Information Sciences 275 (2014) 57–67

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

# Attribute-based key-insulated signature and its applications

Jianhong Chen [a,c,e,*], Yu Long [c], Kefei Chen [b,c,e], Jie Guo [d]

[a] Faculty of Computer Engineering, Huaiyin Institute of Technology, Huaian 223003, PR China
[b] School of Science, Hangzhou Normal University, Hangzhou 310036, PR China
[c] Dept. of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, PR China
[d] School of Information Security Engineering, Shanghai 200240, PR China
[e] Shanghai Key Laboratory of Scalable Computing and System, Shanghai Jiao Tong University, Shanghai 200240, PR China

ARTICLE INFO

*Article history:*
Received 8 November 2011
Received in revised form 6 November 2013
Accepted 9 February 2014
Available online 18 February 2014

*Keywords:*
Key-insulated
Attribute-based
Signature
Key-exposure
Proxy
Bidirectional broadcasting

ABSTRACT

In an attribute-based signature (ABS) system, a signature does not give proof of the identity of the individual who signed a message; it instead gives proof to a claim regarding the attributes that the underlying signer owns. For ABS, investigators have found many practical applications that require signer-attribute privacy. However, this approach is inadequate for handling scenarios in which the signing key is exposed due to viruses, worms or other break-ins that are allowed by operating-system holes. To overcome the limitation of existing ABS systems, we introduce the notion of an attribute-based key-insulated signature (ABKIS), in which signing keys are refreshed at discrete time periods via an interaction between the user and the helper (a physically-secure but computationally-limited device). We formalize this security model and propose a concrete ABKIS scheme, which is proven to be secure under the standard computational Diffie–Hellman assumption. Furthermore, as an application, a time-conditioned attribute-based proxy signature (TC-ABPS) is derived from our proposed ABKIS scheme. Another typical application of our scheme is for anonymous provider authentication in a bidirectional broadcasting service.



## 1. Introduction

In an attribute-based signature (ABS) system [25], a signature does not give proof of the identity of the individual who signed a message; instead, it substantiates a claim regarding the attributes that the underlying signer owns.

Attribute-based signatures have found many practical applications, such as anonymous authentication and attribute-based messaging systems. For example, a faculty member, Bob, who has the attributes of "University A", "Faculty" and "Department of Electronic and Computer Engineering" would like to complain or give some suggestions to an administrator of University A anonymously. In practice, the most important threat to the security of an ABS scheme is the exposure of the secret signing key due to viruses, worms or other break-ins that are allowed by operating-system holes. We provide a means to protect against this type of key exposure by using the key insulation mechanism [13].

To show further motivation, we consider the case in which Bob is to go on a vacation, and he delegates his secretary Alice to complete his daily business. Obviously, the existing ABS schemes do not meet such needs.

In this paper, we introduce the notion of an attribute-based key-insulated signature (ABKIS), whereby the secret signing key is updated at discrete time periods. In addition, we apply ABKIS to a time-conditioned attribute-based proxy signature (TC-ABPS), whereby Alice can sign on behalf of Bob during the designated time periods.

* Corresponding author at: Faculty of Computer Engineering, Huaiyin Institute of Technology, Huaian 223003, PR China. Tel.: +86 517 83591046.
*E-mail address:* jianhong.chen.cis@gmail.com (J. Chen).

http://dx.doi.org/10.1016/j.ins.2014.02.021
0020-0255/

### 1.1. Our results

Our contribution includes a formal definition of an attribute-based key-insulated signature and its security notion. Briefly speaking, an ABKIS scheme involves two principals: a signer and a verifier, which is similar to existing signature systems. The signer can update his secret signing key without the help of an authority and without changing his identity (a set of attributes) via an interaction between the user and the helper (a physically secure but computationally limited device). The signature does not give proof of the identity of the individual who signed a message; instead, it substantiates a claim regarding the attributes that the underlying signer owns. Under the computational Diffie–Hellman assumption, we prove its security in the standard model. We apply the proposed ABKIS scheme to a time-conditioned attribute-based proxy signature (TC-ABPS). In the TC-ABPS system, the proxy signer who has a temporary private key of the original signer can sign on behalf of the original signer during the selected time period. As another application of our ABKIS scheme, provider authentication for a bidirectional broadcasting service with the provider's privacy is proposed.

### 1.2. Related work

#### 1.2.1. Identity-based cryptosystems

In 1984, Shamir [37] introduced a novel cryptography primitive called identity-based cryptosystems to remove public key certificates. In an identity-based cryptosystem, the user's public key can be a binary sequence that corresponds to some information that identifies him, such as a name and an IP address, while the private key is calculated by a trusted authority called a private key generator (PKG). In Crypto 2001, Boneh and Franklin [7] proposed a fully functioning identity-based encryption (IBE) that is based on Weil pairing over elliptic curves. Subsequently, many identity-based signature (IBS) schemes [11,22,30,32,33,46] that use pairings were proposed.

#### 1.2.2. Attribute-based encryption

As a generalization of IBE, fuzzy identity-based encryption (FIBE), which was introduced by Sahai and Waters, [34] can provide an error-tolerance property for IBE. FIBE can be used for attribute-based encryption (ABE) [34], which permits a threshold attribute-based decryption of the encrypted data. As a result, many improvements and extensions [18,6,12] have been presented.

#### 1.2.3. Fuzzy identity-based and attribute-based signature schemes

In Table 1, we compare *fuzzy identity-based signatures* [43] with *attribute-based signatures* [25].

*Fuzzy identity-based signature* (FIBS) schemes [9,43,38] are direct applications of FIBE schemes [34,4] via the known transform [16] from IBE to IBS. These FIBS schemes do not account for the anonymity of the signer. FIBS can be directly used for IBS systems that use biometric identities.

Researchers [35,25,26,29] treated attribute privacy as a fundamental requirement of an *attribute-based signature* (ABS) and constructed some ABS primitives that have signer anonymity. In the sense of *signer anonymity*, a signature attests not to the identity of the user who endorsed a message but instead to a claim regarding the group that he belongs to. Our proposed ABKIS scheme follows this research line.

#### 1.2.4. Key evolving protocols

To mitigate the potential damages of key exposure, key-evolving protocols were studied in three main lines of work, which are shown in Table 2: *forward security* [3,10,5,24,1,2,8,28,30,45], *key insulation* [13,14,20,21,47,39–42] and *intrusion resilience* [23,15,27,19,44].

As in [3,10], *forward secure* systems involve public keys that remain unchanged throughout the lifetime of the protocol, while private keys evolve at the beginning of discrete time intervals. Each private key is used to sign or decrypt messages only during a specific time period and to compute a new private key at the end of that time period.

The notion of *key insulation* complements the notion of forward security. Key-insulated schemes involve a physically-secure (but computationally limited) device called helper, in which certain keys (help keys) are stored. These keys are used for updating, at regular intervals, the user's short-term secret (a temporary private key), which is used to sign or decrypt messages. As in [13,14,42], this action is fulfilled to preserve the security of past and future time periods in which the user device (where the temporary private keys of the user are stored) is compromised (unlike forward-secure cryptosystems [3,10] that only protect past time periods).

**Table 1**
Fuzzy-identity based and attribute-based signature schemes.

| | Letting the user's public key be a set of attributes | Supporting signer anonymity |
|---|---|---|
| Fuzzy identity-based signature [9,43,38] | Yes | No |
| Attribute-based signature [35,25,26,29] | Yes | Yes |