Attribute-Based Identification: Definitions and Efficient Constructions

Hiroaki Anada, Seiko Arita, Sari Handa, and Yosuke Iwabuchi
Graduate School of Information Security, Institute of Information Security, Japan
2-14-1 Tsuruya-Cho, Kanagawa-Ku, Yokohama-Shi, 221-0835, Japan
hiroaki.anada@gmail.com, {arita,mgs125502,mgs123101}@iisec.ac.jp

Abstract. We propose a notion of attribute-based identification (ABID) in two flavors: prover-policy ABID (PP-ABID) and verifier-policy ABID (VP-ABID). In a PP-ABID scheme, a prover has an authorized access policy written as a boolean formula over attributes, while each verifier maintains a set of attributes. The prover is accepted when his access policy fits the verifier’s set of attributes. In a VP-ABID scheme, a verifier maintains an access policy written as a boolean formula over attributes, while each prover has a set of authorized attributes. The prover is accepted when his set of attributes satisfies the verifier’s access policy. Our design principle is first to construct key-policy and ciphertext-policy attribute-based key encapsulation mechanisms (KP-ABKEM and CP-ABKEM). Second, we convert KP-ABKEM and CP-ABKEM into challenge-and-response PP-ABID and VP-ABID, respectively, by encapsulation-and-decapsulation. There, we show that KP-ABKEM and CP-ABKEM only have to be secure against chosen-ciphertext attacks on one-wayness (OW-CCA secure) for the obtained PP-ABID and VP-ABID to be secure against concurrent man-in-the-middle attacks (cMiM secure). According to the design principle, we construct concrete KP-ABKEM and CP-ABKEM with the OW-CCA security by enhancing the KP-ABKEM of Ostrovsky, Sahai and Waters and CP-ABKEM of Waters, respectively. Finally, we obtain concrete PP-ABID and VP-ABID schemes that are proved to be selectively secure in the standard model against cMiM attacks.

Keywords: access policy, attribute, identification, key encapsulation mechanism.

1 Introduction

An identification (ID) scheme enables a prover to convince a verifier that the prover certainly knows a secret key that corresponds to the matching public key. For example, Σ-protocols [7] such as the Schnorr protocol [14,5] are widely recognized. In these ID schemes, the public key to which the verifier refers limits the corresponding secret key uniquely, and also, the corresponding prover.

* Supported by MEXT-Supported Program for the Strategic Research Foundation at Private Universities, 2011-2013.
In this paper, we will describe an attribute-based identification (ABID). In an ABID scheme, each entity has credentials called attributes. On the other hand, an access policy is written as a boolean formula over those attributes. Then, a verifier can identify that a prover certainly belongs to a set of entities that have authorized access policies that fit the verifier’s attributes, or, in the dual flavor, a verifier can identify that a prover certainly belongs to a set of entities that possess authorized attributes that satisfy the verifier’s access policy. Hence, ABID schemes can be considered as an expansion of the usual ID schemes.

However, ABID schemes are not a mere expansion, but have useful applications beyond those of the usual ID schemes. For example, the following scenarios of smart card systems motivate us to apply ABID.

**Functional Tickets.** Suppose that we are going to stay at a resort complex, a ski resort, for instance. We search Web sites or brochures for information about services: available dates, accommodation, ski lifts, restaurants in ski areas and hot springs around the areas. For each service, we usually buy a ticket, paying with money or using a credit card. However, acquiring many tickets and carrying a wallet is inconvenient, and therefore, it would be more convenient if we could gain access to these services by using only one smart card. In the smart card, a service authority writes an access policy in terms of the service names that we choose, for instance, [January 1 to 4, 2014] AND [[Hotel A] OR [Ski Lift AND [Day OR Night]] OR [Lunch OR Beer] OR [Hot Spring X]]. A functional ticket is a ticket embedded in a smart card that realizes an access policy as a boolean formula over services, as in this scenario. Here, the access policy is chosen according to our requirements.

**Functional Gates.** Suppose that we have to design a security gate system for an office building in which different kinds of people work: employees of several companies holding many different positions, security guards, cleaning staffs and janitors. There are also many types of security gates to be designed: building entrances, intelligent elevators to limit available floors, company gates, common refreshment areas and room doors for the above staffs. In this case, one solution is to use smart cards and gates with sensors. That is, an authority issues each person a smart card in which a set of attribute data is written. Each gate decides whether to “pass” each person carrying a smart card according to the gate’s access policy, for instance, [Year 2014] AND [[Company A] AND [Manager]] OR [Security Guard]]. A functional gate is a gate that maintains an access policy as a boolean formula over attributes of people, as in this scenario. Here, the access policy is chosen according to the kind of people that the gate should allow to pass.

### 1.1 Our Contributions

Bearing the above scenarios in mind, we propose a notion of attribute-based identification (ABID) that has two flavors corresponding to the scenarios: prover-policy ABID and verifier-policy ABID.