Attribute-based Access Control with Constant-size Cipher text in Cloud Computing

With the popularity of cloud computing, there have been increasing concerns about its security and privacy. Since the cloud computing environment is distributed and untrusted, data owners have to encrypt outsourced data to enforce confidentiality. Therefore, how to achieve practicable access control of encrypted data in an untrusted environment is an urgent issue that needs to be solved. Attribute-Based Encryption (ABE) is a promising scheme suitable for access control in cloud storage systems. This paper proposes a hierarchical attribute-based access control scheme with constant-size cipher text. The scheme is efficient because the length of cipher text and the number of bilinear pairing evaluations to a constant are fixed. Its computation cost in encryption and decryption algorithms is low. Moreover, the hierarchical authorization structure of our scheme reduces the burden and risk of a single authority scenario. We prove the scheme is of CCA2 security under the decisional q-Bilinear Diffie-Hellman Exponent assumption. In addition, we implement our scheme and analyse its performance. The analysis results show the proposed scheme is efficient, scalable, and fine-grained in dealing with access control for outsourced data in cloud computing.