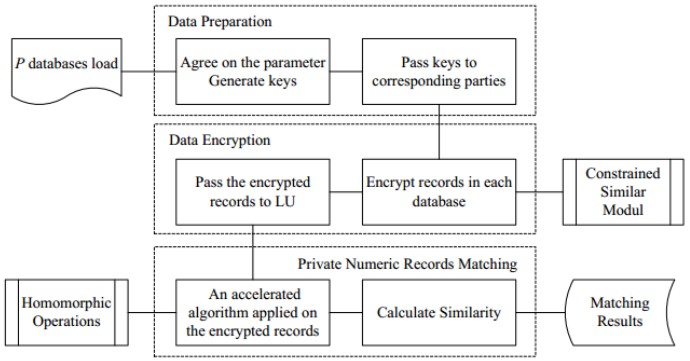
Efficient private multi-party numerical records matching

Shumin HAN, Derong SHEN, Tiezheng NIE, Yue KOU, Ge YU

Frontiers of Computer Science, DOI: 10.1007/s11704-019-9063-7

Problems & Ideas

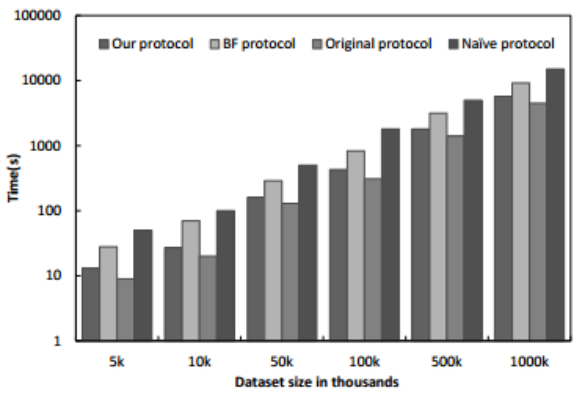
- Problems of private records matching
  - Some methods are limited to linking data from two sources
  - It is an urgent gap when it comes to private linking numerical data
- Ideas: a method designed for linking numerical records from multiple sources in an efficient and secure way
  - A homomorphic encryption method constrained similar modul is introduced to encrypt numerical data in the range of real numbers
  - We propose an accelerated algorithm to reduce the complexity of calculating the similarity among multiple numerical records
  - We draw an inference about the encryption keys to avoid frequent decryptions in multi-party matching protocol

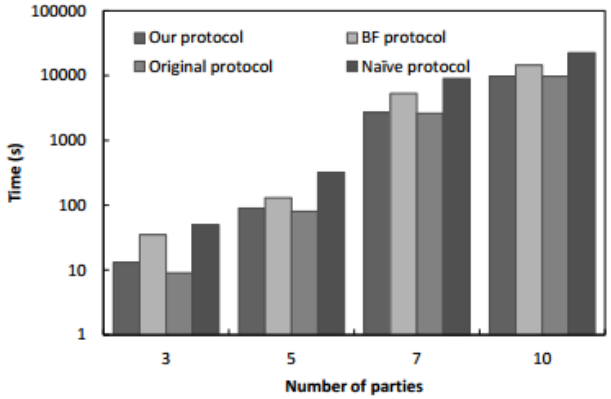


The framework of our method

Main Contributions

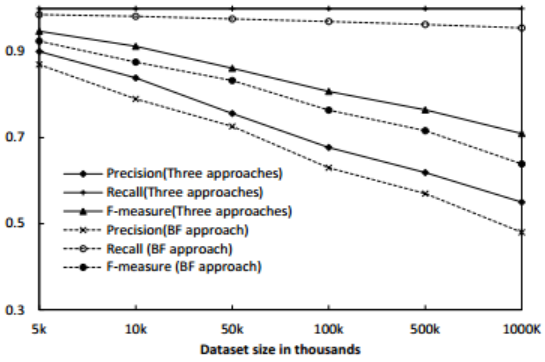
- **Our method has an improvement in efficiency**

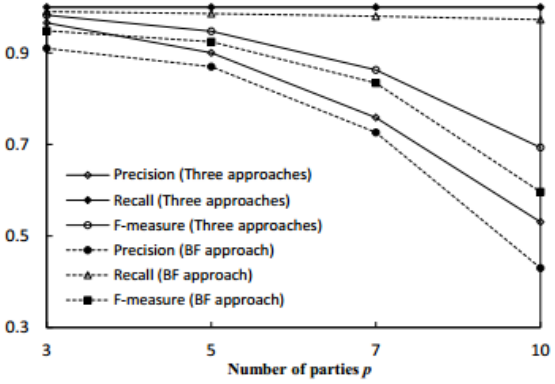




Runtime with different database sizes and number of parties

- **The linkage quality of our method is higher than previous methods**





Matching quality with different database sizes and number of parties