Cryptology ePrint Archive: Report 2013/219

Designing a Hybrid Attribute-Based Encryption Scheme Supporting Dynamic Attributes

Stefan G. Weber

Abstract: This article presents the design of a novel hybrid attribute-based encryption scheme. The scheme is attribute-based, as it allows encrypting under logical combinations of attributes, i.e. properties that users satisfy. It is hybrid, as it combines ciphertext-policy attribute-based encryption (CP-ABE) with location-based encryption (LBE) on the level of symmetric keys. It can efficiently handle dynamic attributes with continuous values, like location, even in resource-constrained settings.

Category / Keywords: public-key cryptography /

Publication Info: Updates some content of the book "Multilaterally Secure Pervasive Cooperation - Privacy Protection, Accountability and Secure Communication for the Age of Pervasive Computing", Cryptology and Information Security Series Vol. 9, IOS Press, 2012

Date: received 14 Apr 2013

Contact author: stefangeorgweber at gmail com

Available formats: PDF | BibTeX Citation

Version: 20130414:154815 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]