FROST Implementation for Bitcoin in secp256k1-zkp

Project Updates

Presenter: Jesse Posner

Event: FROST Implementers Round Table

Date: 9/18/24

Proactive and Dynamic Secret Sharing

Diffie-Hellman Key Exchange with FROST

- Noted as possible in **BIP352 (Silent Payments)**.
- **Implemented here:** github.com/jesseposner/FROST-BIP340.

Diffie-Hellman Key Exchange with FROST

- **FROST Group Private Key:** (x)
- **FROST Key Share:** (s_i)
- **Lagrange Coefficient:** (λ_i)

Computations

- **Counterparty Public Key:** (P)
- **Shared Secret:** (P^x)
- **Partial Shared Secret:** $(P^{s_i \lambda_i})$

Shared Secret Derivation

$$\begin{aligned}\prod_{i=1}^{t} P^{s_i \lambda_i} &= P^{\sum_{i=1}^{t} s_i \lambda_i} \\ &= P^{x}\end{aligned}$$

Unsafe to Use Raw DKG Output Directly On-Chain

- Unlike **MuSig2**, the FROST group public key is **not randomized**.
- A malicious party could add an **undetectable script path** to their polynomial during the DKG.
- Thus, an **unspendable script path should be added** as suggested by **BIP341**.
- It's better not to output an **x-only public key** from the DKG.
- The x-only negation logic should **not be handled in the DKG**.
- **Issue raised here:** github.com/BlockstreamResearch/bip-frost-dkg/issues/41

Next Steps for secp256k1-zkp Implementation

- Pull Request #278
- Pushed significant changes to the **trusted dealer PR** that incorporated feedback and recent improvements to the **MuSig2 implementation** (review welcome!).
- Implements the signing BIP: github.com/siv2r/bip-frost-signing
- **DKG code** will be additive and limited to key generation only.
- It will be in a separate PR following the merging of the trusted dealer PR.
- Based on the DKG BIP: github.com/BlockstreamResearch/bip-frost-dkg

Thank You!

Questions?