Group Signature by David Chaum's 4th Proposal

- KeyGen(1^λ, n); choose a prime p and $g \xleftarrow{\$} \mathbb{Z}_p^*$.

  Each member chooses $s_i \xleftarrow{\$} \mathbb{Z}_{p-1}$ and computes $y_i \equiv g^{s_i} \bmod p$.

  Output $pk = (p, g, \{y_i\})$ and $sk_i = (s_i)$ for all $1 \le i \le n$.

- Sign(m, pk, s_s); compute $\sigma \equiv m^{s_s} \bmod p$

  output (m, σ)

σ is a valid signature of m iff $\sigma \equiv m^{s_s} \bmod p$ and $g^{s_s} \in \{y_i\}$.

To prove this statement without leaking s_i, ZKP is used.

Privacy Problem in BTC

i) anonymity : hiding identities of sender and receiver → by ring signature

ii) confidentially : hiding the amount transferred.

↳ by confidential transaction : every transaction amount is hidden using a commitment to the amount.

to prove: i) the sum of inputs is greater than the sum of outputs.
ii) all transactions values are positive.) range proof.

Current Proposals for CT ZKP

- [PBF+] : large proof size or required a trusted setup.
- SNARKs : required a trusted setup.
- STARKs : range proof size is large

→ [BBB+18] Bulletproof @ S&P'18.

Think thing