Decentralized Evaluation of Quadratic Polynomials on Encrypted Data

- Full Version: https://eprint.iacr.org/2018/1019

Problem Statements

- 2-DNF formulae evaluation is enough, but efficient multiparty decryption is still required to guarantee privacy
- BGN proposed an additive homomorphic encryption scheme supporting one multiplication by using a bilinear map on a composite-order group
  - computation on such elliptic curves turned out to be quite inefficient
- Freeman proposed a generalization, based on prime-order groups
  - better efficiency

Contributions

- show how the Freeman cryptosystem can handle multiple users with one general setup
  - users' key are efficient to generate
  - support efficient multiparty decryption without a trusted server
    - fully decentralized setting

Applications

- Private Information Retrieval (PIR)
- Electronic Voting Protocols
- Group Testing on Encrypted Data
  - an efficient technique to detect positive samples with fewer tests in the case the proportion of positive cases is small
- Machine Learning on Encrypted Data