Cryptology ePrint Archive: Report 2011/190

SHS: Secure Hybrid Search by Combining Dynamic and Static Indexes in PEKS

Peng Xu and Hai Jin

Abstract: With a significant advance in ciphertext searchability, Public-key encryption with keyword search (PEKS) is the first keyword searchable encryption scheme based on the probabilistic encryption, such that it is more secure than almost all previous schemes. However, there is an open problem in PEKS that its search complexity is linear with the sum of ciphertexts, such that it is inefficient for a mass of ciphertexts. Fortunately, we find an elegant method that by adaptively taking the keyword trapdoor of each query as an index, the search complexity of the queried keywords can be decreased in a huge degree. We call this method dynamic index (DI) technique. Furthermore, for keywords having not been queried before, we employ deterministic encryption to establish indexes to decrease their first search complexity. We call this method static index (SI) technique. Consequently, we propose a secure hybrid search (SHS) system by combing DI and SI techniques in PEKS to decrease the search complexity of PEKS. At last, we demonstrate its semantic security and convergent search complexity, which is considerably lower than that of PEKS.

Category / Keywords: public-key cryptography / public-key encryption with keyword search, dynamic index technique, static index technique, secure hybrid search

Date: received 13 Apr 2011

Contact author: xupeng at mail hust edu cn