انجمن رمز ایران
Iranian Society of Cryptology

Public key encryption with keyword search and keyword guessing attack

Searchable encryption is a special case of functional encryption which enables a user to perform secure searches over encrypted data stored on an untrusted server. Searchable encryption techniques can be divided into two main categories: searchable symmetric encryption (SSE) and public key encryption with keyword search (PEKS). Unlike the SSE techniques, PEKS methods are vulnerable to keyword guessing attack. In keyword guessing attack, by accessing a trapdoor, an adversary can generate the searchable ciphertexts corresponding to all possible keywords and check for a match. In this way, the adversary can determine the searched keyword and the files containing it. The feasibility of the attack comes from the fact that the number of possible keywords are limited in practice. In this paper, after reviewing the concept of searchable encryption, the description of keyword guessing attack and vulnerability of some of the PKES schemes to such attacks is provided. Then, the paper proceed by giving an overall picture of the attempts made to overcome this drawback. Finally, open problems and future work directions in this area is addressed.