Chapter 7
An Efficient Attribute-Based Signature with Application to Secure Attribute-Based Messaging System

Piyi Yang
University of Shanghai for Science and Technology, China

Tanveer A Zia
Charles Sturt University, Australia

ABSTRACT

A set of attributes instead of a single string to represent the signer's identity is a challenging problem under standard cryptographic assumption in the standard model. Therefore, designing a fully secure (adaptive-predicate unforgeable and perfectly private) Attribute-Based Signature (ABS) that allows a signer to choose a set of attributes is vital. Existing schemes are either too complicated or have only been proved in the generic group model. In this chapter, the authors present an efficient fully secure ABS scheme in the standard model based on q-parallel BDHE assumption, which is more practical than the generic group model used in the previous schemes. The proposed scheme is highly expressive since it allows any signer to specify claim-predicates in terms of any predicate consisting of AND, OR, and Threshold gates over the attributes in the system. ABS has found many important applications in secure communications, such as anonymous authentication systems and attribute-based messaging systems.

INTRODUCTION

Identity-based signature is a powerful mechanism for providing the authentication of the stored and transmitted information where the identity can be an arbitrary string such as an email address or a registration number, etc. While this is useful for applications, where the data receiver knows specifically the identity of the data signer, in many applications the signer will want to have fine-grained control over how much of their personal information is revealed by the signature.

DOI: 10.4018/978-1-4666-4030-6.ch007

Maji, Prabhakaran, and Rosulek (2008) presented a new vision of identity-based signature that they called Attribute-Based Signature (ABS), in which a signer is defined by a set of attributes instead of a single string representing the signer's identity. In ABS, a user obtains a set of attributes from one or multiple attribute authorities. An attribute-based signature assures the verifier that a signer, whose set of attributes satisfies a (possibly) complex predicate, has endorsed the message. The following example illustrates the concept. Suppose we have the following predicate:

Professor **OR** (((Biology Department **OR** Female) **OR** above 50 years old) **AND** University A).

Alice's attributes are (University A, Female). Bob's attributes are (above 50 years old, Professor). Although their attributes are quite different, it is clear that Alice and Bob can generate a signature on this predicate, and such a signature releases no information regarding the attribute or identity of the signer, i.e. Alice or Bob, except that the attribute of the signer satisfies the predicate.

This kind of authentication required in attribute-based signatures differs from that offered by identity-based signatures. An ABS solution requires a richer semantics, including privacy requirements, similar to more recent signature variants like group signatures (Chaum & Heyst, 1991), ring signatures (Rivest, Shamir, & Tauman, 2001), and mesh signatures (Boyen, 2007). All of these primitives share the following semantics:

- **Unforgeability:** By verifying the signature, one is assured that the message was indeed endorsed by a party who satisfies the condition described in the claim.
- **Privacy:** The signature reveals no information about the signer other than the fact that it satisfies the claim. In particular, different signatures cannot be identified as generated by the same party.

Besides these two semantics, ABS has another important property which is called collusion resistance. It assures different parties should not be able to pool together their attributes to sign a message with a claim which none of them satisfy alone. For instance, if Alice has an attribute Female, and her friend Bob has an attribute Professor, they should not be able to sign a message claiming to have both the attributes.

ABS has found many important applications. For instance, it helps to provide fine-grained access control in anonymous authentication systems (Li, Au, Susilo, Xie, & Ren, 2010). Another application of ABS, given by (Maji, Prabhakaran, & Rosulek, 2008, 2011), is to fulfill a critical security requirement in attribute-based messaging (ABM) systems using ABS.

BACKGROUND STUDY ABOUT ABS

Attribute-Based Signatures were first introduced by Maji, Prabhakaran, and Rosales (2008) as a way to let a signature attest not to the identity of the individual who endorsed a message, but instead to a (possibly complex) claim regarding the attributes they possess. They constructed an ABS scheme that supports a powerful set of predicates, namely, any predicate consists of AND, OR, and Threshold gates. However, the security of their scheme is weak as their construction is only proved in the generic group model. Since then, there have been lots of works on this subject (Escala, Herranz, & Morillo, 2011; Khader, 2007a, 2007b; Li, Au, Susilo, Xie, & Ren, 2010; Li & Kim, 2007, 2010; Maji, Prabhakaran, & Rosulek, 2011; Okamoto & Takashima, 2011; Shahandashti & Safavi-Naini, 2009).

Recently, Maji, Prabhakaran, and Rosulek (2011) presented an ABS scheme that is proven secure in the standard model. But it is much less efficient and more complicated than the scheme in (Maji, Prabhakaran, & Rosulek, 2008), since it employs the Groth-Sahai NIZK protocols (Groth &