Multi-Source Multi-Client Searchable Symmetric Encryption with Post-Compromise Security

Yue GE, Ying GAO, Yunhao LING, Jianxin GAO

Frontiers of Computer Science, DOI: 10.1007/s11704-025-50782-6

Problems & Ideas

- Problems of Multi-Source Multi-Client Searchable Symmetric Encryption with Post-Compromise Security :
  - If the secret keys of participants in the Multi-Source Multi-Client Dynamic Searchable Symmetric Encryption (MM-DSSE) system are compromised, can the data of data sources and the query privacy of clients remain secure?
- Ideas: This work models the key compromise risks of MM-DSSE and leverages set-constrained pseudorandom functions and a two-layer encryption strategy to construct a key-updatable MM-DSSE framework.

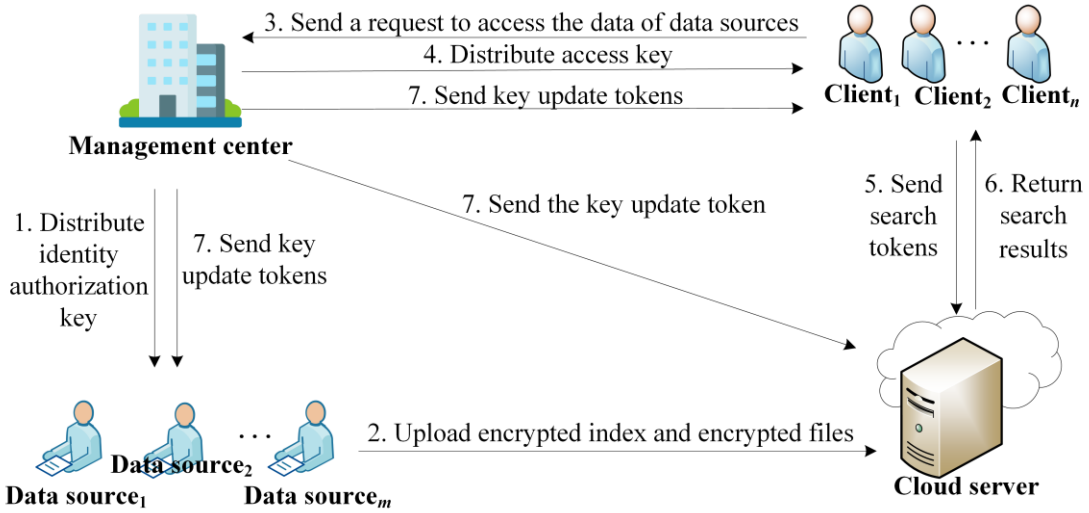

Fig.1 System Framework of Key-Updatable MM-DSSE

Main Contributions

- Contributions:
  - formalize the post-compromise security notion of MM-DSSE using leakage functions. This security definition is compatible with forward and backward privacy.
  - This work proposes a post-compromise secure MM-DSSE framework, Mosaic, which achieves sublinear search complexity and is further extended to support fine-grained range search.
  - Mosaic outperforms the state-of-the-art post-compromise secure DSSE scheme Bamboo, achieving 79.21% higher search efficiency and 33.71% lower key update time in a LAN.

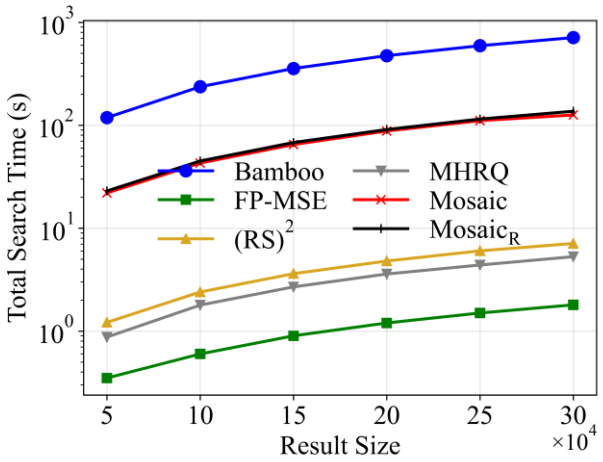

Fig. 2 Search Time Evaluation

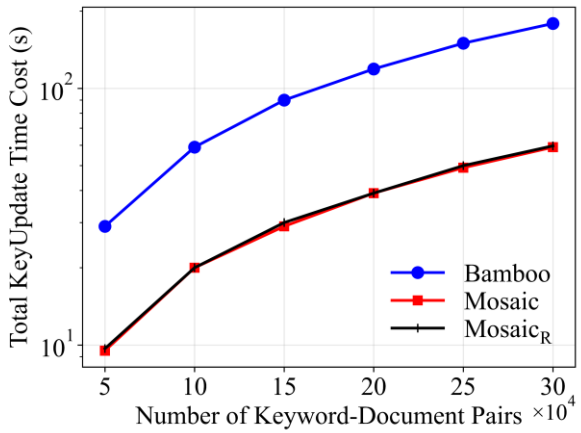

Fig. 3 KeyUpdate Cost