Serai DEX - FROST

An Overview of Serai’s work with FROST

Overview of Serai DEX

- Decentralized, autonomous exchange premised on threshold multisig
- Large signing sets (up to 150 signers in a multisig)
- Adversarial environment

PedPoP with Identifiable Aborts

- PedPoP from the FROST paper
- Shares are encrypted with the result of the Diffie-Hellman of a per-message point and a per-participant point
- Does not attempt to handle authentication/communication/consensus

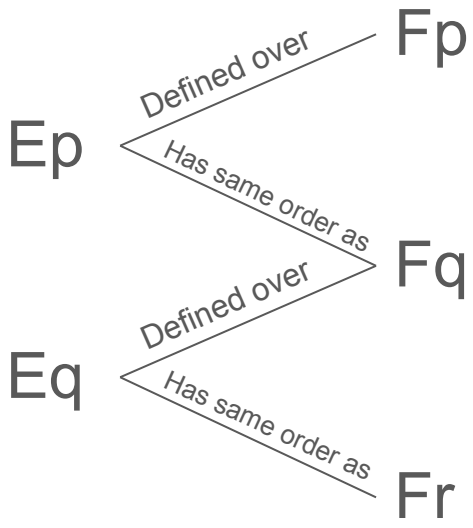
DKG-576

- Novel one-round DKG
- Solely relies on the hardness of the EC DDH problem (proofs pending)
- Does not require consensus on any context/messages
- Achieves identification of faulty participants with consensus on context
- Unbiased if `n`-of-`n`
- Can be done robustly by just `t`-of-`n` (requires agreement on which `t` participated and sacrifices being unbiased)

eVRFs

- https://eprint.iacr.org/2024/397
- Exponent Verifiable Random Functions
- Generates a verifiably random value and a commitment to it
- Posited a one-round DKG
- DDH-variant premised on a tower of elliptic curves

Tower of Elliptic Curves



Points on Eq can be efficiently worked with inside proofs on Ep!

DDH-premised eVRF

- Proves a pair of DHs on Eq within a Bulletproof over Ep, the random value being the sum of their x-coordinates
- Proving a DH is only 7 rows in the resulting inner-product proof thanks to the usage of elliptic curve divisors
- Divisor technique proven and reviewed, while the divisor-based proof of scalar multiplication (and associated R1CS) is actively being proven

eVRF DKG

- Defines the coefficients as the results of eVRFs
- Only one possible polynomial for a key/context

eVRF PVSS (My Contribution)

- Encrypts secret shares by adding the x-coordinates of the results of a pair of DHs
- Proves for a commitment to the summed DHs' x-coordinates using the same techniques as eVRFs

FROST

- Implemented the IETF specification
- Modular to the challenge function
- Modular to the signing protocol itself
- Supports signing with offset keys
- Did not implement with public verification

Achieving Robustness

- Serai uses a bespoke Tendermint blockchain to authenticate and obtain consensus on messages
- This is also used for blame/scheduling re-attempts
- `O(n**2)` is too expensive to be regularly run
- Personally interested in robust `O(n)` protocols premised on Class Groups/LWE

Status

- **`dkg`** crate with PedPoP audited in March, 2023
- DKG-576 implemented yet will be unaudited until proven
- **`modular-frost`** crate also audited in March, 2023
- **`modular-frost`** applied to Bitcoin (BIP-340), Ethereum (via a smart contract), and Monero (CLSAG)
- **`bitcoin-serai`** offers a high-level API for sending Bitcoin transactions from a threshold multisig
- **`bitcoin-serai`** was audited in August, 2023
- **`bitcoin-serai`** is integrated into Stack Wallet to offer FROST-based Bitcoin wallets
- Would support a BIP for FROST and would likely move to one if finalized

Questions?