Cryptology ePrint Archive: Report 2011/409

Efficient Predicate Encryption Supporting Construction of Fine-Grained Searchable Encryption

Xiaoyuan Yang, Weiyi Cai, Xu An Wang

Abstract: Predicate Encryption(PE) is a new encryption paradigm which provides more sophisticated and flexible functionality. We present an efficient construction of Predicate Encryption which is IND-AH-CPA secure by employing the dual system encryption without random oracle. PE is sufficient for searchable encryptions such as fine-grained control over access to encrypted data or search on encrypted data. We also do some particular research on the relations between PE and Searchable Encryption and find that a secure PE implies the existence of a Searchable Encryption scheme. The new notion of Public-Key Encryption with Fine-grained Keyword Search(PEFKS) is proposed. We develop the transformation of PE to PEFKS and use the tranfromation to construct an efficient PEFKS scheme.

Category / Keywords: public-key cryptography /

Date: received 31 Jul 2011

Contact author: weiyi wj at gmail com