Abstract

The Public Key Encryption along with Keyword Search allows one to search the data that is in encrypted form with a keyword without showing any information. This paper gives the detail study on searchable Public-Key Ciphertexts with Hidden Structures (SPCHS) that fasten the keyword search without sacrificing the security of encrypted keywords. In SPCHS, the keyword ciphertexts is structured by hidden relation and by using a trapdoor function used in cryptography to keywords to disclose minimum information to search algorithm. In SPCHS Schema, cipher texts have hidden star like structure. The SPCHS construction is based on IBKEM i.e. Identity Based Keyword Encapsulation Management that splits the computation in
two parts first that perform heavy computation and other cipher text produced by light computation. The generic SPCHS construction is built with IBE i.e. Identity Based Encryption and Collision-free full-identity malleability IBKEM.

References


Index Terms
Keywords
Public-key Searchable Encryption  Semantic Security  Identity-based Key
Encapsulation Mechanism
Identity Based Encryption.