Attribute-Based Encryption with Verifiable Outsourced Decryption

Abstract—

Attribute-based encryption (ABE) is a public-key based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. A promising application of ABE is flexible access control of encrypted data stored in the cloud, using access polices and ascribed attributes associated with private keys and cipher text. One of the main efficiency drawbacks of the existing ABE schemes is that decryption involves expensive pairing operations and the number of such operations grows with the complexity of the access policy. Recently, Green et al. proposed an ABE system with outsourced decryption that largely eliminates the decryption overhead for users. In such a system, a user provides an untrusted server, say a cloud service provider, with a transformation key that allows the cloud to translate any ABE cipher text satisfied by that user’s attributes or access policy into a simple cipher text, and it only incurs a small computational overhead for the user to recover the plaintext from the transformed cipher text. Security of an ABE system with outsourced decryption ensures that an adversary (including a malicious cloud) will not be able to learn anything about the encrypted message; however, it does not guarantee the correctness of the transformation done by the cloud. In this paper, we consider a new requirement of ABE with outsourced decryption: verifiability. Informally, verifiability guarantees that a user can efficiently check if the transformation is done correctly. We give the formal model of ABE with verifiable outsourced decryption and propose a concrete scheme. We prove that our new scheme is both secure and verifiable, without relying on random oracles. Finally, we show an implementation of our