

**Flexible Wildcard Searchable Encryption System**

**Abstract:**

Searchable encryption is an important technique for public cloud storage service to provide user data confidentiality protection and at the same time allow users performing keyword search over their encrypted data. Previous schemes only deal with exact or fuzzy keyword search to correct some spelling errors. In this paper, we propose a new wildcard searchable encryption system to support wildcard keyword queries which has several highly desirable features. First, our system allows multiple keywords search in which any queried keyword may contain zero, one or two wildcards, and a wildcard may appear in any position of a keyword and represent any number of symbols. Second, it supports simultaneous search on multiple data owner’s data using only one trapdoor. Third, it provides flexible user authorization and revocation to effectively manage search and decryption privileges. Fourth, it is constructed based on homomorphic encryption rather than Bloom filter and hence completely eliminates the false probability caused by Bloom filter. Finally, it achieves a high level of privacy protection since matching results are unknown to the cloud server in the test phase. The proposed system is thoroughly analyzed and is proved secure. Extensive experimental results indicate that our system is efficient compared with other existing wildcard searchable encryption schemes in the public key setting.