Fast Secure Multiparty ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody

- Full Version: https://eprint.iacr.org/2018/987

Motivation

- Threshold cryptography
  - used in applications where muiltiple signers are needed to generate a signature
  - used to provide a high level of key protection
- ECDSA signing is used in Bitcoin and other cryptocurrencies
  - the theft of a signing key can be translated into concrete financial loss
- Bitcoin uses a multisignature solution
  - the flexibility of Bitcoin multisig is limited
    - not supporting arbitary and complex access structures
  - plain multisig solutions introduce anonymity and scalability problems
  - do not support revoking a party's share

Contribution

- present the *first truly practical* full threshold ECDSA signing protocol that has pratical distributed key generation and fast signing
- securely computing ECDSA in a distributed manner

Technical Contribution

- replacing the Paillier additively homomorphic encryption with ElGamal in-the-exponent
  - distributed key generation is very easy
  - Elliptic curve operations are more efficient than Paillier operations
  - zero-knowledge proofs are more efficient in the Elliptic curve group
    - zero-knowledge is easier in known-order groups