Cryptology ePrint Archive: Report 2013/163

Search Pattern Leakage in Searchable Encryption: Attacks and New Constructions

Chang Liu and Liehuang Zhu and Mingzhong Wang and Yu-an Tan

Abstract: Searching on remote encrypted data (commonly known as \textit{searchable encryption}) is becoming an important technique in secure data outsourcing, since it allows users to outsource encrypted data to the third party and maintains the keyword searching on the data at the same time.

It has been widely accepted in the literature that searchable encryption techniques should leak as little information as possible to the third party. An early classical method called oblivious RAM hides all information at the cost of poly-logarithmic computation and communication overheads, which turns out to be impractical in the real world applications (e.g., cloud computing). A number of efficient searchable encryption schemes have been proposed under weaker security guarantees afterwards, however, such schemes leak statistical information about the user's search pattern.

In this paper, we show that the search pattern leakage can result in non-trivial risks. As pioneer work, we present two concrete attack models exploiting user's search pattern and some auxiliary background knowledge aiming to disclose the underlying keywords of user's queries. To resist these attacks, we develop two new searchable encryption constructions that hide the search pattern. Our constructions are designed to be independent from the underlying searchable encryption scheme. Our experiments, which are based on the real world dataset, demonstrate the effectiveness and efficiency of proposed attack models and new constructions.

Category / Keywords: secret-key cryptography / search pattern, searchable encryption, index, fake query

Date: received 21 Mar 2013

Contact author: changliu bit at gmail com

Available formats: PDF | BibTeX Citation

Version: 20130326:135610 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]