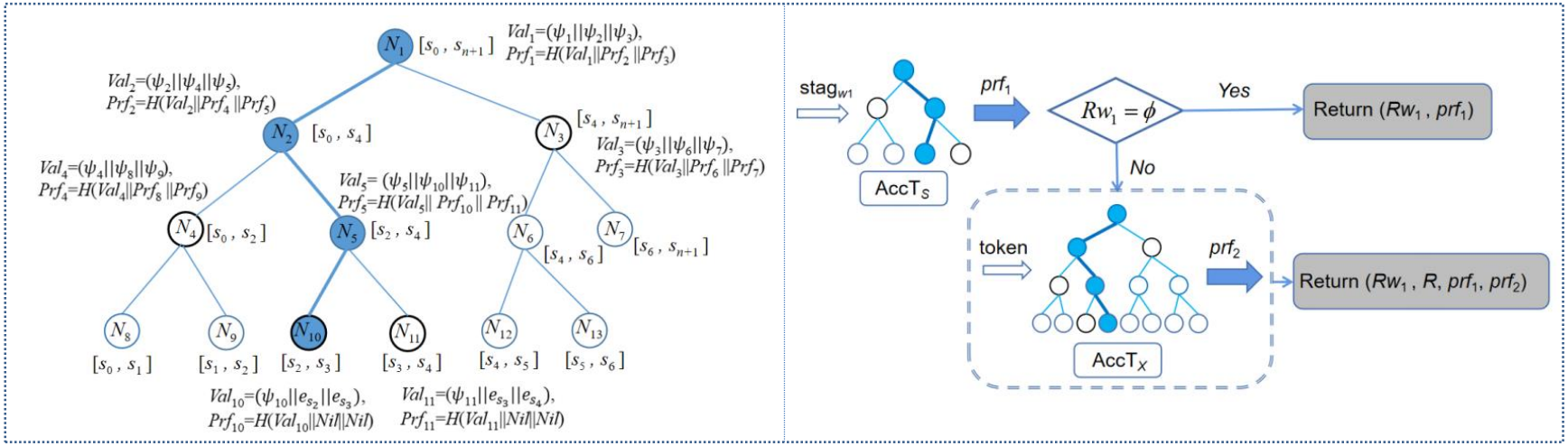
Verifiable Searchable Symmetric Encryption for Conjunctive Keyword Queries in Cloud Storage

Qingqing GAN, Joseph K. LIU, Xiaoming WANG, Xingliang YUAN, Shi-Feng SUN, Daxin HUANG, Cong ZUO, Jianfeng WANG

Frontiers of Computer Science, DOI: 10.1007/s11704-021-0601-8

Problems & Ideas

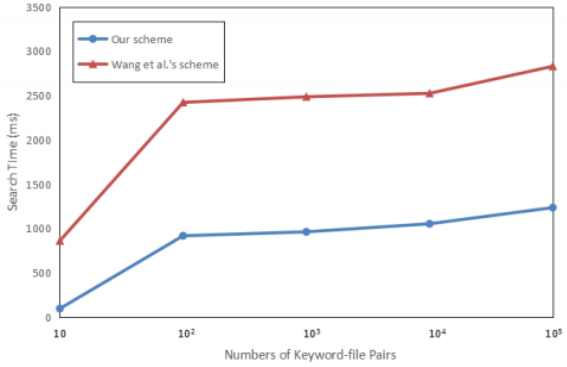
- Problems of Verifiable Searchable Symmetric Encryption (VSSE) approaches:
  - Existing VSSE approaches cannot provide a proof for the empty search result or only focus on the single-keyword search;
  - VSSE schemes supporting conjunctive keyword queries bring security issues or incur heavy computational cost on the verifier.
- Ideas: To present a secure and efficient VSSE scheme for conjunctive keyword queries, based on a privacy-preserving hash-based accumulator and the OXT protocol.



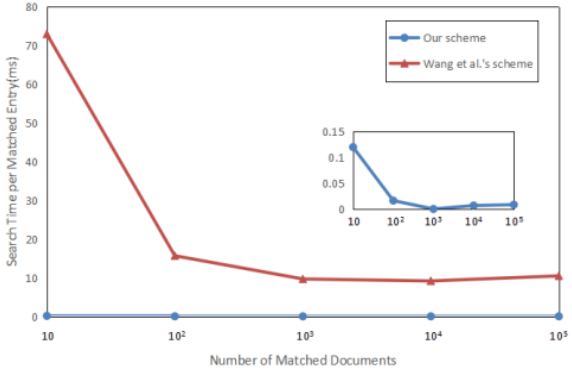
Left: Accumulator tree model; Right: Overview of the proof generation procedure.

Main Contributions

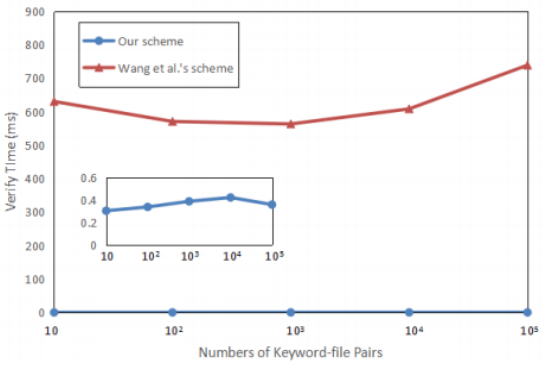
- Contributions:
  - A privacy-preserving hash-based accumulator is designed by using Symmetric Hidden Vector Encryption (SHVE);
  - By applying the new-designed hash-based accumulator to the OXT protocol, a novel VSSE scheme is built to support conjunctive keyword queries, achieving correctness and completeness verification for the search result, even if the search result is empty;
  - A formal security proof is provided to show that the proposed VSSE scheme meet semantically security. And an experimental evaluation is conducted to demonstrate the efficiency of the proposed scheme.



(a) Time cost of `Search` with real-world data.



(b) Time cost of `Search` with synthetic data.



(c) Time cost of `Verify` algorithm.

The performance comparison with related works.