Abstract

Revocation problem is a critical issue for key management of public key encryption systems. All identity (ID)-based encryption (IBE) systems, hierarchical IBE (HIBE) systems, or certificateless public key encryption (CL-PKE) systems must provide a revocation method to revoke misbehaving or compromised users from the systems. In the past, there was little work on studying the revocation problem of these systems. For the revocation problem, Boneh and Franklin suggested that the key generation center (KGC) generates all non-revoked users' new private keys of each period and then uses secure channels to transmit these periodic private keys to non-revoked users. Certainly, the existing IBE, HIBE or CL-PKE systems can inherit the revocation method suggested by Boneh and Franklin to revoke misbehaving compromised users. However, these IBE, HIBE or CL-PKE constructions using Boneh and Franklin's revocation method still require enormous computational cost between users and the KGC in each period, because computational workload for encrypting and decrypting the new private keys are required for each period.

In the thesis, we first present an efficient revocable IBE (RIBE) with a public channel in the random oracle model, which provides a practical alternative to the previously proposed revocation solutions while remaining efficient for encryption and decryption. We then extend the proposed RIBE to propose an efficient revocable multi-receiver-based encryption (RMIBE) scheme in the random oracle model. Our RMIBE scheme needs only one pairing operation to encrypt an identical message for n receivers while remaining the merit of user revocability in the RIBE scheme. Although the RIBE schemes based on the random oracle model can offer better performance, they could be insecure when random oracles are instantiated with concrete hash functions. Hence, we employ the same revocable concept to propose a new RIBE without random oracles (standard model) to provide full security. Furthermore, we also adopt the same revocable concept to propose the first HIBE scheme with a public revocation mechanism, called revocable HIBE (RMHIBE), which is extended from Lewko and Waters's unbounded HIBE scheme presented in Eurocrypt 2011. Finally, we also propose two revocable certificateless public key encryption (RCL-PKE) schemes in the random oracle model and standard model, respectively. Under related assumptions, we demonstrate that the proposed schemes mentioned above are semantically secure.