Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption

http://www.firstlight.cn 2010-11-05

This paper presents a fully secure functional encryption scheme for a wide class of relations, that are specified by non-monotone access structures combined with inner-product relations. The security is proven under a standard assumption, the decisional linear (DLIN) assumption, in the standard model. The proposed functional encryption scheme covers, as special cases, (1) key-policy and ciphertext-policy attribute-based encryption with non-monotone access structures, and (2) (hierarchical) predicate encryption with inner-product relations and functional encryption with non-zero inner-product relations.