Abstract: Multi-authority Attribute-based Signature Scheme with Constant-length Signature

Dan Cao, Xiaofeng Wang*, Baokang Zhao, Jinshu Su
School of Computer, National University of Defense Technology, Changsha, 410073, China
E-mail: d_cao@yahoo.cn, {xf_wang, bkzhao, sjs}@nudt.edu.cn

Abstract

The attribute-based signature (ABS) is a recent cryptography primitive, in which a signature does not attest to the identity of a signer, but to a policy regarding the attributes possessed by the underlying signer. The advantages of unforgeability and signer privacy make ABS a good prospect in access control and anonymous authentication systems. However, most existing work of ABS does not take into account the scenario of multiple authorities, which is more likely to be used by real world applications. In this paper, we propose a multi-authority ABS scheme named CL-MABS under the computational Diffie-Hellman (CDH) assumption. It has constant-size signatures, i.e. its signature size is independent of the number of attributes used in the signature generation. Moreover, it can support policies consisting of AND, OR, threshold and even NOT gates of attributes. We prove the correctness and unforgeabilty of our scheme. In addition, the cost of dynamically adding or removing an attribute authority in CL-MABS is low.

Acknowledgement

The work described in this paper is partially supported by the grants of the project of National Science Foundation of China under Grant No. 61103194; the program for Changjiang Scholars and Innovative Research Team in University (No. IRT 1012), Science and Technology Innovative Research Team in Higher Educational Institutions of Hunan Province: "network technology"; and Hunan Province Natural Science Foundation of China (11JJ7003).