Liu, Zhen; Cao, Zhenfu; Wong, Duncan S.

Fully collusion-resistant traceable key-policy attribute-based encryption with sub-linear size ciphertexts. (English) Zbl 1403.94070

Lin, Dongdai (ed.) et al., Information security and cryptology. 10th international conference, Inscrypt 2014, Beijing, China, December 13–15, 2014. Revised selected papers. Cham: Springer (ISBN 978-3-319-16744-2/pbk; 978-3-319-16745-9/ebook). Lecture Notes in Computer Science 8957, 403-423 (2015).

Summary: Recently a series of expressive, secure and efficient attribute-based encryption (ABE) schemes, both in key-policy flavor and ciphertext-policy flavor, have been proposed. However, before being applied into practice, these systems have to attain traceability of malicious users. As the decryption privilege of a decryption key in key-policy ABE (resp. ciphertext-policy ABE) may be shared by multiple users who own the same access policy (resp. attribute set), malicious users might tempt to leak their decryption privileges to third parties, for financial gain as an example, if there is no tracing mechanism for tracking them down. In this work we study the traceability notion in the setting of key-policy ABE, and formalize key-policy ABE supporting fully collusion-resistant blackbox traceability. An adversary is allowed to access an arbitrary number of keys of its own choice when building a decryption-device, and given such a decryption-device while the underlying decryption algorithm or key may not be given, a blackbox tracing algorithm can find out at least one of the malicious users whose keys have been used for building the decryption-device. We propose a construction, which supports both fully collusion-resistant blackbox traceability and high expressivity (i.e. supporting any monotonic access structures). The construction is fully secure in the standard model (i.e. it achieves the best security level that the conventional non-traceable ABE systems do to date), and is efficient that the fully collusion-resistant blackbox traceability is attained at the price of making ciphertexts grow only sub-linearly in the number of users in the system, which is the most efficient level to date.

For the entire collection see [Zbl 1319.94006].

MSC:

94A60	Cryptography	Cited in **1** Document

Keywords:

attribute-based encryption; key-policy; blackbox traceability; efficiency

Full Text: DOI