FROSTR

Simple t-of-n remote signing and key rotation, using the powers of FROST.

Problems with on-chain Multi-Sig

If a key is compromised, you have to move funds to a new address.

If funds are spent, all keys must be published on-chain.

You have to pay the cost for storing this data on-chain.

Benefits of FROST on Bitcoin

No data about the multi-sig is shared on-chain.

Moving the funds on-chain requires a single (FROST) signature.

Updating your keys does not change the on-chain address.

No need to move your funds when updating your keys.

Benefits of FROST on Nostr.

- You can break up your secret key into distributable shares.
- If one share is compromised, your secret key is still safe.
- You can discard and replace shares without changing your identity.

Architecture

Bifrost : FROST cryptography library.

Igloo : Remote signing server and key-set manager.

Frost2x : Browser signing extension (forked from nos2x).

How it Works

Website makes a request to the user's signer (web-extension).

Signer partially signs the note, then sends it to the remote server.

Server verifies the partial signature, then returns a complete signature.

Signer delivers the signed note to the website.

How to Setup

Use Igloo to generate a new set of FROST shares.

Choose a key-share to input into the remote signer.

Copy/paste a second key-share into your signing device.

Store the third key-share as a recovery key.

How to Rotate

Collect 2/3 key-shares together.

Drag & drop the key-shares into Igloo.

Click "rotate" to produce a set of new shares.

Update each device (and recovery) with the new shares.

What works

FROST library is complete, with unit tests and E2E tests.

Igloo generates shares and runs a remote signing server.

Frost2x extension signs via FROST and makes requests to remote server.

Remote server verifies, co-signs and returns a response.

What is Unfinished

Signing process needs to be debugged (invalid signatures).

Key rotation needs to be implemented in igloo.

Other signing methods need to be added (PSBT, ECDH, etc.)

Closing

The nostr key rotation problem needs a solution.

FROST is the best solution on the market.

Let's make nostr and self-custody great again!