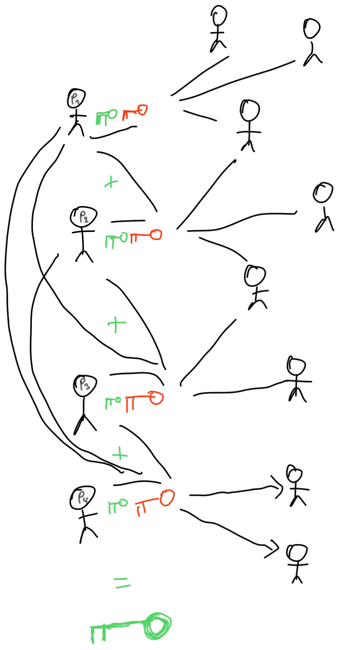
Federated DKG

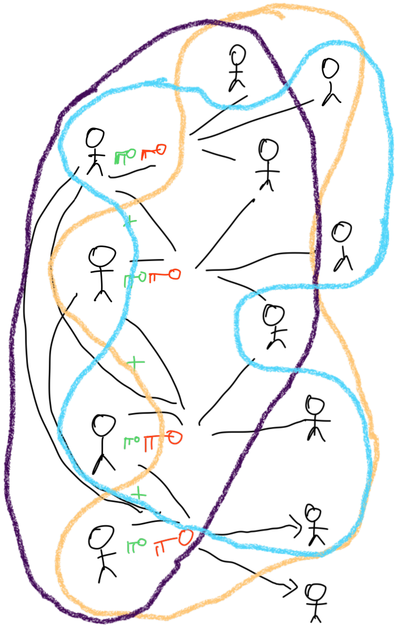


Each party:

- Generates key pair 🔑.
- Split secret key 🔑 among trusted parties and previous participants. Each share is encrypted and published on chain.
- Publish public key 🔑.

Encryption key 🔑 is the sum of all 🔑 keys.

Decryption



Any subset of t parties for each share have to provide its shares to decrypt the result.

Examples ○, ○, ○