University of Wollongong

Research Online

Faculty of Engineering and Information
Sciences - Papers: Part A

Faculty of Engineering and Information
Sciences

1-1-2014

Attribute-based signature with message recovery

Kefeng Wang

University of Wollongong, kw909@uowmail.edu.au

Yi Mu

University of Wollongong, ymu@uow.edu.au

Fuchun Guo

University of Wollongong, fuchun@uow.edu.au

Follow this and additional works at: <https://ro.uow.edu.au/eispapers>

Part of the [Engineering Commons](#), and the [Science and Technology Studies Commons](#)

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

Attribute-based signature with message recovery

Abstract

We present a new notion called the attribute-based signature with message recovery. Compared with the existing attribute-based signature schemes, an attribute-based signature with message recovery scheme does not require transmission of the original message to verify the validity of the signature, since the original message can be recovered from the signature. Therefore, this scheme shortens the total length of the original message and the appended attribute-based signature. The contributions of this paper are threefold. First, we introduce the notion of attribute-based signature with message recovery. Second, we present a concrete construction of an attribute-based signature with message recovery scheme based on bilinear pairing. Finally, we extend our scheme to deal with large messages. The proposed schemes support extensible predicates and are proven to be existentially unforgeable against adaptively chosen message attacks in the random oracle model under the assumption that the Computational Diffie-Hellman problem is hard. We demonstrate that the proposed schemes are also equipped with the attribute privacy property.

Keywords

message, recovery, attribute, signature

Disciplines

Engineering | Science and Technology Studies

Publication Details

Wang, K., Mu, Y. & Guo, F. (2014). Attribute-based signature with message recovery. Lecture Notes in Computer Science, 8434 433-447.

Attribute-Based Signature with Message Recovery

Kefeng Wang, Yi Mu, Willy Susilo, and Fuchun Guo

Centre for Computer and Information Security Research
School of Computer Science and Software Engineering
University of Wollongong, Wollongong NSW 2522, Australia
{kw909, ymu, wsusilo, fuchun}@uow.edu.au

Abstract. We present a new notion called the *attribute-based signature with message recovery*. Compared with the existing attribute-based signature schemes, an attribute-based signature with message recovery scheme does not require transmission of the original message to verify the validity of the signature, since the original message can be recovered from the signature. Therefore, this scheme shortens the total length of the original message and the appended attribute-based signature. The contributions of this paper are threefold. First, we introduce the notion of attribute-based signature with message recovery. Second, we present a concrete construction of an attribute-based signature with message recovery scheme based on bilinear pairing. Finally, we extend our scheme to deal with large messages. The proposed schemes support flexible threshold predicates and are proven to be existentially unforgeable against adaptively chosen message attacks in the random oracle model under the assumption that the Computational Diffie-Hellman problem is hard. We demonstrate that the proposed schemes are also equipped with the attribute privacy property.

Keywords: Signature, Attribute-Based Signature, Message Recovery

1 Introduction

Essentially, there are two general classes of digital signature schemes. Signature schemes with appendix require the original message as input to the verification algorithm. Signature schemes with message recovery do not require the original message as input to the verification algorithm. In networks with limited bandwidth and lightweight mobile devices, long digital signatures will obviously be a drawback. Apart from shortening the signature itself, the other effective approach for saving bandwidth is to eliminate the requirement of transmitting the signed original message for the sake of verifying the attached digital signature. In this work, we consider the latter approach. In signature schemes with message recovery, all or part of the original message is embedded within the signature and can be recovered from the signature itself. It is somewhat related to the problem of signing short messages using a scheme that minimizes the total length of the

original message and the appended signature, and hence it is useful in an organization where bandwidth is one of the main concerns and useful for applications in which short messages should be signed.

An attribute-based signature is an elaborated cryptographic notion that supports fine-grain access control in anonymous authentication systems. A related approach, but much simpler, to an attribute-based signature is identity-based signature. Compared with an identity-based signature in which a single string representing the signer's identity, in an attribute-based signature, a signer who obtains a certificate for a set of attributes from the attribute authority is defined by a set of attributes. An attribute-based signature attests not to the identity of the individual who signed a message, but assures the verifier that a signer whose set of attributes satisfies a predicate has endorsed the message. In an attribute-based signature, the signature reveals no more than the fact that a single user with some set of attributes satisfying the predicate has attested to the message. In particular, the signature hides the attributes used to satisfy the predicate and any identifying information about the signer. Furthermore, users cannot collude to pool their attributes together.

Our Contributions. In this paper, we introduce the notion of attribute-based signature with message recovery. This notion allows fine-grain access control as well as enjoys the shortness of message-signature length. We propose two efficient schemes supporting flexible threshold predicate. The first one embeds short original message in the signature and it will be recovered in the process of verification, while keeping the signature size the same as existing scheme which requires transmission of the original message to verify the signature. For large messages, the second scheme separates the original message to two parts. The signature is appended to a truncated message and the discarded bytes can be recovered by the verification algorithm. The security of our schemes are proven to be existentially unforgeable against adaptively chosen message attacks in the random oracle model under the assumption that the CDH problem is hard. These schemes are also equipped with attribute-privacy property.

Paper Organization. The rest of this paper is organized as follows: In Section 2, we introduce some related work that has been studied in the literature. In Section 3, we introduce some preliminaries used throughout this paper. In Section 4, we propose a notion of attribute-based signature with message recovery scheme and present a concrete scheme based on bilinear pairing. We also present a security model and security proofs about existential unforgeability against adaptively chosen message attacks and attribute-privacy property. We also extend the first scheme in order to deal with large messages. Section 5 concludes the paper.

2 Related Work

Attribute-based signatures extend the identity-based signature of Shamir [11] by allowing the identity of a signer to be a set of descriptive attributes rather than a single string. As a related notion to attribute-based signature, fuzzy identity-based signature was proposed and formalized in [13], which enables users to

generate signatures with part of their attributes. An attribute-based signature was also proposed in [12], to achieve almost the same goal. However, these kinds of signatures do not consider the anonymity for signers. Khader [3, 2] proposed a notion called attribute-based group signatures. This primitive hides the identity of the signer, but reveals which attributes the signer used to satisfy the predicate. It also allows a group manager to identify the signer of any signature. In Khader [4] and Maji et al. [7, 8], they treated attribute-privacy as a fundamental requirement of attribute-based signatures.

Maji et al. [7] constructed an attribute-based signature scheme that supports a powerful set of predicates, namely, any predicate consists of AND, OR and Threshold gates. However, their construction is only proved in the generic group model. Li and Kim [6] first proposed an attribute-based signature scheme that is secure under the standard CDH assumption. Their scheme only considered (n, n) -threshold, where n is the number of attributes purported in the signature. Shahandashti and Safavi-Naini [10] extended Li and Kim's scheme [6] and presented an attribute-based signature scheme supporting (k, n) -threshold. Li et al. [5] explored a new signing technique integrating all the secret attributes components into one. Their constructions provide better efficiency in terms of both the computational cost and signature size.

In order to minimize the total length of the original message and the appended signature, message recovery schemes were introduced (e.g. [9]). Zhang et al. [14] presented the seminal construction of an identity-based message recovery signature scheme. Inspired by the schemes due to Zhang et al. [14] and Li et al. [5], we propose our attribute-based signature with message recovery scheme.

Comparison As we have mentioned above, the scheme of Li et al. [5] have improved schemes of [6, 10] to provide better efficiency in terms of both the computational cost and signature size. Compared with the scheme of Li et al. [5] which requires transmission of the original message, our scheme embeds the original message in the signature while keeping the signature size same as that of [5]. We also note that Gagné et al. [1] proposed a new threshold attribute-based signature scheme which they claimed the signature size is independent of the number of attributes. However, this result is restricted only to a very special (t, t) threshold scenario. For general attribute policies such as (t, n) threshold scenario, the signature size still grows linearly with the number of attributes used to generate the signature. Furthermore, the scheme of Gagné et al. [1] only deals with fixed threshold. While our scheme can deal with flexible threshold from 1 to d which is predefined in the setup step.

3 Preliminaries

3.1 Lagrange Interpolation

Given d points $q(1), \dots, q(d)$ on a $d - 1$ degree polynomial, let S be this d -element set. The Lagrange coefficient $\Delta_{j,S}(i)$ of $q(j)$ in the computation of $q(i)$

is:

$$\Delta_{j,S}(i) = \prod_{\eta \in S, \eta \neq j} \frac{i - \eta}{j - \eta}$$

We can use Lagrange interpolation to compute $q(i)$ for any $i \in \mathbb{Z}_p$.

3.2 Bilinear Pairing

Let $\mathbb{G}_1$ be a cyclic additive group whose order is a prime p . Let $\mathbb{G}_2$ be a cyclic multiplicative group with the same order p . Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a bilinear mapping with the following properties:

- Bilinearity: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $\{P, Q\} \in \mathbb{G}_1, \{a, b\} \in \mathbb{Z}_q$.
- Non-degeneracy: There exists $P \in \mathbb{G}_1$ such that $\hat{e}(P, P) \neq 1$.
- Computability: There exists an efficient algorithm to compute $\hat{e}(P, Q)$ for all $\{P, Q\} \in \mathbb{G}_1$.

3.3 CDH Problem

Let $\mathbb{G}_1$ be a group of prime order p . Let g be a generator of $\mathbb{G}_1$. Let $\mathcal{A}$ be an attacker. $\mathcal{A}$ tries to solve the following problem: Given (g, g^a, g^b) for some unknown $a, b \in \mathbb{Z}_p^*$, compute g^{ab} .

The CDH problem is said to be intractable, if for every probabilistic polynomial time algorithm $\mathcal{A}$, the success probability is negligible.

4 Attribute-Based Signature with Message Recovery

4.1 Definitions

We assume there is a universal set of attributes U . Each signer is associated with a subset $\omega \subset U$ of attributes that is verified by an attribute authority. Our scheme consists of the following four algorithms.

Setup: On input of a security parameter, this algorithm selects the master secret key and generates the corresponding public key.

Extract: When a party requires its attribute private key $\{D_i\}_{i \in \omega}$ corresponding to an attribute set ω , this algorithm generates the attribute private key using the master key and attributes in ω if he is eligible to be issued with these attributes.

Sign: This scheme supports all predicates $\mathcal{R}_{t,\bar{\omega}}(\cdot) \rightarrow 0/1$ consisting of t out of n threshold gates, in which $\bar{\omega}$ is an n -element attribute set with threshold value t flexible from 1 to d where $\mathcal{R}_{t,\bar{\omega}}(\omega) = 1$ when $|\omega \cap \bar{\omega}| \geq t$. On input a message m , a predicate $\mathcal{R}_{t,\bar{\omega}}(\cdot) \rightarrow 0/1$, and a sender's private key $\{D_i\}_{i \in \omega}$, this algorithm generates a signature σ when $|\omega \cap \bar{\omega}| \geq t$.

Verify: When receiving a signature σ and a predicate $\mathcal{R}_{t,\bar{\omega}}(\cdot) \rightarrow 0/1$, this algorithm checks whether the signature is valid corresponding to the predicate $\mathcal{R}_{t,\bar{\omega}}(\cdot) \rightarrow 0/1$. If the signature σ is valid, this algorithm recovers the original message m .

4.2 Our Scheme

Setup: First, define the attributes in universe U as elements in $\mathbb{Z}_p^*$ where p is a sufficient large prime. A $(d-1)$ default attribute set from $\mathbb{Z}_p^*$ is given as $\Omega = \{\Omega_1, \Omega_2, \dots, \Omega_{d-1}\}$. Select a random generator $g \in \mathbb{G}_1$, a random $x \in \mathbb{Z}_p^*$, and set $g_1 = g^x$. Next, pick a random element $g_2 \in \mathbb{G}_1$. Five hash functions are also chosen such that $H_1 : \mathbb{Z}_p^* \rightarrow \mathbb{G}_1$, $H_2 : \{0, 1\}^* \rightarrow \mathbb{Z}_p^*$, $H_3 : \{0, 1\}^* \rightarrow \mathbb{G}_1$, $F_1 : \{0, 1\}^{k_2} \rightarrow \{0, 1\}^{k_1}$, $F_2 : \{0, 1\}^{k_1} \rightarrow \{0, 1\}^{k_2}$. The public parameters are $params = (g, g_1, g_2, d, H_1, H_2, H_3, F_1, F_2)$, the master secret key is x .

Extract: To generate private key for an attribute set ω ,

- First, randomly choose a $(d-1)$ degree polynomial $q(z)$ such that $q(0) = x$;
- Generate a new attribute set $\hat{\omega} = \omega \cup \Omega$. For each $i \in \hat{\omega}$, choose $r_i \in_R \mathbb{Z}_p$ and compute $d_{i0} = g_2^{q(i)} \cdot H_1(i)^{r_i}$ and $d_{i1} = g^{r_i}$;
- Finally, output $D_i = (d_{i0}, d_{i1})$ as the private key for each $i \in \hat{\omega}$.

Sign: Suppose one has private key for the attribute set ω . To sign a message m which length is equal to k_2 with predicate $\mathcal{Y}_{t, \hat{\omega}}(\cdot)$, namely, to prove owning at least t attributes among an n -element attribute set $\hat{\omega}$, he selects a t -element subset $\omega' \subseteq \omega \cap \hat{\omega}$ and selects randomly an element j from subset $\hat{\omega}/\omega'$, and proceeds as follows:

- First, select a default attribute subset $\Omega' \subseteq \Omega$ with $|\Omega'| = d - t$ and choose $(n + d - t - 1)$ random values $r'_i \in \mathbb{Z}_p^*$ for $i \in (\hat{\omega}/j) \cup \Omega'$, choose a random value $s \in \mathbb{Z}_p^*$;
- Compute $v = e(g_1, g_2)$;
- Compute $f = F_1(m) || (F_2(F_1(m)) \oplus m)$;
- Compute $r = H_2(v) + f$;
- Compute $\sigma_i = d_{i1}^{A_{i, s(0)}} \cdot g^{r'_i}$ for $i \in \omega' \cup \Omega'$;
- Compute $\sigma_i = g^{r_i}$ for $i \in \hat{\omega}/(\omega' \cup j)$;
- Compute $\sigma_j = g^s$;
- Compute $\sigma_0 = \left[\prod_{i \in \omega' \cup \Omega'} d_{i0}^{A_{i, s(0)}} \right] \cdot \left[\prod_{i \in (\hat{\omega} \cup \Omega')/j} H_1(i)^{r_i} \right] \cdot (H_1(j) \cdot H_3(r, \{\sigma_i\}_{i \in (\hat{\omega} \cup \Omega')/j}, \sigma_j))^s$;
- Finally, output the signature $\sigma = (r, \sigma_0, \{\sigma_i\}_{i \in (\hat{\omega} \cup \Omega')/j}, \sigma_j)$.

To sign a message m which length is shorter than k_2 , one can just pad spaces after the message until k_2 .

Verify: To verify the validity of a signature $\sigma = (r, \sigma_0, \{\sigma_i\}_{i \in (\hat{\omega} \cup \Omega')/j}, \sigma_j)$ with threshold t for attributes $\hat{\omega}$, the verifier performs the following verification procedure to recover the message m :

$$\frac{e(g, \sigma_0)}{\prod_{i \in \hat{\omega} \cup \Omega'} e(H_1(i), \sigma_i) \cdot e(\sigma_j, H_3(r, \{\sigma_i\}_{i \in (\hat{\omega} \cup \Omega')/j}, \sigma_j))} = v$$

$$r - H_2(v) = f.$$

Then, $m = [f]_{k_2} \oplus F_2([f]^{k_1})$ is recovered from f . The verifier checks whether the equation $[f]^{k_1} = F_1(m)$ holds. If it holds, output accept and the message m is recovered. Otherwise, output reject to denote the signature is not valid.

In the above computation, the subscript k_2 of f denotes the least significant k_2 bits of f , and the superscript k_1 of f denotes the most significant k_1 bits of f .

4.3 Security model

Existential unforgeability against chosen message attacks.

It can be defined using a game between an adversary and a challenger.

The adversary $\mathcal{A}$ knows the public key of the signer. Its goal is to forge a valid signature of a message m^* with a predicate $\mathcal{Y}_{t,\omega}(\cdot) \rightarrow 0/1$ that his attributes do not satisfy.

Firstly, challenger $\mathcal{C}$ runs the Setup algorithm to get the master secret key with respect to a security parameter and the system's public parameters $params$. Then, $\mathcal{C}$ sends $params$ to adversary $\mathcal{A}$. $\mathcal{A}$ can access polynomially bounded number of the following oracles.

H_1 Oracle: For H_1 hash query with respect to an attribute $i \in \mathbb{Z}_p^*$, $\mathcal{C}$ returns a hash value $H_1(i) \in_R \mathbb{G}_1$ corresponding to the attribute i .

H_3 Oracle: For H_3 hash query with respect to a tuple $(r, \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j)$ in which the first $r \in \mathbb{Z}_p^*$ and the rest elements all come from group $\mathbb{G}_1$, $\mathcal{C}$ returns a hash value $H_3(r, \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j) \in_R \mathbb{G}_1$ corresponding to the tuple $(r, \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j)$.

Extract Oracle: For Extract query with respect to an attribute set ω such that $|\bar{\omega} \cap \omega| < t$, $\mathcal{C}$ returns $D_i = (d_{i0}, d_{i1})$ for each $i \in \omega$ as the private key of attribute set ω .

Sign Oracle: For Sign query on arbitrary designated attribute set ω and arbitrary message m , $\mathcal{C}$ returns a valid signature σ with respect to m on behalf of the designated signer who possesses the attribute set ω .

Output: $\mathcal{A}$ outputs an alleged signature σ^* on message m^* on behalf of a user who possesses an attribute set ω^* such that $|\bar{\omega} \cap \omega^*| \geq t$. If no Sign queries of message m^* with an attribute set ω such that $|\bar{\omega} \cap \omega| \geq t$ and no Extract queries with respect to an attribute set ω such that $|\bar{\omega} \cap \omega| \geq t$ have been queried, $\mathcal{A}$ wins the game if the signature σ^* is valid.

If there is no such polynomial-time adversary $\mathcal{A}$ that can forge a valid signature in the game described above, we say this scheme is secure against existential forgery under chosen message attacks.

It is worth noting that this model also guarantees *collusion resistance*. This is because if a group of signers can cooperate to construct a signature that none of them could individually produce, then they can build another adversary which can forge a valid signature to win the above game.

Attribute privacy.

In an attribute-based signature scheme, a legitimate signer is indistinguishable among all the users whose attributes satisfying the predicate specified in the signature. The signature reveals nothing about the identity or attributes of the signer beyond what is explicitly revealed by the claim being made.

It can be defined using a game between an adversary and a challenger.

The adversary $\mathcal{A}$ even knows the master secret key. So he could generate all signer's private keys as well as public keys. Its goal is to distinguish between two signers which one generates the valid signature of a message with a predicate such that both of their attributes satisfy the predicate.

Firstly, challenger $\mathcal{C}$ runs the Setup algorithm to get the master secret key and the public parameters $params$. Then, $\mathcal{C}$ sends $params$ as well as the master secret key to adversary $\mathcal{A}$. $\mathcal{A}$ can access polynomially bounded number of $\mathbf{H}_1$ and $\mathbf{H}_3$ oracles which are the same as described in the previous game. $\mathcal{A}$ can generate private keys and signatures itself, because he has got the master secret key.

Challenge: $\mathcal{A}$ outputs a message m^* , two attribute sets ω_0^*, ω_1^* , and challenged attribute set ω^* for signature query, where $\omega^* \subseteq \omega_0^* \cap \omega_1^*$. $\mathcal{C}$ chooses $b \in \{0, 1\}$, computes the challenge signature σ^* on behalf of the signer who possesses attribute set ω^* selected from ω_b^* and provides σ^* to $\mathcal{A}$.

Guess: $\mathcal{A}$ tries to guess which attribute set between ω_0^* and ω_1^* is used to generate the challenge signature σ^* . Finally, $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$ and wins the game if $b' = b$.

If there is no such polynomial-time adversary $\mathcal{A}$ that can win the game described above, we say this scheme holds attribute privacy property.

It is worth noting that this property holds even for the attribute authority, because the master secret key is also given to the adversary.

4.4 Security analysis

Theorem 1. *This attribute-based signature with message recovery scheme is correct.*

Proof. The correctness of this scheme can be proven by straight-forward substitutions. $\square$

Theorem 2. *This attribute-based signature with message recovery scheme is existentially unforgeable under chosen message attacks in the random oracle model, under the assumption that the CDH problem is hard.*

Proof. Assume there is an algorithm $\mathcal{A}$ that can forge a valid signature under chosen message attacks. There will be another algorithm $\mathcal{B}$ that can run the algorithm $\mathcal{A}$ as a subroutine to solve the CDH problem.

We assume that the instance of the CDH problem consists of group elements $(g, g^x, g^y) \in \mathbb{G}_1^3$, and our goal is to compute an element $g^{xy} \in \mathbb{G}_1$.

Setup: Let the default attribute set be $\Omega = \{\Omega_1, \Omega_2, \dots, \Omega_{d-1}\}$. Since the threshold in our scheme is flexible from 1 to d , without loss of generality, we fix the threshold to $t \leq d$ in this proof. Firstly, $\mathcal{B}$ selects randomly a subset $\Omega' \subseteq \Omega$ with $|\Omega'| = d - t$. $\mathcal{B}$ selects g as the generator of $\mathbb{G}_1$, and sets $g_1 = g^x$ and $g_2 = g^y$.

$\mathbf{H}_1$ Queries: $\mathcal{B}$ creates and keeps one list H_1 -List to simulate H_1 Oracle. This list is used to store tuples like $(i, \alpha_i, H_1(i))$.

Upon receiving an H_1 hash query with respect to an attribute i , if this i is not included in this H_1 -List and $i \in \bar{\omega} \cup \Omega'$, $\mathcal{B}$ randomly selects a number $\alpha_i \in \mathbb{Z}_q^*$ and returns $H_1(i) = g^{\alpha_i}$ as the H_1 hash value of this i . Then, $\mathcal{B}$ records the tuple $(i, \alpha_i, g^{\alpha_i})$ in this H_1 -List. If this i is not included in this H_1 -List and $i \notin (\bar{\omega} \cup \Omega')$, $\mathcal{B}$ randomly selects a number $\alpha_i \in \mathbb{Z}_q^*$ and returns $H_1(i) = g_1^{-\alpha_i}$ as the H_1 hash value of this i . Then, $\mathcal{B}$ records the tuple $(i, \alpha_i, g_1^{-\alpha_i})$ in this H_1 -List. If the i is already in a record in this H_1 -List, $\mathcal{B}$ only returns the corresponding $H_1(i)$ in the record as the H_1 hash value.

H₃ Queries: $\mathcal{B}$ creates and keeps one list H_3 -List to simulate H_3 Oracle. This list is used to store tuples like

$$((r, \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j), \beta, H_3(r, \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j)).$$

Part of the records in this H_3 -List corresponding to the queries which are queried by the adversary $\mathcal{A}$. We will discuss this situation soon. The other part of the records in this H_3 -List corresponding to the queries which are conducted by the simulator $\mathcal{B}$ when $\mathcal{B}$ responds to the Sign queries. We will postpone to discuss this situation in the Sign Queries.

Upon receiving the k -th H_3 hash query which is conducted by the adversary $\mathcal{A}$ with respect to a tuple $(r, \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j)_k$, if this tuple is not included in this H_3 -List, $\mathcal{B}$ randomly selects a number $\beta_k \in \mathbb{Z}_q^*$ and returns $H_3((r, \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j)_k) = g^{\beta_k}$ as the H_3 hash value of this tuple. Then, $\mathcal{B}$ records $((r, \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j)_k, \beta_k, g^{\beta_k})$ in this H_3 -List. If the tuple is already in a record in this H_3 -List, $\mathcal{B}$ only returns the corresponding $H_3((r, \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j)_k)$ in the record as the H_3 hash value.

Extract Queries: $\mathcal{A}$ can make requests for private keys of attribute set ω such that $|\bar{\omega} \cap \omega| < t$. First define three sets Γ, Γ', S in the following manner: $\Gamma = (\omega \cap \bar{\omega}) \cup \Omega'$, Γ' such that $\Gamma \subseteq \Gamma' \subseteq S$ and $|\Gamma'| = d - 1$, and $S = \Gamma' \cup \{0\}$.

Similar to the case in the normal scheme, $\mathcal{B}$ should randomly choose a $(d - 1)$ degree polynomial $q(z)$ such that $q(0) = x$. We will show how $\mathcal{B}$ simulate private keys for attribute sets although $\mathcal{B}$ does not know exactly the value of x .

For $i \in \Gamma'$, $\mathcal{B}$ randomly selects two numbers $\tau_i, r_i \in \mathbb{Z}_p^*$. In this case, $\mathcal{B}$ assumes the value $q(i)$ corresponding to this i of the randomly chosen $(d - 1)$ degree polynomial $q(z)$ is $q(i) = \tau_i$. Then, $\mathcal{B}$ can compute D_i for $i \in \Gamma'$ as follows:

$$D_i = (g_2^{q(i)} \cdot H_1(i)^{r_i}, g^{r_i}) = (g_2^{\tau_i} \cdot H_1(i)^{r_i}, g^{r_i})$$

For $i \notin \Gamma'$, $\mathcal{B}$ looks up the H_1 -List which is created by H_1 Oracle to find the record about attribute i and get the corresponding α_i . $\mathcal{B}$ randomly selects a number $r'_i \in \mathbb{Z}_p^*$, and let

$$r_i = \frac{\Delta_{0,S}(i)}{\alpha_i} y + r'_i$$

We will show how $\mathcal{B}$ simulate private keys for attribute $i \notin \Gamma'$ although $\mathcal{B}$ does not know exactly the value of y . In case of the values $q(i)$ for $i \in \Gamma'$ are determined in the previous stage, $\mathcal{B}$ can compute the value $q(i)$ corresponding to

$i \notin \Gamma'$ of the randomly chosen $(d-1)$ degree polynomial $q(z)$ by using Lagrange interpolation as

$$q(i) = \sum_{j \in \Gamma'} \Delta_{j,S}(i) \cdot q(j) + \Delta_{0,S}(i) \cdot q(0)$$

in which $q(0) = x$. Then, $\mathcal{B}$ can compute D_i for $i \notin \Gamma'$ as follows:

$$\begin{aligned} D_i &= (g_2^{q(i)} \cdot H_1(i)^{r_i}, g^{r_i}) \\ &= (g_2^{\sum_{j \in \Gamma'} \Delta_{j,S}(i) \cdot q(j)} \cdot (g_1^{-\alpha_i})^{r'_i}, g_2^{\frac{\Delta_{0,S}(i)}{\alpha_i}} \cdot g^{r'_i}) \end{aligned}$$

although $\mathcal{B}$ does not know exactly the value of x and y .

$\mathcal{B}$ returns D_i for each $i \in (\omega \cup \Omega)$ as the private key of ω .

Sign Queries: For a Sign query on message m with respect to an attribute set ω . If $|\bar{\omega} \cap \omega| < t$, $\mathcal{B}$ can get a simulated private key with respect to ω by querying the Extract Oracle, and compute a signature on message m with respect to ω normally.

If $|\bar{\omega} \cap \omega| \geq t$, $\mathcal{B}$ selects a t -element subset $\omega' \subseteq \bar{\omega} \cap \omega$ and selects randomly an element j from subset $\bar{\omega}/\omega'$, and simulates the signature as follows:

Firstly, $\mathcal{B}$ selects a random $(d-t)$ -element subset Ω' from Ω . Then, $\mathcal{B}$ chooses two random numbers r_i and r'_i for each $i \in \omega' \cup \Omega'$, and let $r'_i = r_i \cdot \Delta_{i,S}(0) + r''_i$. It is obviously that r'_i is still a random number for each $i \in \omega' \cup \Omega'$. $\mathcal{B}$ also chooses random number r'_i for each $i \in \bar{\omega}/(\omega' \cup j)$. $\mathcal{B}$ also chooses two random values $\beta_h, s' \in \mathbb{Z}_p^*$ and let $s = \frac{1}{\beta_h}y + s'$ which is also a random number because β_h and s' are randomly chosen. We will show how $\mathcal{B}$ simulate a correct signature although $\mathcal{B}$ does not know exactly the value of y .

Firstly, $\mathcal{B}$ computes every part except for σ_0 by using previous parameters as in the normal scheme, and inserts a record $((r, \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j)$,

$$\beta_h, g_1^{-\beta_h}) \text{ in the } H_3\text{-List. Then, } \mathcal{B} \text{ computes } \sigma_0 = g_2^x \cdot \left[\prod_{i \in (\bar{\omega} \cup \Omega')/j} H_1(i)^{r'_i} \right] \cdot H_1(j)^s \cdot H_3(r, \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j)^s = g_1^{-\beta_h s'} \cdot (g_2^{\frac{\alpha_j}{\beta_h}} \cdot g^{\alpha_j s'}) \cdot \left[\prod_{i \in (\bar{\omega} \cup \Omega')/j} H_1(i)^{r'_i} \right]$$

We will show this simulated σ_0 have the same form as in the normal scheme as follows:

$$\begin{aligned} \sigma_0 &= g_2^x \cdot \left[\prod_{i \in (\bar{\omega} \cup \Omega')/j} H_1(i)^{r'_i} \right] \cdot (H_1(j) \cdot H_3(r, \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j))^s \\ &= \prod_{i \in \omega' \cup \Omega'} (g_2^{q(i)} \cdot H_1(i)^{r_i})^{\Delta_{i,S}(0)} \cdot \prod_{i \in \omega' \cup \Omega'} H_1(i)^{r''_i} \cdot \prod_{i \in \bar{\omega}/(\omega' \cup j)} H_1(i)^{r'_i} \\ &\quad \cdot (H_1(j) \cdot H_3(r, \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j))^s \end{aligned}$$

Compared with a signature generated from the normal scheme, we will find out that this simulated signature can be regarded as a normal signature which is generated by a signer who possesses private keys $D_i = (g_2^{q(i)} \cdot H_1(i)^{r_i}, g^{r_i})$ for attribute $i \in \omega' \cup \Omega'$ in which $q(z)$ is a random $(d-1)$ degree polynomial such

that $q(0) = x$. It is worth noting that although r_i'' and r_i' are not the same form at the first glance, they are indeed the same form because both of r_i'' and r_i' are random numbers. So the two parts $\prod_{i \in \omega' \cup \Omega'} H_1(i)^{r_i''}$ and $\prod_{i \in \bar{\omega}/(\omega' \cup j)} H_1(i)^{r_i'}$ can be merged into one part as $\prod_{i \in (\bar{\omega} \cup \Omega')/j} H_1(i)^{r_i'}$ in the normal scheme.

Verify: While $|\bar{\omega} \cap \omega| < t$, the simulated signature on message m with respect to ω is computed by querying the Extract Oracle to get a simulated private key with respect to ω normally. It will certainly pass the normal verification process. While $|\bar{\omega} \cap \omega| \geq t$, we can check that the simulated signature can also pass the normal verification process by straight-forward substitutions.

Finally, The adversary outputs a forged signature σ^* on message m^* for attribute set ω^* such that $|\bar{\omega} \cap \omega^*| \geq t$. It satisfies the verification equation, which means that

$$\sigma^* = \{r^*, g_2^x \cdot \left[\prod_{i \in (\bar{\omega} \cup \Omega')/j} H_1(i)^{r_i'} \right] \cdot H_1(j)^s \cdot H_3(r^*, \{\sigma_i^*\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j^*)^s, \{g^{r_i'}\}_{i \in (\bar{\omega} \cup \Omega')/j}, g^s\}.$$

Then, $\mathcal{B}$ can compute

$$\frac{\sigma_0^*}{\prod_{i \in (\bar{\omega} \cup \Omega')/j} (\sigma_i^*)^{\alpha_i} \cdot (\sigma_j^*)^{\alpha_j} \cdot (\sigma_j^*)^{\beta_k}} = g^{xy}.$$

So, $\mathcal{B}$ can solve an CDH problem if $\mathcal{A}$ is able to forge valid signatures.

If there is no such polynomial-time adversary that can forge a valid attribute-based signature with a predicate that his attributes do not satisfy, we say that this attribute-based signature with message recovery scheme is secure against existential forgery under chosen message attacks. $\square$

Theorem 3. *This attribute-based signature with message recovery scheme is equipped with the attribute privacy property in the random oracle model.*

Proof. Setup: First, a $(d - 1)$ default attribute set from $\mathbb{Z}_p^*$ is given as $\Omega = \{\Omega_1, \Omega_2, \dots, \Omega_{d-1}\}$ for some predefined integer d . $\mathcal{C}$ selects a random generator $g \in \mathbb{G}_1$, a random $x \in \mathbb{Z}_p^*$ as the master secret key, and set $g_1 = g^x$. Next, $\mathcal{C}$ picks a random element $g_2 \in \mathbb{G}_1$. $\mathcal{C}$ sends these public parameters $params$ as well as the master secret key x to adversary $\mathcal{A}$.

Both of the $\mathbf{H}_1$ oracle and $\mathbf{H}_3$ oracle are the same as described in Theorem 2.

Challenge: The adversary outputs two attribute sets ω_0^* and ω_1^* . Both the adversary $\mathcal{A}$ and the challenger $\mathcal{C}$ can generate secret keys corresponding to these two attribute sets as D_i^0 for $i \in \omega_0^* \cup \Omega$ and D_i^1 for $i \in \omega_1^* \cup \Omega$ respectively. Then, the adversary outputs a message m^* and a t -element challenge attribute subset $\omega^* \subseteq \omega_0^* \cap \omega_1^*$. The adversary $\mathcal{A}$ asks the challenger to generate a signature on message m^* with respect to ω^* from either ω_0^* or ω_1^* . The challenger $\mathcal{C}$ chooses a random bit $b \in \{0, 1\}$, a $(d - t)$ -element subset $\Omega' \subseteq \Omega$, and outputs a signature

$\sigma^* = \{r^*, \sigma_0^*, \{\sigma_i^*\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j^*\}$ by running algorithm which is described as the Sign oracle in Theorem 2 using the secret key D_i^b for $i \in \omega_b^* \cup \Omega$.

As we have mentioned in Theorem 2, part of the signature σ_0^* can be written as

$$\prod_{i \in \omega^* \cup \Omega'} (g_2^{q(i)} \cdot H_1(i)^{r_i})^{\Delta_{i,S}(0)} \cdot \prod_{i \in \omega^* \cup \Omega'} H_1(i)^{r_i''} \cdot \prod_{i \in \bar{\omega}/(\omega^* \cup j)} H_1(i)^{r_i'} \cdot (H_1(j) \cdot H_3(r, \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j))^s, \sigma_i$$
 for $i \in \omega^* \cup \Omega'$ can be written as $\sigma_i = (g^{r_i})^{\Delta_{i,S}(0)} \cdot g^{r_i''} = g^{r_i \cdot \Delta_{i,S}(0) + r_i''} = g^{r_i'}$.

So, the challenge signature can be regarded as generated by a signer who possesses private keys $D_i = (g_2^{q(i)} \cdot H_1(i)^{r_i}, g^{r_i})$ for attributes $i \in \omega^* \cup \Omega'$ in which $q(z)$ is a random $(d-1)$ degree polynomial such that $q(0) = x$. Thus, if this challenge signature is generated by using the secret key D_i^0 for $i \in \omega_0^* \cup \Omega$, it can also be generated by using the secret key D_i^1 for $i \in \omega_1^* \cup \Omega$ since the secret key D_i^1 for $i \in \omega_1^* \cup \Omega$ also satisfy the situation mentioned above. Similarly, if this challenge signature is generated by using the secret key D_i^1 for $i \in \omega_1^* \cup \Omega$, it can also be generated by using the secret key D_i^0 for $i \in \omega_0^* \cup \Omega$.

Therefore, even the adversary has access to the master secret key and has unbounded computation ability, he cannot distinguish between two signers which one generates a valid signature of a message with a predicate such that both of their attributes satisfy the predicate. $\square$

5 Extended Scheme

In order to deal with messages which are larger than k_2 , we can extend the previous scheme as follows.

Setup: The Setup algorithm is same as in the previous scheme.

Extract: The Extract algorithm is also same as in the previous scheme.

Sign: Suppose one has private key for the attribute set ω . To sign a message m which length is larger than k_2 with predicate $\Upsilon_{t,\bar{\omega}}(\cdot)$, namely, to prove owning at least t attributes among an n -element attribute set $\bar{\omega}$, he selects a t -element subset $\omega' \subseteq \omega \cap \bar{\omega}$ and selects randomly an element j from subset $\bar{\omega}/\omega'$, and proceeds as follows:

- First, separate the message m into two parts $m = m_1 || m_2$, and let the length of m_1 be k_2 .
- Select a default attribute subset $\Omega' \subseteq \Omega$ with $|\Omega'| = d - t$ and choose $(n + d - t - 1)$ random values $r_i' \in \mathbb{Z}_p^*$ for $i \in (\bar{\omega}/j) \cup \Omega'$, choose a random value $s \in \mathbb{Z}_p^*$;
- Compute $v = e(g_1, g_2)$;
- Compute $f = F_1(m_1) || (F_2(F_1(m_1)) \oplus m_1)$;
- Compute $r = H_2(v) + f$;
- Compute $c = H_2(r, m_2)$;
- Compute $\sigma_i = d_{i1}^{\Delta_{i,S}(0)} \cdot g^{r_i'}$ for $i \in \omega' \cup \Omega'$;
- Compute $\sigma_i = g^{r_i'}$ for $i \in \bar{\omega}/(\omega' \cup j)$;
- Compute $\sigma_j = g^s$;

- Compute $\sigma_0 = \left[\prod_{i \in \omega' \cup \Omega'} d_{i0}^{\Delta_{i,S}(0)} \right] \cdot \left[\prod_{i \in (\bar{\omega} \cup \Omega')/j} H_1(i)^{r'_i} \right] \cdot (H_1(j) \cdot H_3(c, \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j))^s$;
- Finally, output the signature $\sigma = (m_2, r, \sigma_0, \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j)$.

Verify: To verify the validity of a signature $\sigma = (m_2, r, \sigma_0, \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j)$ with threshold t for attributes $\bar{\omega}$, the verifier performs the following verification procedure to recover the message m_1 :

$$\frac{e(g, \sigma_0)}{\prod_{i \in \bar{\omega} \cup \Omega'} e(H_1(i), \sigma_i) \cdot e(\sigma_j, H_3(H_2(r, m_2), \{\sigma_i\}_{i \in (\bar{\omega} \cup \Omega')/j}, \sigma_j)))} = v$$

$$r - H_2(v) = f.$$

Then, $m_1 = [f]_{k_2} \oplus F_2([f]^{k_1})$ is recovered from f . The verifier checks whether the equation $[f]^{k_1} = F_1(m_1)$ holds. If it holds, output accept. Then the verifier combines $m = m_1 || m_2$ and the message m is recovered. Otherwise, output reject to denote the signature is not valid.

In the above computation, the subscript k_2 of f denotes the least significant k_2 bits of f , and the superscript k_1 of f denotes the most significant k_1 bits of f .

Theorem 4. *This extended attribute-based signature with message recovery scheme is correct.*

Proof. Correctness can be verified similarly with the above attribute-based signature with message recovery scheme in Theorem 1. $\square$

Theorem 5. *This extended attribute-based signature with message recovery scheme is existentially unforgeable under chosen message attacks in the random oracle model, under the assumption that the CDH problem is hard.*

Proof. This proof is similar to the proof of Theorem 2 and therefore it is omitted. $\square$

Theorem 6. *This extended attribute-based signature with message recovery scheme is equipped with the attribute privacy property in the random oracle model.*

Proof. This proof is similar to the proof of Theorem 3 and therefore it is omitted. $\square$

6 Conclusion

We proposed a new notion of attribute-based signature with message recovery, and presented two concrete attribute-based signature with message recovery schemes based on bilinear pairing that support flexible threshold predicates. The first scheme allows the signer to embed the original message in the signature without the need of sending the original message to the verifier, while

keeping the same signature size. The original message can be recovered from the signature. Therefore, our first scheme minimizes the total length of the original message and the appended signature. The second scheme is extended from the first scheme in order to deal with large messages. These schemes have been proven to be existentially unforgeable against adaptively chosen message attacks in the random oracle model under the assumption that the CDH problem is hard. These schemes have also been proven to have the attribute privacy property.

References

1. M. Gagné, S. Narayan, and R. Safavi-Naini. Short pairing-efficient threshold-attribute-based signature. In *Pairing-Based Cryptography—Pairing 2012*, pages 295–313. Springer, 2013.
2. D. Khader. Attribute based group signature with revocation. *IACR Cryptology ePrint Archive*, 2007:241, 2007.
3. D. Khader. Attribute based group signatures. *IACR Cryptology ePrint Archive*, 2007:159, 2007.
4. D. Khader. Authenticating with attributes. *IACR Cryptology ePrint Archive*, 2008:31, 2008.
5. J. Li, M. H. Au, W. Susilo, D. Xie, and K. Ren. Attribute-based signature and its applications. In *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, pages 60–69. ACM, 2010.
6. J. Li and K. Kim. Attribute-based ring signatures. *IACR Cryptology ePrint Archive*, 2008:394, 2008.
7. H. K. Maji, M. Prabhakaran, and M. Rosulek. Attribute-based signatures: Achieving attribute-privacy and collusion-resistance. *IACR Cryptology ePrint Archive*, 2008:328, 2008.
8. H. K. Maji, M. Prabhakaran, and M. Rosulek. Attribute-based signatures. In *Topics in Cryptology—CT-RSA 2011*, pages 376–392. Springer, 2011.
9. K. Nyberg and R. Rueppel. A new signature scheme based on the dsa giving message recovery. In *Proceedings of the 1st ACM conference on Computer and communications security*, pages 58–61. ACM, 1993.
10. S. F. Shahandashti and R. Safavi-Naini. Threshold attribute-based signatures and their application to anonymous credential systems. In *Progress in Cryptology—AFRICACRYPT 2009*, pages 198–216. Springer, 2009.
11. A. Shamir. Identity-based cryptosystems and signature schemes. In *Advances in cryptology*, pages 47–53. Springer, 1985.
12. G. Shaniqng and Z. Yingpei. Attribute-based signature scheme. In *Information Security and Assurance, 2008. ISA 2008. International Conference on*, pages 509–511. IEEE, 2008.
13. P. Yang, Z. Cao, and X. Dong. Fuzzy identity based signature. *IACR Cryptology ePrint Archive*, 2008:2, 2008.
14. F. Zhang, W. Susilo, and Y. Mu. Identity-based partial message recovery signatures (or how to shorten id-based signatures). *Financial Cryptography and Data Security*, pages 578–578, 2005.