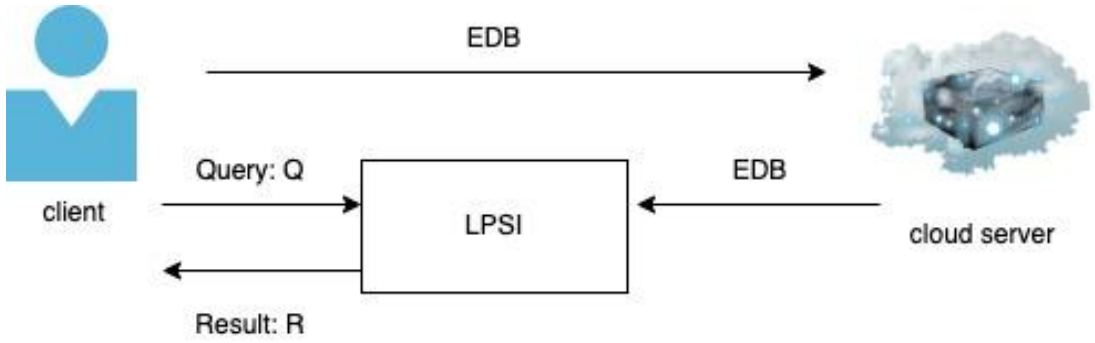
IXT: Improved Searchable Encryption for Multi-word Queries Based on PSI

Yunbo YANG, Xiaolei DONG, Zhenfu CAO, Jiachen SHEN, Shangmin DOU

Frontiers of Computer Science, DOI: 10.1007/s11704-022-2236-9

Problems & Ideas

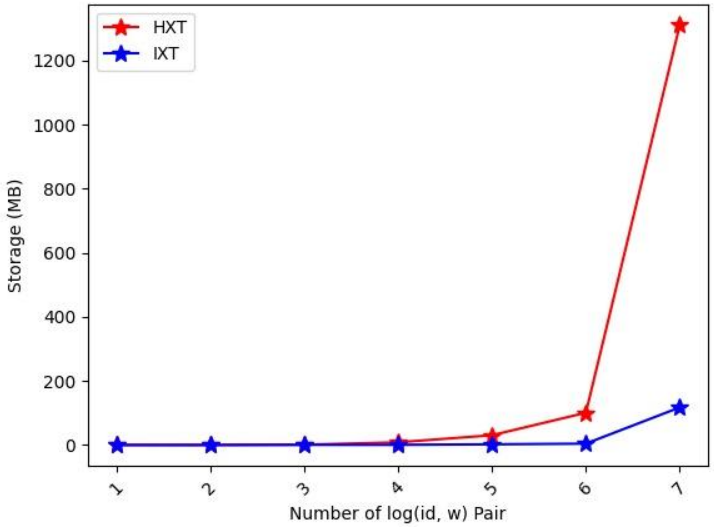
- Problems of existing searchable encryption scheme:
  - Most existing searchable encryption schemes leak search pattern or access pattern to achieve better performance.
  - Most existing searchable encryption schemes do not support various types of search queries (e.g. multi-word query, disjunctive query).
- Ideas: Private set intersection (PSI) can be used to protect both parties' privacy while retaining efficiency. It can combined with searchable encryption to have stronger security while retaining efficiency.



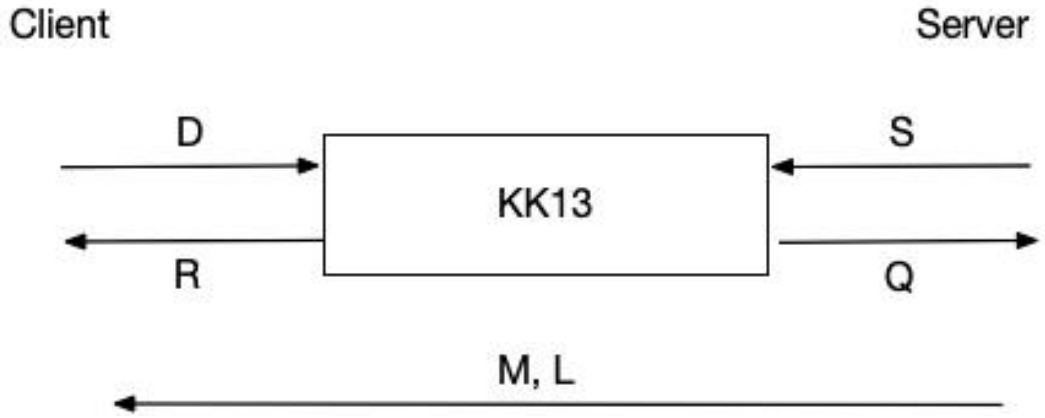
Architecture of IXT

Main Contributions

- Conclusions:
- 1. IXT provides stronger security guarantee compared with existing state-of-the-art searchable encryption (SE) while retaining efficiency in single-reader single-writer framework.
- 2. IXT supports both conjunctive query and disjunctive query.
- 3. IXT has lower storage overhead, low computation overhead at client side and fewer interaction rounds between client and server compared with most state-of-the-art SE schemes.



Storage overhead comparison between IXT and HXT



Interaction between client and server