Further Observations on Certificate-Base Encryption and its Generic Construction from Certificateless Public Key Encryption

http://www.firstlight.cn 2010-12-04

Certificate-based encryption (CBE) is a new asymmetric encryption paradigm which was introduced to solve the certificate management problem in traditional public key encryption (PKI). It combines PKE and identity-based encryption (IBE) while preserving some of their most attractive features. CBE provides an efficient implicit certificate mechanism which eliminates the third-party queries and simplifies the certificate revocation problem in the traditional PKI. It also solves the key escrow problem and key distribution problem inherent in IBE. In this paper, we introduce the key replacement attack and the malicious-but-passive certifier attack into CBE, and define a class of new security models for CBE under different security levels according to the power of the adversaries against CBE. Our new security models are more elaborated and stronger compared with other existing ones. Then, we propose a generic construction of CBE from certificateless public key encryption and prove its security under the proposed security models in the standard model. We also show a concrete conversion using the proposed generic construction.

存档文本