Non-Interactive Zero-Knowledge Proofs for Composite Statements

- Full Version: https://eprint.iacr.org/2018/557

Problem Statement

- proving the balance in Bitcoin is enough to exchange requires
    1. signature computation
    2. hash function evalutaion
- How to fuse two primitive such that performing faster than Σ-protocol based approach or SNARK based approch?

Contribution

- A new NIZK (non-interactive zero-knowledge) proof of knowledge of x_1, x_2, x, y_1, y_2 s.t.
    1. $f_1(x_1, f_2(x_2)) = z$
    2. $f_1(x, y_1) = z_1 \wedge f_2(x, y_2) = z_2$
    3. $f_1(x, y_1) = z_1 \vee f_2(x, y_2) = z_2$, where z, z_1, z_2 are public

by constructing

1. Σ-protocols for
    - proof of addition of two points
    - proof of double-discrete logs
    - proof of equliaty over different gorups
2. SNARKS to efficient handle commitments from Σ-protocols