Bulletproofs: Short Proofs for Confidential Transactions and More

Problem Statement

- Privacy Problem in Bitcoin
  - anonymity: hiding identities of sender and receiver
  - confidentially: hiding the amout transferred
    - using Confidential Transaction (CT)
      - every transaction amount is hidden using a commitment to the amount
- Confidential Transaction needs range proofs
  - the sum of inputs is greater than the sum of outputs
  - all transaction values are positive
- Current Proposal for CT ZKP
  - [PBF+]: large proof size or required a trusted setup
  - SNARK: requires a trusted setup
  - STARK: the proof size of range proofs is large

Contribution

- construct new NIZK with very shrot proofs without a trusted setup
  - only logarithm in the witness size
- well-suited for efficient range proofs
  - committed value is in a range using only $2\log n + 9$ group and finite elements
  - n: bit length of range
- improve on the linear sized range proofs
- support aggregation of range proofs
  - m commitments lie in a given range in a single proof
- provide short zero-knowledge proofs for general circuits relying on DL without requiring a trusted setup