Liu, Ximeng; **Ma, Jianfeng**; **Xiong, Jinbo**; **Li, Qi**; **Zhang, Tao**

A ciphertext-policy weighted attribute based encryption scheme. (Chinese. English summary)

Zbl 1299.68029
J. Xi'an Jiaotong Univ. 47, No. 8, 44-48, 86 (2013).

Summary: The previous ciphertext-policy attribute based encryption schemes scarcely consider the significance of attributes. The concept of weight is thus introduced into the ciphertext-policy attribute-based encryption scheme. The authority assigns different weights to attributes according to their importance in the system. The authority transfers the attribute set into weight attribute separation set according to the weight of attributes. A ciphertext-policy weighted attribute-based encryption scheme is realized with linear secret sharing methods. And the security model of the ciphertext-policy weighted attribute-based encryption scheme is proposed. This scheme verifies the security against chosen-plaintext attack under the decisional bilinear Diffie-Hellman exponent assumption in the standard model. Although the size of ciphertext and private key increase, the new scheme achieves fine-grained access control, and reflects the significance of attributes, which is more suitable for the practical applications.

MSC:

68P25 Data encryption (aspects in computer science)
94A60 Cryptography

Keywords:

access control; attribute-based encryption; weighted attribute

Full Text: DOI