ORAL DEFENSE ANNOUNCEMENT

Chen Jie

ON FUNCTIONAL ENCRYPTION: NEW CONSTRUCTIONS AND SOME RELATIONS

Abstract:

In recent years, a new, generalized notion of public-key primitive called Functional Encryption (FE) has emerged. In the FE setting, public keys and their matching secret keys can be associated with identities, attributes, policies, predicates and so on. FE covers a large number of primitives, notably, Identity-Based Encryption (IBE), Inner Product Encryption (IPE), Spatial Encryption (SE), Attribute-Based Encryption (ABE) and has numerous applications, particularly in the domains of access control, content distribution, mail filtering, data searching, broadcasting, tracing, and biometrics. Many works on FE in the literature have been targeting on improving the efficiency of constructions, simplifying the relevant assumptions, and achieving stronger security (e.g. full security and adaptively attribute-hiding). In this thesis, we examine three aspects of FE: efficiency of IBE, key revocation in IBE, and the relation between two major classes of FE, namely, Hierarchical IPE (HIPE) and SE.