Compact Multi-Signatures for Smaller Blockchains

- Full Version: https://eprint.iacr.org/2018/483

Motivation

- A muilti-signature scheme enables to n signers to jointly generate a shorty signature σ on m.
  - Each party *independently* generates a key pair for a signature scheme
- σ convinces a verifier that all n parties signed m
- it can be used to shrink the size of the Bitcoin blockchain.

Contribution

1. construct new multi-signature schemes that provide *new* functionality
   - design to reduce the size of the Bitcoin blockchain
   - the verifier only needs a short multi-signature, a short aggregation of their public keys, and the message m to verify a signature
2. construct the first short accountable-subgroup multi-signature (ASM) scheme
   - enables any subset S of a set of n parties to sign a message m
   - a valid signature discloses which subset generated the signature