Threshold Attribute-Based Signatures and Their Application to Anonymous Credential Systems

Siamak F. Shahandashti[1] and Reihaneh Safavi-Naini[2]

[1] School of Computer Science and Software Engineering
University of Wollongong, Australia
http://www.uow.edu.au/∼sfs166
[2] Department of Computer Science
University of Calgary, Canada
http://www.cpsc.ucalgary.ca/∼rei

Abstract. In this paper we propose *threshold attribute-based signatures* (t-ABS). A t-ABS scheme enables a signature holder to prove possession of signatures by revealing only the relevant attributes of the signer, hence providing *signer-attribute privacy* for the signature holder. We define t-ABS schemes, formalize their security and propose two t-ABS schemes: a basic scheme secure against selective forgery and a second one secure against existential forgery, both provable in the standard model, assuming hardness of the CDH problem. We show that our basic t-ABS scheme can be augmented with two extra protocols that are used for efficiently issuing and verifying t-ABS signatures on committed values. We call the augmented scheme a threshold attribute based c-signature scheme (t-ABCS). We show how a t-ABCS scheme can be used to realize a secure *threshold attribute-based anonymous credential system* (t-ABACS) providing issuer-attribute privacy. We propose a security model for t-ABACS, give a concrete scheme using t-ABCS scheme, and prove that the credential system is secure if the t-ABCS scheme is secure.

1 Introduction

Inspired by the recent works on attribute based encryption, we introduce a new signature scheme that we call a *threshold attribute-based signature*, or t-ABS for short. In a t-ABS scheme, a central authority issues secret keys to the signers according to their *attributes*. A signer with an attribute set Att can use his secret key to sign using any subset $A \subset Att$ of attributes. A signature can be verified against a verification attribute set B and verification succeeds if $A \cap B$ has at least size d. Threshold attribute-based signatures have attractive applications that are outlined below.

A t-ABS scheme provides *threshold attribute-based verification*. This can be used for applications such as identity-based signatures that use biometric information as user identities. Since different measurements by different entities will not be exactly the same, *fuzzy verification* is required. Using a threshold

B. Preneel (Ed.): AFRICACRYPT 2009, LNCS 5580, pp. 198–216, 2009.
© Springer-Verlag Berlin Heidelberg 2009

attribute-based signature scheme with suitable choices of mapping and threshold, "close" biometric measurements map to attribute sets for signing and verification that have sufficient overlap and result in successful verification of signature.

A t-ABS scheme enables the signer to choose their "signing identity" (relevant attributes) at the time of signing, and also enables *signature holders* to present for verification a signature that corresponds to subset of signer's attributes. John Smith, a member of 2008 Executive Committee of the Workers' Union (WU), can sign documents as, and a document signed by him can be presented as signed by an Executive Committee member of the WU, a 2008 Executive Committee member of the WU, or simply John Smith. In general, to provide the above functionalities for signers with n "atomic" identities, a t-ABS scheme can be implemented that has signing keys and signatures, both of size $O(n)$. Providing the same functionalities using standard or identity-based signatures requires $O(2^n)$ signing keys, one for each "combined" identity, and $O(2^n)$ signatures, each produced using one of the keys. Note that the naïve solution of $O(n)$ signing keys of a standard or an identity-based signature, is not secure because signatures can be "mixed and matched" with each other. A group of signers, for example, can collude to produce a signature corresponding to the union of their identities. A t-ABS scheme provides *collusion resistance*: that is, no group of colluding signers can produce a signature that could not be generated by a single member of the group.

A t-ABS scheme supports *signer-attribute privacy* for users. Consider a scenario where participation in a poll requires proof of residency in one of the 27 counties in a state. Assume these proofs are cards that are signed by either the local government or police authorities of the counties and are given to the long-time residents and foreign workers, respectively. For privacy reasons, card holders may want to be able to prove that they own a card but protect their other details. Proving possession of such a card is equivalent to proving possession of a card issued by one of the 2×27 possible entities. Using standard or identity-based signatures, a voter can prove possession of a valid signature with respect to one of the 2×27 public keys or identities through a proof of size 2×27 (see *proofs of partial knowledge* [9]). A t-ABS can provide a proof of size $2+27$ and ensures that the attributes of the signer (and hence unnecessary information of the card holder) are not revealed. Signers in such schemes will each have two attributes: one corresponding to 'police' or 'local government', and the other representing one of the 27 counties. Verification of residency is then equivalent to requiring that a card is verifiable with a threshold of $d = 2$ attributes from the set of all $2+27$ attributes above. Generally, if the universal set of attributes can be partitioned such that each signer has at most one attribute from each partition, a t-ABS enables threshold verification with additive cost in terms of the sizes of partitions, while the cost of proofs of partial knowledge is multiplicative. The functionality becomes the only solution in cases where, because of the size and spread of the system, it is practically infeasible for the signature holder and the verifier to know all possible signers.