signatures?
- Recent developments on multi-party Schnorr signatures
- New directions

Adaptive Security:
Attacker cannot forge signatures, even if it can corrupt signers during signing.

New directions

- Adaptive security
    - **Sparkle** [**C**KM23] is the only adaptively secure threshold Schnorr signature scheme to date, without secure erasure of secret state
- Efficient deterministic threshold Schnorr signatures (a.k.a. EdDSA signatures)
    - nonce R very sensitive
    - current deterministic schemes require heavyweight zk proofs **MuSig-DN** [NRSW202], [GKMN21] or are only secure for small numbers of parties **Arctic** [KG24]
- Practical key generation protocols

NIST Threshold 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

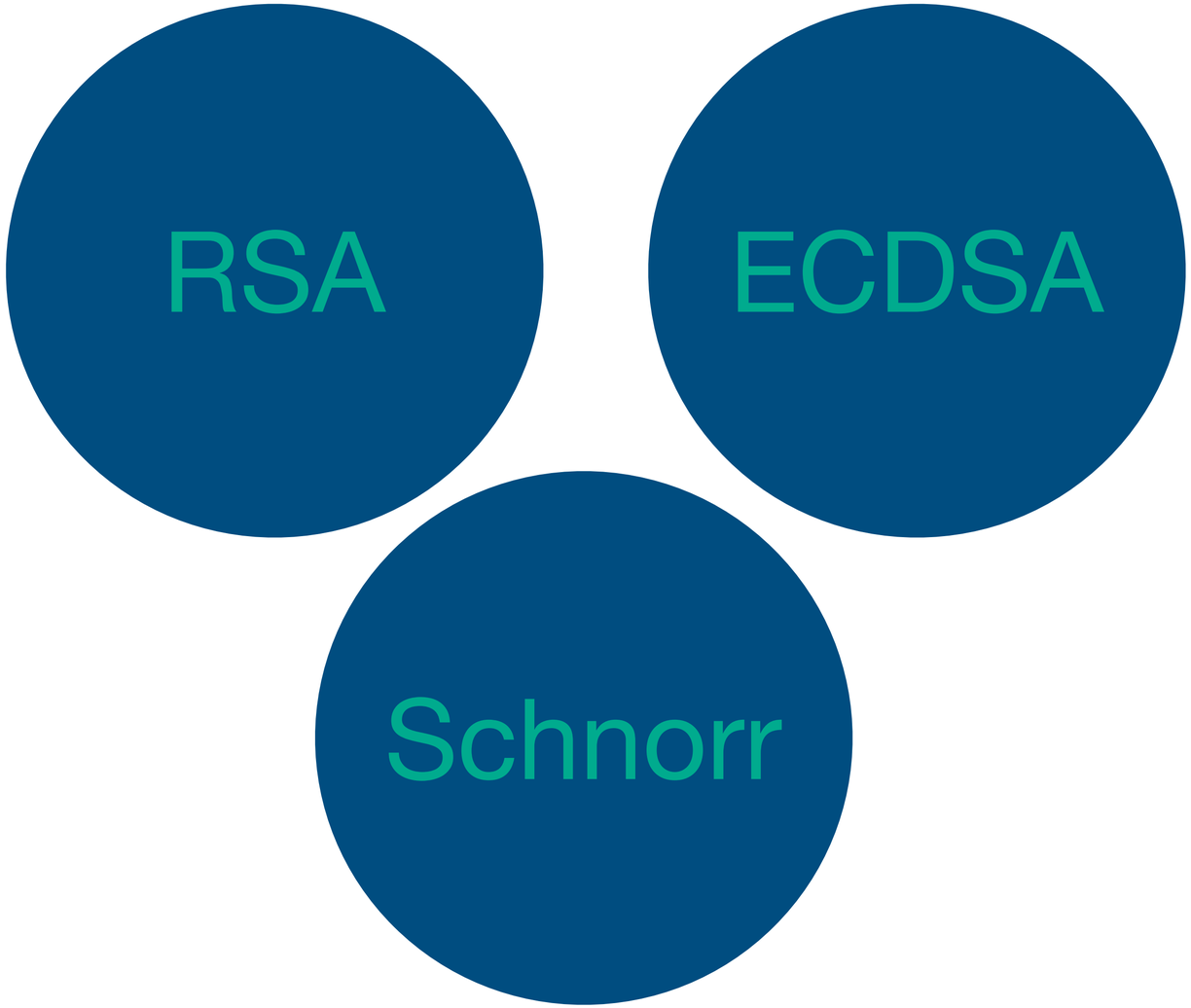
Email Comments to: nistir-8214C-comments@nist.gov

Author(s)

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

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

NIST Standardized Signatures



NIST COMPUTER SECURITY RESOURCE CENTER CSRC

NIST Standardized Signatures

- state-of-the-art threshold RSA is from 2006 [ADN06]
    - achieves adaptive security
- 1 round if all parties are honest (otherwise constant-round)

NIST Standardized Signatures

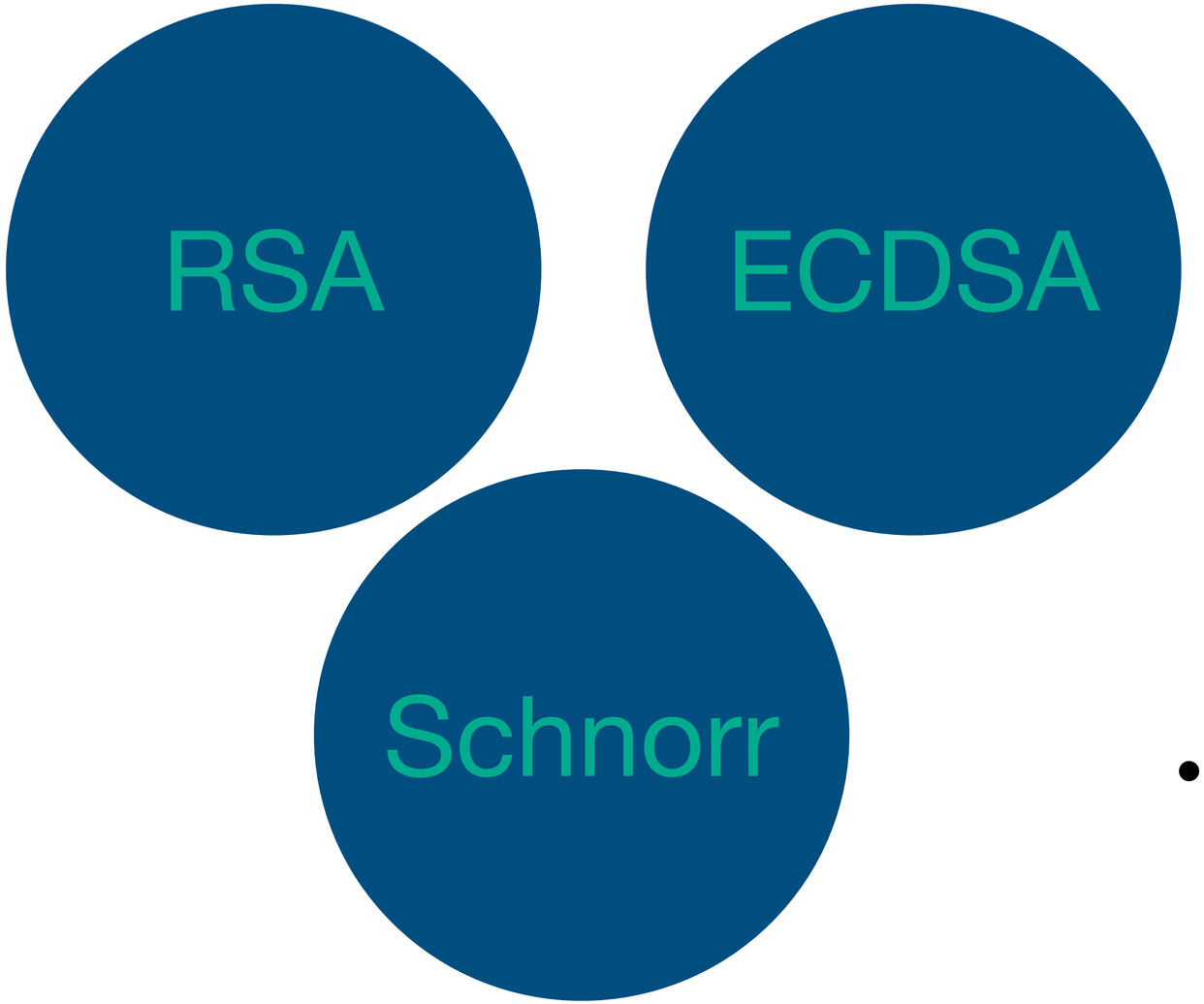
- threshold ECDSA is complex
- [GennaroG19} relies on the security of ECDSA, the Strong RSA assumption, DDH, and the security of a non-malleable equivocable commitment scheme
- [CanettiGGMP20} relies on the security of ECDSA, the Strong RSA assumption, DDH, the semantic security of Paillier encryption, and the global random oracle model (GROM)

NIST Standardized Signatures

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

- all the schemes you have seen today
- security relies on the discrete logarithm (DL) or one-more discrete logarithm (OMDL) problem in the random oracle model (ROM)

NIST Standardized Signatures



Honourable Mention

- threshold (blind) BLS in 1 round

NIST FROST Submission Team

Elizabeth Crites

Conrado Gouvea

Ian Goldberg

Jack Grigg

Jonathan Katz

Chelsea Komlo

Mary Maller

Stefano Tessaro

Nikita Sorokovikov

Denis Varlakov

Chenzhi Zhu

Takeaways

- Multi-party Schnorr signatures are being used in practice today
- Many challenges remain to improve usability and security
- Come talk to me if you are using these schemes or are interested in collaborating or learning more

Thank you!