Xu, Shengmin; **Yang, Guomin**; **Mu, Yi**; **Liu, Ximeng**

Efficient attribute-based encryption with blackbox traceability. (English) Zbl 1421.94079

Baek, Joonsang (ed.) et al., Provable security. 12th international conference, ProvSec 2018, Jeju, South Korea, October 25–28, 2018. Proceedings. Cham: Springer. Lect. Notes Comput. Sci. 11192, 182-200 (2018).

Summary: Traitor tracing scheme can be used to identify a decryption key is illegally used in public-key encryption. In CCS 2013, *Z. Liu* et al. [ACM SIGSAC Conference on Computer and Communications Security, CCS 2013, 475–486 (2013)] proposed an attribute-based traitor tracing (ABTT) scheme with blackbox traceability which can trace decryption keys embedded in a decryption blackbox/device rather than tracing a well-formed decryption key. However, the existing ABTT schemes with blackbox traceability are based on composite order group and the size of the decryption key depends on the policies and the number of system users. In this paper, we revisit blackbox ABTT and introduce a new primitive called attribute-based set encryption (ABSE) based on key-policy ABE (KP-ABE) and identity-based set encryption (IBSE), which allows aggregation of multiple related policies and reduce the decryption key size in ABTT to be irrelevant to the number of system users. We present a generic construction of the ABTT scheme from our proposed ABSE scheme and fingerprint code based on the Boneh-Naor paradigm in [*D. Boneh* and *M. Naor*,CCS 2008. New York: ACM, 501–510 (2008)]. We then give a concrete construction of the ABSE scheme which can be proven secure in the random oracle model under the decisional BDH assumption and a variant of q-BDHE assumption.

For the entire collection see [Zbl 1398.94007].

MSC:

94A60 Cryptography

Keywords:

public-key cryptosystems; attribute-based encryption; blackbox traceability

Full Text: DOI