Cryptology ePrint Archive: Report 2013/169

Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries

David Cash and Stanislaw Jarecki and Charanjit Jutla and Hugo Krawczyk and Marcel Rosu and Michael Steiner

Abstract: This work presents the design, analysis and implementation of the first sub-linear searchable symmetric encryption (SSE) protocol that supports conjunctive search and general Boolean queries on symmetrically-encrypted data and that scales to very large data sets and arbitrarily-structured data including free text search. To date, work in this area has focused mainly on single-keyword search. For the case of conjunctive search, prior SSE constructions required work linear in the total number of documents in the database and provided good privacy only for structured attribute-value data, rendering these solutions too slow and inflexible for large practical databases.

In contrast, our solution provides a realistic and practical trade-off between performance and privacy by efficiently supporting very large databases at the cost of moderate and well-defined leakage to the outsourced server (leakage is in the form of data access patterns, never as direct exposure of plaintext data or searched values). A key aspect of our protocols is that it allows the searcher to pivot its conjunctive search on the estimated least frequent keyword in the conjunction. We show that a Decisional Diffie-Hellman (DDH) based pseudo-random function can be used not just to implement search tokens but also to hide query access pattern of non-pivot, and hence possibly highly frequent, keywords in conjunctive queries. We present a formal cryptographic analysis of the privacy and security of our protocols and establish precise upper bounds on the allowed leakage.

To demonstrate the real-world practicality of our approach, we provide performance results of a prototype applied to several large representative data sets.

Category / Keywords: cryptographic protocols / Encrypted search, privacy,implementation

Publication Info: To be published: Crypto'2013.

Date: received 28 Mar 2013, last revised 22 May 2013

Contact author: hugo at ee technion ac il