Broadcast Scheme Access Policy Using Descriptive Attributes with the Ciphertext

Md Azharl Islam

ABSTRACT
In a secure broadcast scheme, a broadcaster can encrypt the data such that only a selected subset of users picked during encryption time from a set S of users, can decrypt it. Most of the existing works have addressed issues such as collision resistance, short ciphertext, short secret and public keys and anonymity of the recipient. Encryption schemes used in those works are not able to enforce fine grained access policy to the ciphertext without knowing the identity of the users. But, in our scheme, the broadcaster can enforce any access policy in terms of a set of descriptive attributes with the ciphertext. So, before encryption, broadcaster only need to know what type of access policies are applicable for a particular data item rather than the list of allowed users who have access to the data. This gives broadcaster more flexibility in enforcing access control in broadcast data.