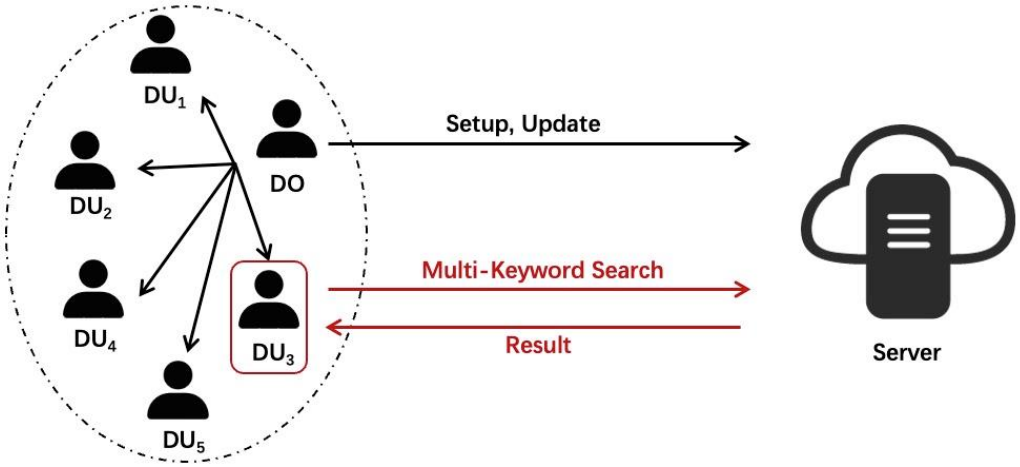
MMKFB: Multi-client and Multi-keyword Searchable Symmetric Encryption with Forward and Backward Privacy

Panyu WU, Jiachen SHEN, Zhenfu CAO, Xiaolei DONG

Frontiers of Computer Science, DOI: 10.1007/s11704-024-3390-z

Problems & Ideas

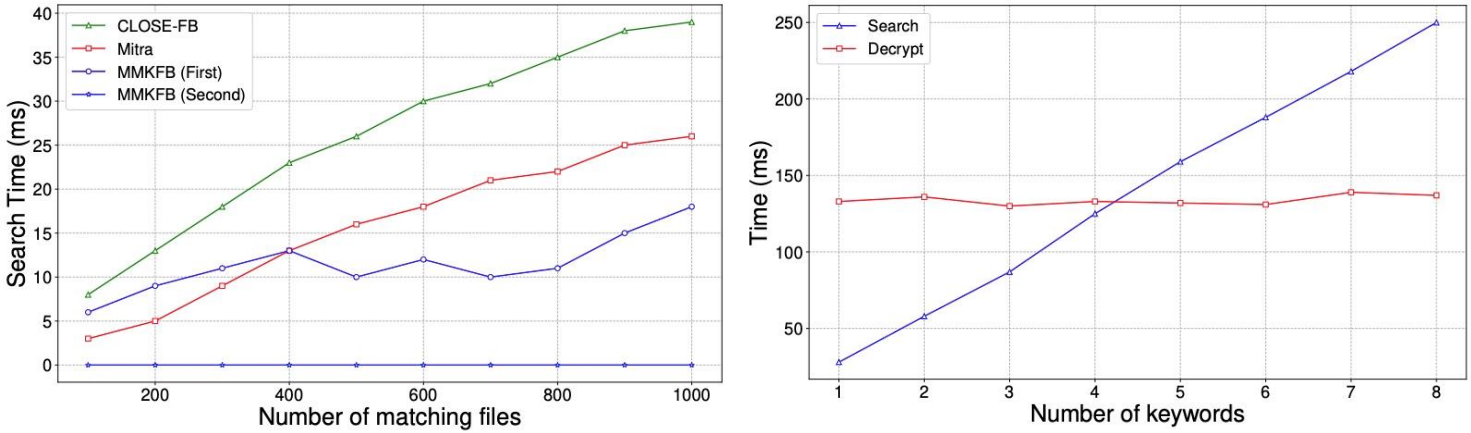
- Problems of conventional Dynamic Searchable Symmetric Encryption:
  - Existing data leakage issues that fail to meet forward and backward security guarantees.
  - The need for multi-client setting and rich search expressions in real-life situations is not satisfied.
- Ideas: Further consideration of multi-keyword search scheme under multi-client setting based on satisfying backward and forward security.



Multi-client are divided into single data owner and multiple data user forms based on their functions, and data users do not need to rely on the data owner to perform searches. This multi-client model is also combined with multi-keyword search to design an efficient scheme.

Main Contributions

- Contributions:
  - We design a DSSE scheme with forward security and backward security that supports multi-client. The clients are divided into a data owner and multiple data users. And data users can complete the multi-keyword search without the help of the data owner;
  - We propose a new form of multi-keyword search which implements threshold queries, i.e., obtaining file identifiers that satisfy the match greater than or equal to the threshold;
  - We prove the security of the proposed scheme and conduct simulation experiments, which proves that the scheme has good efficiency in both update and search processes.



The left figure compares the search efficiency of this paper ‘s scheme with other schemes. The right graph shows the change in search and decryption time as the number of keywords grows. If multithreading is used, the change in search time will be slower.