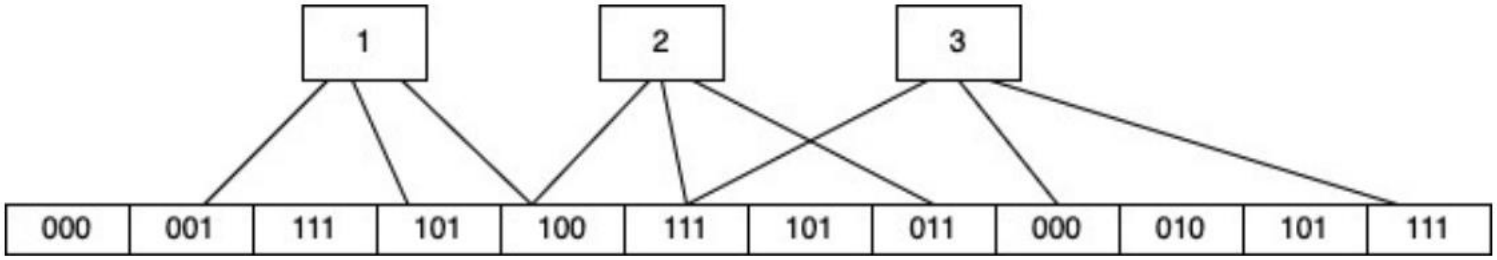
EMPSI: Efficient Multiparty Private Set Intersection (with Cardinality)

Yunbo YANG, Xiaolei DONG, Zhenfu CAO, Jiachen SHEN, Ruofan LI, Yihao YANG, Shangmin DOU

Frontiers of Computer Science, DOI: 10.1007/s11704-022-2269-0

Problems & Ideas

- Problems of existing private set intersection scheme:
  - Most existing private set intersection schemes focus on two-party settings and are computationally expensive.
- Ideas: This paper first proposes a new variant of Bloom filter called Zero-sharing Garbled Bloom Filter (ZGBF), then apply this new Bloom filter to construct an efficient MPSI protocol. In addition, EMPSI also uses OPRF protocol to disturb each parties'input in order to make EMPSI convert more functionalities such as PSI with cardinality.

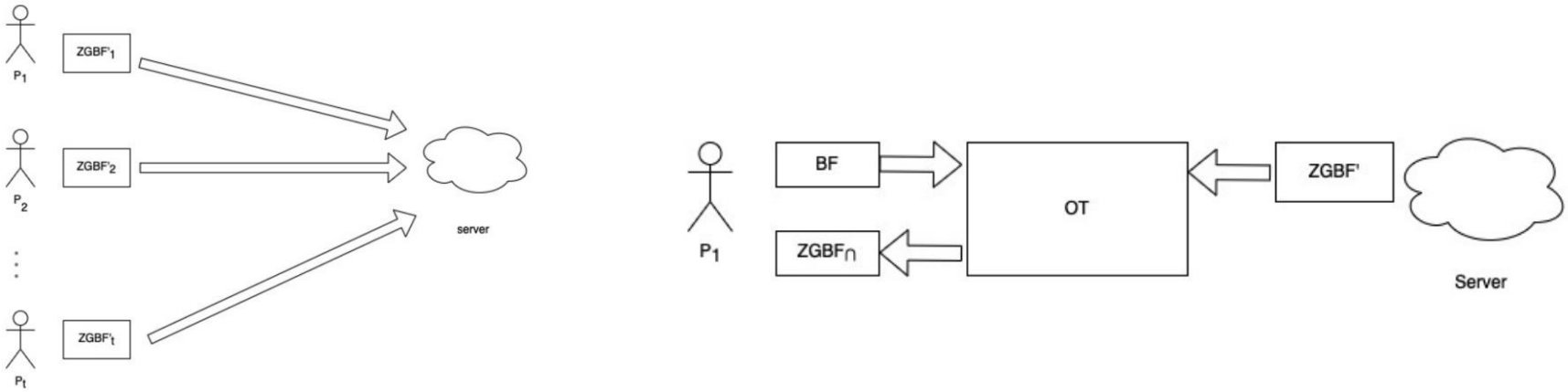


Toy example for ZGBF

Main Contributions

- Conclusions:
- 1. Garbled Bloom filter (GBF) can be combined with zero-sharings to achieve wider range of applications.

- 2.EMPSI is efficient compared to other state-of-the-art works as it mainly bases on symmetric-key encryption and also supports PSI with cardinality operation.



EMPSI(-CA) system model