Abstract

In this paper, we present a comprehensive picture and the state of the art of Identity Based Cryptography (IBC) and their security implications with applications. First, we introduce the basic concepts of security and principles of cryptography and then move into identity-based cryptography, an overview of its development process and research progress. We explain identity-based encryption (IBE) schemes and identity-based signature (IBS) schemes and their security analysis. Later, we discuss the hierarchical identity-based encryption (HIBE) present in standard model as well as in random oracle model. We also discuss Revocable Identity Based Encryption (RIBE) schemes from the view point of security models and constructions.

We review several encryption schemes and their advantages and disadvantages along with their efficiency and security considerations.

References


Index Terms

Computer Science Security

Keywords

Identity based Encryption, Hierarchical IBE, Signature, Pairings, Fuzzy IBE, Revocation IBE.