2012

Attribute-Based Oblivious Access Control

Jinguang Han
*University of Wollongong*

Willy Susilo
*University of Wollongong, wsusilo@uow.edu.au*

Yi Mu
*University of Wollongong, ymu@uow.edu.au*

Jun Yan
*Hokai University, China, jyan@uow.edu.au*

Publication Details


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 Oblivious Access Control

Abstract
In an attribute-based system (ABS), users are identified by various attributes, instead of their identities. Since its seminal introduction, the attribute-based mechanism has attracted a lot of attention. However, current ABS schemes have a number of drawbacks: (i) the communication cost is linear in the number of the required attributes; (ii) the computation cost is linear in the number of the required attributes and (iii) there are no efficient verification algorithms for the secret keys. These drawbacks limit the use of ABS in practice. In this paper, we propose an attribute-based oblivious access control (ABOAC) scheme to address these problems, where only the receiver whose attributes satisfy the access policies can obtain services obliviously. As a result, the receiver does not release anything about the contents of the selected services and his attributes to the sender, and even the number and supersets of his attributes are protected. The sender only knows the number of the services selected by the authorized receiver. Notably, the costs of computation and communication are constant and independent of the number of required attributes. While, in the prior comparable schemes, both the costs of computation and communication are linear in the required attributes. Therefore, our ABOAC scheme provides a novel and elegant solution to protect user's privacy in the systems where both the bandwidth and the computing capability are limited, such as wireless sensor and actor networks, mobile ad hoc networks, etc.

Disciplines
Physical Sciences and Mathematics

Publication Details

This journal article is available at Research Online: http://ro.uow.edu.au/infopapers/2074
Attribute-Based Oblivious Access Control

JINGUANG HAN1,3*, WILLY SUSILO1, YI MU1 AND JUN YAN2

1Centre for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW 2522, Australia
2School of Information Systems and Technology, University of Wollongong, Wollongong, NSW 2522, Australia
3College of Sciences, Hohai University, Nanjing 210098, China
*Corresponding author: jh843@uowmail.edu.au

In an attribute-based system (ABS), users are identified by various attributes, instead of their identities. Since its seminal introduction, the attribute-based mechanism has attracted a lot of attention. However, current ABS schemes have a number of drawbacks: (i) the communication cost is linear in the number of the required attributes; (ii) the computation cost is linear in the number of the required attributes and (iii) there are no efficient verification algorithms for the secret keys. These drawbacks limit the use of ABS in practice. In this paper, we propose an attribute-based oblivious access control (ABOAC) scheme to address these problems, where only the receiver whose attributes satisfy the access policies can obtain services obliviously. As a result, the receiver does not release anything about the contents of the selected services and his attributes to the sender, and even the number and supersets of his attributes are protected. The sender only knows the number of the services selected by the authorized receiver. Notably, the costs of computation and communication are constant and independent of the number of required attributes. While, in the prior comparable schemes, both the costs of computation and communication are linear in the required attributes. Therefore, our ABOAC scheme provides a novel and elegant solution to protect user’s privacy in the systems where both the bandwidth and the computing capability are limited, such as wireless sensor and actor networks, mobile ad hoc networks, etc..

Keywords: attribute-based system; access control; oblivious transfer; privacy

Received 7 February 2012; revised 11 April 2012
Handling editor: Chris Mitchell

1. INTRODUCTION

Access control is usually designed to determine which resources can be accessed by the authorized users. In order to access a resource, a user must authenticate himself to a trusted third party (TTP) to be granted an access permission. Considering different access requirements, various access control protocols have been proposed to protect sensitive resources, such as discretionary access control [1], mandatory access control [2], attribute-based access control (ABAC) [3–7], role-based access control [8–10], purpose-based access control [11, 12] and hierarchical access control [13, 14].

In an ABAC system, an access request is accepted or denied depending upon whether the attributes of the requester satisfy the access policies. The ‘magic’ of ABAC not only lies in its high flexibility and strong expressibility, but also in its anonymity. For example, Jack associates a service with a set of attributes $S = \{\text{European}, \text{Adult}, \text{Student}\}$ such that only the user whose attributes includes $S$ can access the service. Suppose that two users Alice and Bob hold attribute $S_A = \{\text{European}, \text{Married}, \text{Adult}, \text{Student}\}$ and $S_B = \{\text{European}, \text{Adult}, \text{Vegetarian}, \text{Student}\}$, respectively. Jack cannot decide whether the service is obtained by Alice or Bob, because both of them are authorized to access the service. What Jack knows is $S \subseteq S_A$ and $S \subseteq S_B$. Therefore, Jack cannot identify the identity of the real receiver from the required attributes. This implies that ABAC can provide anonymity to users.

Although attribute-based systems are flexible, the computation cost and communication cost are linear in the number of the required attributes. Current ABAC schemes are not suitable to the system with limited communication and computation ability, such as wireless sensor and actor networks (WSANs) and mobile ad hoc networks (MANETs). In WSANs,
the sensors are lower price and lower power devices with limited sensing, computation and wireless communication ability [15]. The nodes in MANETs have limited power, computation ability and small memory space [16]. Therefore, it is an interesting and challenging work to construct an ABAC scheme where both the communication cost and the computation cost are constant.

1.1. Related work

Being different from an identity-based encryption (IBE) [17–20], attribute-based encryption (ABE) provides a sound solution to encrypt a message for all users who hold the required attributes, without any knowledge of their exact identities. The first ABE scheme was proposed by Sahai and Waters [21] based on linear secret sharing [22], where both the ciphertext and the secret key are labeled with a set of attributes. A user can decrypt the ciphertext if and only if there is a match between his secret key and the ciphertext. This idea was originally used to design an error-tolerant (or fuzzy) IBE. There are two types of ABE: Key-Policy ABE (KP-ABE) and Cipher-Policy ABE (CP-ABE).

(i) In a KP-ABE scheme, the ciphertext is labeled with a set of attributes; while the secret keys of the user are associated with an access policy (access structure). A user can decrypt the ciphertext, if and only if he has obtained the required secret keys corresponding to attributes listed in the ciphertext [21, 23, 24].

(ii) In a CP-ABE scheme, the ciphertext is associated with an access policy (access structure); while the secret keys of the user are labeled with a set of attributes. A user can decrypt the ciphertext, if and only if his attributes satisfy the access policy [25–29].

To obtain the fine-grained access, Goyal et al. [23] proposed a new ABE scheme, where access trees were exploited. There is a threshold gate in each non-leaf node of the tree, which consists of its children and a threshold value. Each leaf is associated with an attribute. Both ABE schemes in [21, 23] are monotonic, namely Alice, who holds a set of attributes $S_A$, can decrypt a ciphertext, then Bob, who holds a set of attributes $S_B$, can decrypt the ciphertext, if and only if $S_A \subseteq S_B$.

Two non-monotonic ABE schemes were proposed by Ostrovsky et al. [24] and Cheung and Newport [26], respectively. In these schemes, negative attributes are considered. Comparatively, non-monotonic ABE can express more complicated access policies than monotonic ABE [24]. The former is referred to as KP-ABE, while the latter CP-ABE.

Goyal et al. [30] proposed a bounded CP-ABE, where the access tree is bounded. This bound is determined in the system setup phase, and is represented by the maximum depth of the tree and the maximum number of children that each non-leaf node in the tree has. Any access tree that satisfies the upper bound can be selected by the encryptor to encrypt messages [31].

Attrapadung and Imai [32] proposed a new variant of ABE called dual-policy ABE which combines KP-ABE with CP-ABE. There are two access structures. One is over the subjective attributes held by the user, and the other is over the objective attributes ascribed to the encrypted data. Nevertheless, there is only one access structure in both KP-ABE and CP-ABE schemes.

In their seminal paper, Sahai and Waters [21] questioned how to construct ABE schemes with multi-authorities, to ensure the practicality of ABE. Chase [33] answered this question affirmatively by proposing an ABE scheme with multi-authorities. In this scheme, the user is required to obtain his secret keys from some of the distributed authorities. This scheme can be used to resist the attack from the untrusted authority.

One intrinsic flaw of ABE is that the length of the ciphertext is linear in the number of the required attributes in both KP-ABE and CP-ABE. Solutions towards reducing the length of the ciphertext have been proposed. Although the computational costs of the encryption algorithms in these schemes are constant, the exponential and pairing operations executed in the decryption stage are linear in the number of the required attributes. Therefore, these schemes are not an ideal primitive for the systems where the receiver only has limited computing ability (such as WSANs, MANETs, etc.). To name a few, Herranz et al. [27] proposed a threshold ABE with constant ciphertext. This scheme was based on the threshold public-key encryption proposed by Delerablée and Pointcheval [34]. For each attribute, there exists a secret key. Before decryption, the user must aggregate all his secret keys to one value, by using the algorithm Aggregate introduced in [35]. As mentioned in [35], the running time of the algorithm Aggregate is about $(y(y - 1)/2T_{exp})$, where $y$ and $T_{exp}$ denote the number of the attributes and the running time of one exponentiation, respectively. Zhou and Huang [36] proposed a CP-ABE scheme with constant ciphertext based on the $q$-decisional bilinear Diffie-Hellman exponential ($q$-DBDHE) assumption. The computational cost of the encryption algorithm is constant, while the pairing operations in the decryption stage is linear in the number of the required attributes. Emura et al. [37] also proposed an CP-ABE scheme with constant ciphertext, where for a set of attributes, there is only one secret key. In this scheme, a user can only decrypt the ciphertext that requires the exact attributes which he holds. The user cannot decrypt the ciphertext where the required attributes are included in his attributes, because the user cannot use his attributes separately. From this point, this scheme is more like an IBE scheme, where all the held attributes can be mapped into the sole identity of the user. Attrapadung et al. [38] proposed a KP-ABE scheme with constant ciphertext. Whereas, both the exponential and the pairing operations executed in the decryption phase are linear in the number of the required attributes.

Recently, Chen et al. [39] proposed a non-monotonic CP-ABE scheme with constant ciphertext and constant computation cost. Both [38, 39] are based on non-standard assumption, namely $q$-DBDHE assumption.
ABE schemes based on linear secret key sharing scheme [22] are subject to collusion attack. This attack was defined by Sahai and Waters [21]. Referring back to the example described in the beginning, suppose that Alice holds a set of attributes $\delta_A = \{\text{European, Student}\}$, and Bob holds a set of attributes $\delta_B = \{\text{American, Adult}\}$. If Alice and Bob collude, they can collaborate to get attributes $S = \{\text{European, Adult, Student}\}$ to access the source. An ABE scheme is secure against the collusion attacks, if multiple users collude, they can only decrypt the ciphertext which one of them can decrypt by himself.

In an ABE scheme, a user is required to obtain a secret key for each attribute of him. Generally speaking, the user can decrypt a ciphertext by using a subset of his secret keys. If the received secret keys cannot be verified, it is hard to guarantee that the secret keys are generated correctly and not tampered. In the scenario that the user cannot decrypt a ciphertext when his attributes satisfy the access policies, he cannot determine which secret keys caused this. He also cannot detect whether his secret keys or the ciphertext are not constructed correctly. Especially, if the issuer and the encrypter are different entities, the user cannot detect who is malicious. This will risk the user’s access right. Meanwhile, most of the previous schemes did not provide a verification algorithms for the secret keys.

Although anonymity can be used to protect the privacy of users, it is unfortunately insufficient [40]. This is because anonymity can hide who the user is, but it cannot hide what actions the user performed. For instance, suppose that a user can access resources anonymously. We cannot identify who he/she is, but we can guess that it is Alice with high probability, if it can access Alice’s medical data, financial condition and insurance records. Hence, in terms of privacy, we require a system to hide both the identity of the user and the actions performed.

Proposed by Rabin [41], $k$-out-of-$m$ oblivious transfer (OT\textsuperscript{k\_m}) is a protocol where the sender and the receiver have a set of messages $\mathcal{M} = \{M_1, M_2, \ldots, M_n\}$ and a set of choices $\mathcal{C} = \{\sigma_1, \sigma_2, \ldots, \sigma_k\} \subseteq \{1, 2, \ldots, m\}$, respectively. After a transfer, the receiver can obtain messages $\{M_{\sigma_1}, M_{\sigma_2}, \ldots, M_{\sigma_k}\}$, while the sender knows nothing about the receiver’s choices. Adaptive $k$-out-of-$m$ oblivious transfer (OT\textsuperscript{m\_k\_x}) is a strongly secure OT, where the receiver can obtain messages from the sender adaptively [42, 43]. OT has been used as a primitive to hide users’ actions [44–46].

Friken et al. [5] proposed three ABAC schemes, where both the access policies and the attributes of the receiver can be hidden. In the first scheme, the receiver knows a superset of the attributes required by the access policy. In the second scheme, the receiver knows the number of the attributes that he satisfies. While, in the third scheme, the receiver only knows the upper bound of the attributes that he can use to access the system. The sender knows the number of attributes that the receiver uses to access the system, and nothing else. They based their scheme on homomorphic encryption [47], 1-out-of-2 oblivious transfer [41] and set intersection [48]. Their schemes provided a sound solution to protect users’ privacy. One pitiable thing of their schemes is their efficiency. The communication complexity in these three schemes are $O(n)$, $O(\gamma n)$ and $O(\gamma)$, respectively, where $n$ is the number of the attributes listed in the access policies, and $\gamma$ is the number of the attributes held by the user. For each attribute listed in the access policy, the encryption operations required in these schemes are $O(1)$, $O(\gamma)$ and $O(\gamma)$, respectively. The interactions for each attribute are three rounds, five rounds and five rounds, respectively. And also, the cost of computation will depend on the exploited encryption scheme and the OT scheme.

Coul et al. [45] proposed an oblivious transfer with access control (AC-OT) scheme by introducing an anonymous credential scheme to an OT scheme, where the access policy is a state graph. Each node in the graph is a state, and each edge denotes a transaction from one state to another. For each access to the database, the user must prove he has obtained the required credentials (attribute) in zero-knowledge. Camenisch et al. [46] proposed another AC-OT scheme that improved Coull et al. [45] scheme. This scheme avoids to re-issue credentials at each transfer by following two approaches. In the first approach, they assign a state to a subset of attributes that a user can access to, with a self-loop which can be accessed using this subset of attributes. In the second approach, they assign a state to a subset of attributes which are published as the access policy, with a self-loop for each data which is associated with this subset of attributes. Let $|\mathcal{S}_C|$ denote that the number of the attributes required by the $i$th record (data), for $i = 1, 2, \ldots, m$. For a set of choices $\mathcal{C} = \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$, the computational cost and communication cost in these two schemes are $O(\sum_{i=1}^{\ell} |\mathcal{S}_{C_i}|)$ and $O(m)$, respectively.

Zhang et al. [49] proposed a new AC-OT scheme which is based on the CP-ABE scheme [28] and OT\textsuperscript{e} scheme [50]. As mentioned in [29], the CP-ABE scheme [28] constructed in the composite order $(N = p_1 p_2 p_3)$ bilinear groups is not efficient, where $p_1$, $p_2$ and $p_3$ are different prime numbers. This scheme has the ciphertext which is linear in the number of the required attributes. Both the exponential and the pairing operations executed in the decryption stage are linear in the number of the required attributes. Furthermore, in order to introduce the CP-ABE scheme [40] to OT\textsuperscript{e} scheme [50], a data encapsulated mechanism must be employed to encrypt the messages from different message spaces. Hence, the computational cost and communication cost in this scheme are $O(\sum_{i=1}^{\ell} |\mathcal{S}_{C_i}|)$ and $O(\sum_{i=1}^{m} |\mathcal{S}_C|)$, respectively.

Rial and Preneel [51] proposed a blind ABE and an AC-OT scheme by providing a blind key extract protocol for the CP-ABE scheme [25]. CP-ABE scheme [25] was proved to be secure in the generic group model, instead of reducing to a complexity assumption. The ciphertext text and the computing cost in the decryption stage in the CP-ABE scheme [25] are linear in the number of the required attributes. Therefore, the computational cost and communication cost in this scheme are $O(\sum_{i=1}^{\ell} |\mathcal{S}_{C_i}|)$ and $O(\sum_{i=1}^{m} |\mathcal{S}_C|)$, respectively.
1.2. Our contribution

An ABE scheme is more efficient and it can express a fine-grained access structure. An OT scheme is a primitive used to protect the action performed by the user. Hence, the combination of ABE and OT schemes provide a sound solution to protect user’s privacy in an access control mechanism, especially, in the privacy-sensitive systems, such as medical records, patent searches, etc. However, the computational cost and communication cost in the existing schemes are linear in the number of the required attributes. It is a challenging work to construct an attribute-based oblivious access control (ABOAC) scheme where both the computation cost and communication cost are independent of the number of the required attributes. This is necessary in the systems where both the computing cost and communication cost are limited, such as WSANs [15], MANETs [16], etc.

In this paper, we propose an ABE scheme with constant ciphertext. We note that both the encryption and decryption algorithms in our scheme are very efficient. For an encryption and decryption procedure, only three exponentiations and two pairing operations are executed, respectively. This is in contrast to the previous ABE schemes where the numbers of pairings and exponentiations executed in the encryption and decryption phases are linear in the number of the required attributes. Additionally, the secret key for each attribute can be efficiently verified. Further, we extend our ABE scheme to an ABOAC scheme, where the user can obtain services obliviously, if his attributes satisfy the access policies. As a result, the receiver releases nothing about his attributes and the selected services to the sender. The sender only knows the number of the selected services. Hence, both the identity of the receiver and the actions performed by him can be protected. In our ABOAC scheme, for each service encrypted with the required attributes, only one-round interaction is executed between the sender and the receiver. The sender is required to execute three exponential operations, and the receiver needs to execute two pairing and two exponential operations.

1.3. Paper organization

The remainder of this paper is organized as follows. In Section 2, we review the preliminaries that are used throughout this paper. A new ABE with constant communication cost and computation cost is proposed, and proved in Section 3. In Section 4, based on the ABE proposed in Section 3, an ABOAC scheme is proposed and proved. Section 5 concludes this paper.

2. PRELIMINARIES

In this section, we introduce the definitions and security models of ABE and ABOAC. Then, the complexity assumptions used throughout this paper are reviewed.

2.1. Attribute-based encryption

In the rest of this paper, by \( a \overset{R}{\leftarrow} A \), we denote that \( a \) is selected at random from \( A \). Especially, by \( a \overset{\Phi}{\leftarrow} A \), we denote that \( a \) is selected uniformly from \( A \), if \( A \) is a finite set. By \( R \overset{\Phi}{\rightarrow} S \) and \( R \overset{\phi}{\rightarrow} S \), we denote that party \( S \) sends \( \Phi \) to party \( R \) and party \( R \) sends \( \phi \) to party \( S \), respectively. If \( S \) is a finite set, we denote \(|S|\) as the cardinality of \( S \). By \( y \leftarrow A(x) \), we denote that \( y \) is obtained by running algorithm \( A \) on input \( x \). We say that a function \( \epsilon : \mathbb{Z} \rightarrow \mathbb{R} \) is a negligible function, if for all \( z \in \mathbb{Z} \) there exists a \( k \in \mathbb{Z} \) such that \( |\epsilon(x)| < 1/x^k \) for all \( x > k \). By \( \ell \) and \( 1^\ell \), we denote a security parameter and the string of \( \ell \) ones. We denote \( K_G(1^\ell) \) as a key generator which takes as input \( 1^\ell \) and outputs a secret-public key pair.

**Definition 2.1 (Access Structure) [52]** Let \( \{P_1, P_2, \ldots, P_n\} \) be a set of parties. A collection \( \mathcal{A} \subset 2^{\{P_1, P_2, \ldots, P_n\}} \) is monotone, if \( S_1 \subset \mathcal{A} \) and \( S_1 \subset S_2 \) implies \( S_2 \in \mathcal{A} \). An access structure (respectively, monotone access structure) \( \mathcal{A} \) is a collection (respectively, monotone collection) \( \mathcal{A} \) of non-empty subsets of \( \{P_1, P_2, \ldots, P_n\} \), namely \( \mathcal{A} \subset 2^{\{P_1, P_2, \ldots, P_n\}} \setminus \{\phi\} \), where \( \phi \) is the empty set. A set \( S \) is called authorized set, if \( S \in \mathcal{A} \); otherwise, \( S \) is called unauthorized set.

A cipher-policy ABE (CP-ABE) scheme consists of the following four algorithms:

(i) **Setup.** The setup algorithm takes \( 1^\ell \) as inputs, and outputs the public key \( PK \) and the master key \( MK \), where \( (PK, MK) \leftarrow K_G(1^\ell) \).

(ii) **Key Generation.** The key generation algorithm takes the master key \( MK \) and a set of attributes \( SU \) as inputs, and outputs a secret key \( SK_U \) for \( SU \).

(iii) **Encryption.** The encryption algorithm takes an access structure \( \mathcal{A} \), the public key \( PK \), and a message \( M \) as inputs, and outputs the ciphertext \( C \), which can be decrypted by the receiver who holds a set of attributes \( SU \) if \( SU \in \mathcal{A} \).

(iv) **Decryption.** The decryption algorithm takes the public key \( PK \), the ciphertext \( C \) and the secret key \( SK_U \) as inputs, and outputs the message \( M \).

**Correctness:** An ABE scheme is correct if the user can decrypt the ciphertext when his attributes satisfy the access structure.

2.1.1. Security model For ABE

With respect to the security of ABE, there are two security models: selective-set model [23] and full security model [25]. In the selective-set model, the adversary must submit a set of attributes that she wants to be challenged with prior to obtaining the public parameters. This limitation is canceled in the full security model. All previous ABE schemes were proven in the selective-set model, except [25, 28]. Bethencourt et al. [25] proposed the full security model, and proved their scheme in the generic group model. Lewko et al. [40] proposed the
Attribute-Based Oblivious Access Control

An ABOAC scheme consists of the following four algorithms:

(i) Setup. The setup algorithm takes $1^\ell$ as input, and outputs the public key PK and the master key MK, where $(PK, MK) \leftarrow KG(1^\ell)$.

(ii) Key Generation. The key generation algorithm takes as input the master key MK and a set of attributes $S_i$, and outputs a secret key $SK_i$ for $S_i$.

(iii) Commitment. The sender generates his secret-public key pairs $(SSK, SPK) \leftarrow KG(1^\ell)$. To commit messages $M_1, M_2, \ldots, M_m$ under the corresponding access structures $A_1, A_2, \ldots, A_m$, the commitment algorithm takes as input SSK, $(M_1, A_1), (M_2, A_2), \ldots, (M_m, A_m)$, and outputs the ciphertexts $C_1, C_2, \ldots, C_m$. $C_i$ can be decrypted by the receiver who holds a set of attributes $S$ if $S \in A_i$, for $i = 1, 2, \ldots, m$.

(iv) Transfer. The sender inputs his secret key $SSK$. The receiver inputs his choices $C = \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$ and his secret key $SK_U$, where $S_U \in A_i$, for $j = 1, 2, \ldots, k$. The sender and the receiver interact. At the end, the receiver outputs $M_{\sigma_1}, M_{\sigma_2}, \ldots, M_{\sigma_k}$, without releasing anything about his attributes and choices to the sender; while the sender outputs nothing.

Correctness: An ABOAC scheme is correct if the receiver can obtain his intended messages when the receiver and the sender follow the steps of the scheme.

2.2. Security model for ABOAC

We define the security model for ABOAC as follows. For the privacy of the receiver, we require that his choices are unconditionally secure. Nothing about his attributes is released to the sender, even the number and a superset of his attributes. For the security of the sender, we employ the real world and ideal world paradigms. If there is an adversary in the real world, there will exist an adversary in the ideal world such that the outputs of these two adversaries are indistinguishable. We name this model as half-simulation model, which is similar to the models in [42, 43].

Privacy of Receiver.

(i) The receiver releases nothing about his attributes to the sender.

(ii) For any two different choice sets $\{\sigma_1, \sigma_2, \ldots, \sigma_k\}$ and $\{\sigma'_1, \sigma'_2, \ldots, \sigma'_k\}$, the transcripts received by the sender corresponding to $\{M_{\sigma_1}, M_{\sigma_2}, \ldots, M_{\sigma_k}\}$ and $\{M'_{\sigma'_1}, M'_{\sigma'_2}, \ldots, M'_{\sigma'_k}\}$ are indistinguishable. Especially, the choices of the receiver are unconditionally secure, if the received messages $\{M_{\sigma_1}, M_{\sigma_2}, \ldots, M_{\sigma_k}\}$ and $\{M'_{\sigma'_1}, M'_{\sigma'_2}, \ldots, M'_{\sigma'_k}\}$ are identically distributed.

Security of the sender. Suppose that the receiver has possessed the required secret keys. To define the security of the sender, we compare the real world and the ideal world experiments. In the real world, the receiver and the sender execute the protocol. Meanwhile, in the ideal world, the functionality of the protocol is replaced by a TTP. The sender sends all his messages $\{M_1, M_2, \ldots, M_m\}$ to the TTP. The receiver submits his choices $\{\sigma_1, \sigma_2, \ldots, \sigma_k\}$ adaptively to the TTP. If $\sigma_1, \sigma_2, \ldots, \sigma_k \in \{1, 2, \ldots, n\}$, the TTP responds $\{M_{\sigma_1}, M_{\sigma_2}, \ldots, M_{\sigma_k}\}$ to the receiver. An ABOAC scheme is sender-secure, if for any malicious receiver $R$ in the real world, there exists an receiver $\bar{R}$ in the ideal world such that the outputs of $R$ and $\bar{R}$ are indistinguishable.

Semantic security. Let $S^*$ be the set of the attributes that the adversary holds. If $S^* \notin A_i$, the adversary cannot obtain anything about the protected message $M_i$, for $i = 1, 2, \ldots, m$.

2.3. Complexity assumptions

Let $G$ and $G_\tau$ be two multiplicative cyclic groups with prime order $p$, and $g$ be a generator of $G$. A bilinear map $e : G \times G \rightarrow G_\tau$...
Let $G$ be a group generator that takes as input $1^t$ and outputs the description of group $G$ with prime order $p$. Let $G\mathcal{G}(1^t)$ be a bilinear group generator that takes as input $1^t$ and outputs the description of groups $G$ and $G_\tau$ with prime order $p$ and a bilinear map $e: G \times G \to G_\tau$. Let $G\mathcal{G}(1^t)$ be a group generator which takes as input $1^t$ and outputs the description of group $G$ with prime order $p$.

**Definition 2.3. (Decisional Bilinear Diffie-Hellman (DBDH) Assumption) [17].** Let $a, b, c, g \in \mathbb{Z}_p$, and $G$ be the generator of $G$. The DBDH assumption holds in the bilinear group $(e, G, G_\tau)$, if no probabilistic polynomial-time adversary $A$ can distinguish $(A, B, C, Z) = (g^a, g^b, g^c, e(g, g)^{abc})$ from $(A, B, C, Z) = (g^a, g^b, g^c, e(g, g)^{abc})$ with the advantage

$$\text{Adv}_{A}^{\text{DBDH}} = \left| \Pr[A(g^a, g^b, g^c, e(g, g)^{abc}) = 1] - \Pr[A(g^a, g^b, g^c, e(g, g)^{abc}) = 1] \right| > \epsilon(\ell),$$

where the probability is over the random choice of $a, b, c, Z \in \mathbb{Z}_p$ and the random bits consumed by the adversary $A$.

**Definition 2.4. (Chosen-Target Computational Diffie-Hellman (CT-CDH) Assumption) [54].** Let $g$ be a generator of the group $G \leftarrow \mathcal{G}(1^t)$ with prime order $p$, and $x \in \mathbb{Z}_p$. Let $H: \{0, 1\}^* \to G$ be a cryptographic hash function. $T_G(\cdot)$ is a target oracle, which takes as input $i \in \mathbb{Z}_p$, and outputs $g_i \in G$. $H_G(\cdot)$ is a help oracle, which takes as input $g_i \in G$, and outputs $g_i^\tau \in G$. Let $q_T$ and $q_H$ be the number of times that the two oracles are queried, respectively. The CT-CDH assumption holds in $G$, if no probabilistic polynomial-time adversary $A$ can break the CT-CDH assumption with the advantage

$$\text{Adv}_{A}^{\text{CT-CDH}} = \left| \Pr[A(\theta_{\tau+1}, i_{\tau+1}, \ldots, \theta_1, i_1)] - \Pr[A(T_G(\cdot), H_G(\cdot), g, g^\tau)] \right| > \epsilon(\ell),$$

where $\theta_j = g_j^\tau$, for $j = 1, 2, \ldots, \tau + 1$, and $q_H < \tau + 1 \leq q_T$.

The CT-CDH assumption is the analogous version of the chosen-target RSA inversion (RSA-CTI) assumption [55]. Intuitively, the CT-CDH assumption implies that, after the adversary $A$ queries the help oracle on the elements of $G$ for $q_H$ times, she cannot compute a new element of $G$ to the power of $x$, if its orders on the generator and the $q_H$ queried elements are unknown. Based on the CT-CDH assumption, we propose the extended CT-CDH (XCT-CDH) assumption, by replacing the target oracle in CT-CDH assumption with $q_H + 1$ random elements of $G$. We will prove that the proposed XCT-CDH assumption and the CT-CDH assumption are equivalent.
In this section, we will propose a new ABE scheme. The proposed ABE has constant ciphertext, and efficient encryption and decryption algorithms. For each encryption requiring \( t \) attributes, there are only three exponentiations and two pairings executed in the encryption and decryption phase, respectively. Our idea is derived from the schemes \([20, 29, 56]\). We describe our ABE scheme in Fig. 1.

**Correctness.** The correctness of the scheme is shown as follows.

\[
e(a_U, C_2) = e \left( g^{rv}, \left( h \prod_{j=1}^{t} A_{c_j} \right)^{\omega} \right)
\]

\[
e(g, h)^{rv \omega} = \prod_{j=1}^{t} e(g, A_{c_j})^{rv \omega},
\]

(1)

\[
s_c = b_U \prod_{j=1}^{t} s_{c_j} = g_2^{2 \times h^{rv}} \prod_{j=1}^{t} A_{c_j}^{rv}
\]

(2)

\[
e(C_1, s_c) = e \left( g^{\omega}, g_2^{2 \times h^{rv}} \prod_{j=1}^{t} A_{c_j}^{rv} \right) = e(g, g_2)^{\omega} e(g, h)^{rv \omega} \prod_{j=1}^{t} e(g, A_{c_j})^{rv \omega}
\]

\[
e(g_1, g_2)^{\omega} e(a_U, C_2)
\]

(3)
Define and compute:

\[ C_3 \cdot \frac{e(a_T, C_2)}{e(C_1, s_c)} = M \cdot \frac{e(g_1, g_2)^{\omega}}{e(g_1, g_2)^{\omega}e(a_T, C_2)} = \frac{M}{e(g_1, g_2)^{\omega}} = M. \]  

(4)

Theorem 3.1. Our ABE scheme is \((\mathcal{T}, q, \epsilon(e))\) semantically secure (CPA-ABE) in the selective-attribute model, assuming that \((\mathcal{T}', \epsilon'(\ell))\) decisional bilinear Diffie-Hellman assumption holds in \((e, G, \mathbb{G}_r)\), where

\[ T' = T + (|U| + 4(q + 1) + 3(|S_1| + |S_2| + \cdots + |S_q|))t_{\text{exp}} \]

and

\[ \epsilon'(\ell) = \frac{\epsilon(e)}{2}. \]

\(t_{\text{exp}}\) denotes the running time of one exponentiation. \(U\) is the set of universal attributes, \(S_j\) is the set of attributes queried by the adversary, for \(j = 1, 2, \ldots, q\).

Proof. Suppose that there exists an adversary \(A\) who can \((\mathcal{T}, q, \epsilon)\) break our ABE in the selective-attribute model, we will show that there exists an algorithm \(B\) who can \((\mathcal{T}', \epsilon')\) break the decisional bilinear Diffie-Hellman assumption as follows.

The challenger generates the bilinear group \((e, p, G, \mathbb{G}_r)\) \(\rightarrow\) \(G_1 H(1^\ell)\), and chooses a generator \(g \in G\). It flips an unbiased coin \(\mu\) from \([0, 1]\). If \(\mu = 0\), the challenger sends \((A, B, C, Z) = (g^e, g^b, g^c, e(g, g)^{ab/c})\) to \(B\); otherwise, the challenger sends \((A, B, C, Z) = (g^a, g^b, g^c, e(g, g)^{y})\) to \(B\), where \(z \xrightarrow{\text{R}} U_{\mathbb{G}_p} B\) will output its guess \(\mu^*\) on \(\mu\). \(B\) sends \(g_1 = g^a, g_2 = g^b\) and \(g_3 = g^c\).

Initialization. The adversary submits an attribute string \(\hat{S}\) \(\xrightarrow{\text{R}}\) \{\text{attr}_j\}. Setup. \(B\) selects \(n\) random integers \(e_1, e_2, \ldots, e_n \xrightarrow{\text{R}} U_{\mathbb{Z}_p}\), and computes \(A_i = g^{e_i}\) and \(A_j = g^{e_i}, \) for \(j \in \{1, 2, \ldots, n\} \setminus \{i\}\). \(B\) chooses \(Y \xrightarrow{\text{R}} U_{\mathbb{G}_r}\) and sets \(h = g_1^{-e_i} g^{y}\).

\(B\) sends \(A\) the public parameters

\[(e, G, \mathbb{G}_r, g, g_1, g_2, h, A_1, A_2, \ldots, A_n).\]

Phase 1. \(A\) queries secret keys on the set of attributes \(S_0 = \{\text{attr}_{r_1}, \text{attr}_{r_2}, \ldots, \text{attr}_{r_n}\}\), where \(\sigma = 1, 2, \ldots, q_1, \sigma < n\) and \(S^* \subseteq S_0\), for \(i = 1, 2, \ldots, q_1\). \(B\) chooses \(\sigma_0 \xrightarrow{\text{R}} U_{\mathbb{Z}_p}\), and computes

\[ a_\sigma = g^{-r_\sigma} \frac{1}{g_2^{\ell/e_i}}, b_\sigma = g^{x/e_i} h^{-r_\sigma}, s_{r_\sigma} = (g^{-r_\sigma} g_2^{1/e_i} e_\sigma) \]

for \(j = 1, 2, \ldots, \sigma_0\), and \(\sigma = 1, 2, \ldots, q_1\).

We claim that \(\{a_\sigma, b_\sigma, (s_{r_\sigma})^2\}_{\sigma = 1}^{q_1}\) are correctly distributed. Because, we have

\[ g_2^{y/e_\sigma} h^{-r_\sigma} = g_1^{y/e_\sigma} (g_1^{-e_\sigma + y/e_\sigma})^{-r_\sigma} = (g_1^{-e_\sigma + y/e_\sigma} g_1^{y/e_\sigma})^{-r_\sigma} = g_1^{y/e_\sigma} (g_1^{y/e_\sigma} g_1^{-e_\sigma + y/e_\sigma} + b/e_\sigma) = g_1^{y/e_\sigma} g_1^{-r_\sigma + b/e_\sigma} = g_1^{y/e_\sigma} g_1^{-r_\sigma + b/e_\sigma} \]

Let \(\tilde{r}_\sigma = -r_\sigma + b/e_\sigma\), we have

\[ g_2^{y/e_\sigma} h^{-r_\sigma} = g_2^{y/e_\sigma} h^{\tilde{r}_\sigma}, g^{-r_\sigma} g_2^{1/e_\sigma} = g^{-r_\sigma + b/e_\sigma} = g^{\tilde{r}_\sigma} \]

and

\[(g^{-r_\sigma} g_2^{1/e_\sigma} e_\sigma) \text{ is correctly distributed.} \]

Challenge. \(A\) sends \(B\) two messages \(M_0, M_1\). \(B\) flips an unbiased coin from \([0, 1]\), and gets back with \(\hat{\mu} \in [0, 1]\). \(B\) chooses \(S = \{\text{attr}_{r_1}, \text{attr}_{r_2}, \ldots, \text{attr}_{r_n}\} \subseteq U\), and computes

\[ C_1^* = g_3, C_2 = g_3^{y + \sum_{i=1}^{r} e_\sigma}, C_3^* = Z \cdot M_\hat{\mu}, \]

where \(S^* \subseteq S\).

\(B\) responds with the challenge ciphertext \(C^* = (C_1^*, C_2^*, C_3^*)\). So, \(C^* = (g^e, (h^{A_1} \prod_{j=1}^{r} A_j)^y, Z \cdot M_\hat{\mu})\) is a valid encryption of \(M_\hat{\mu}\) with the correct distribution whenever \(Z = e(g, g)^{abc}\).

Phase 2. \(A\) can query secret keys for sets of attributes \(S_{q_1+1}, S_{q_1+2}, \ldots, S_q\), where the only constraint is \(S^* \subseteq S_\sigma\), for \(\sigma = 1, 2, \ldots, q\). \(B\) responds as Phase 1.

Guess. \(A\) outputs his guess \(\hat{\mu}\) on \(\mu\). If \(\hat{\mu} = \mu\), \(B\) outputs \(\mu = 0\); otherwise \(B\) outputs \(\mu = 1\).

As shown above, the public parameters and secret keys generated in the simulation paradigm are identical to those in the real scheme. Now, we compute the probability with which \(B\) can break the DBDH assumption.

In the case where \(\mu = 0\), \(C^* = (C_1^*, C_2^*, C_3^*)\) is a correct ciphertext of \(M_\hat{\mu}\). Therefore, \(A\) can output \(\hat{\mu} \neq \mu\) with advantage at least \(\epsilon(e)\), namely \(\Pr[\hat{\mu} = \mu | \mu = 0] \geq \frac{1}{2} + \epsilon(e)\). Since \(B\) guesses \(\mu = 0\) when \(\hat{\mu} = \mu\), we have \(Pr[\mu = \mu | \mu = 0] \geq \frac{1}{2} + \epsilon(e)\).

If \(\mu = 1\), \(A\) can obtain no information about \(\mu\). Therefore, \(A\) can output \(\hat{\mu} \neq \mu\) without advantage, namely \(\Pr[\hat{\mu} = \mu | \mu = 1] = \frac{1}{2}\). Since \(B\) guesses \(\mu = 1\) when \(\hat{\mu} = \mu\), we have \(Pr[\mu = \mu | \mu = 1] = \frac{1}{2}\).

So, the advantage that \(B\) can break the DBDH assumption is

\[ \frac{1}{2} \Pr[\mu = \mu | \mu = 0] + \frac{1}{2} \Pr[\mu = \mu | \mu = 1] - \frac{1}{2} \]

\[ \geq \frac{1}{2} \times \left( \frac{1}{2} + \epsilon(e) \right) + \frac{1}{2} \times \frac{1}{2} - \frac{1}{2} = \frac{\epsilon(e)}{2}.\]
The receiver does not release anything about the content of attributes which the ciphertext requires, respectively. By $\mathcal{E}P$ scheme in this section. In our ABOAC, both the identity of the receiver and the actions performed by him can be protected. The receiver does not release anything about the content of the selected services and his attributes to the sender, even the number and supersets of his attributes are protected. The sender only knows the number of services selected by the authorized receiver. We describe our ABOAC scheme in Fig. 2.

**Overview.** Our idea on ABOAC is that we introduce ABAC to OT. At the beginning, the receiver authenticates himself to the issuer, and obtains the secret keys for his attributes. Then, the sender encrypts all messages under different attributes using OT technique. At the end, the receiver interacts with the sender adaptively. We claim that the receiver does not release anything about the selected services and his attributes to the sender, even the number and a superset of his attributes. This is because all services are encrypted under different attributes by the sender, but he cannot know which services the receiver selected. So, he cannot conclude anything about the receiver’s attributes from the selected services.

### 4. ATTRIBUTE-BASED OBLIVIOUS ACCESS CONTROL

Based on the ABE proposed in Section 3, we propose an ABOAC scheme in this section. In our ABOAC, both the identity of the receiver and the actions performed by him can be protected. The receiver does not release anything about the content of the selected services and his attributes to the sender, even the number and supersets of his attributes are protected. The sender only knows the number of services selected by the authorized receiver. We describe our ABOAC scheme in Fig. 2.

**Overview.** Our idea on ABOAC is that we introduce ABAC to OT. At the beginning, the receiver authenticates himself to the issuer, and obtains the secret keys for his attributes. Then, the sender encrypts all messages under different attributes using OT technique. At the end, the receiver interacts with the sender adaptively. We claim that the receiver does not release anything about the selected services and his attributes to the sender, even the number and a superset of his attributes. This is because all services are encrypted under different attributes by the sender, but he cannot know which services the receiver selected. So, he cannot conclude anything about the receiver’s attributes from the selected services.

#### TABLE 1. The comparison of computation cost.

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Setup</th>
<th>Key generation</th>
<th>Encryption</th>
<th>Decryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW [21]</td>
<td>($</td>
<td>\mathcal{U}</td>
<td>+ 1)E$</td>
<td>$</td>
</tr>
<tr>
<td>GPSW [23]</td>
<td>($</td>
<td>\mathcal{U}</td>
<td>+ 1)E$</td>
<td>$</td>
</tr>
<tr>
<td>OSW [24]</td>
<td>2($</td>
<td>\mathcal{U}</td>
<td>+ 1)E$</td>
<td>3($</td>
</tr>
<tr>
<td>BSW [25]</td>
<td>3E</td>
<td>2(($</td>
<td>\mathcal{S}_U</td>
<td>+ 1)E$</td>
</tr>
<tr>
<td>CN [26]</td>
<td>3($</td>
<td>\mathcal{U}</td>
<td>+ 1)E$</td>
<td>($</td>
</tr>
<tr>
<td>HLR [27]</td>
<td>2($</td>
<td>\mathcal{U}</td>
<td>+ 1)E$</td>
<td>($</td>
</tr>
<tr>
<td>LOSTW [28]</td>
<td>($</td>
<td>\mathcal{U}</td>
<td>+ 2)E$</td>
<td>($</td>
</tr>
<tr>
<td>Waters [29]</td>
<td>3E</td>
<td>($</td>
<td>\mathcal{S}_U</td>
<td>+ 2)E$</td>
</tr>
<tr>
<td>ZH [36]</td>
<td>6$</td>
<td>\mathcal{U}</td>
<td>E$</td>
<td>($</td>
</tr>
<tr>
<td>EMONS [37]</td>
<td>($</td>
<td>\mathcal{U}</td>
<td>+ 1)E$</td>
<td>4E</td>
</tr>
<tr>
<td>ALP [38]</td>
<td>($</td>
<td>\mathcal{U}</td>
<td>+ 1)E$</td>
<td>($</td>
</tr>
<tr>
<td>CZF [39]</td>
<td>2$</td>
<td>\mathcal{U}</td>
<td>(E + P)$</td>
<td>$</td>
</tr>
<tr>
<td>Our scheme</td>
<td>2E</td>
<td>($</td>
<td>\mathcal{S}_U</td>
<td>+ 2)E$</td>
</tr>
</tbody>
</table>

#### TABLE 2. The comparison of type, access structure, security model and the length of ciphertext.

<table>
<thead>
<tr>
<th>Schemes</th>
<th>KP/CP-ABE</th>
<th>Access structure</th>
<th>Security model</th>
<th>Length of ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW [21]</td>
<td>KP-ABE</td>
<td>Monotonic</td>
<td>Selective-set</td>
<td>$</td>
</tr>
<tr>
<td>GPSW [23]</td>
<td>KP-ABE</td>
<td>Monotonic</td>
<td>Selective-set</td>
<td>$</td>
</tr>
<tr>
<td>OSW [24]</td>
<td>KP-ABE</td>
<td>Non-monotonic</td>
<td>Selective-set</td>
<td>(($</td>
</tr>
<tr>
<td>BSW [25]</td>
<td>CP-ABE</td>
<td>Monotonic</td>
<td>Full security</td>
<td>(($</td>
</tr>
<tr>
<td>CN [26]</td>
<td>CP-ABE</td>
<td>Non-monotonic</td>
<td>Selective-set</td>
<td>(($</td>
</tr>
<tr>
<td>HLR [27]</td>
<td>CP-ABE</td>
<td>Monotonic</td>
<td>Selective-set</td>
<td>$2E_G + 2E_{\mathcal{G}_r}$</td>
</tr>
<tr>
<td>LOSTW [28]</td>
<td>CP-ABE</td>
<td>Monotonic</td>
<td>Full security</td>
<td>($2</td>
</tr>
<tr>
<td>Waters [29]</td>
<td>CP-ABE</td>
<td>Monotonic</td>
<td>Selective-set</td>
<td>($2</td>
</tr>
<tr>
<td>ZH [36]</td>
<td>CP-ABE</td>
<td>Non-monotonic</td>
<td>Selective-set</td>
<td>$2E_G + E_{\mathcal{G}_r}$</td>
</tr>
<tr>
<td>EMONS [37]</td>
<td>CP-ABE</td>
<td>Monotonic</td>
<td>Selective-set</td>
<td>$2E_G + E_{\mathcal{G}_r}$</td>
</tr>
<tr>
<td>ALP [38]</td>
<td>KP-ABE</td>
<td>Non-monotonic</td>
<td>Selective-set</td>
<td>$3E_G + E_{\mathcal{G}_r}$</td>
</tr>
<tr>
<td>CZF [39]</td>
<td>KP-ABE</td>
<td>Non-monotonic</td>
<td>Selective-set</td>
<td>$2E_G + E_{\mathcal{G}_r}$</td>
</tr>
<tr>
<td>Our scheme</td>
<td>CP-ABE</td>
<td>Monotonic</td>
<td>Selective-attribute</td>
<td>$2E_G + E_{\mathcal{G}_r}$</td>
</tr>
</tbody>
</table>
Setup. Taking as input $1^λ$, this algorithm responds with bilinear group $(e, p, G, G_r) ← G(1^λ)$ with prime order $p$, where $e : G × G → G_r$. Let $g, g_2, h$ be the generators of $G$, and the set of universal attributes $U = \{\text{attr}_1, \text{attr}_2, \ldots, \text{attr}_n\} \subseteq \{0, 1\}^n$. The issuer generates his master secret-public key pair $(α, g_1) ← K(1^λ)$, where $α$ $∈$ $\mathbb{Z}_p$ and $g_1 = g^α$. For each $\text{attr}_j$ $∈$ $U$, he chooses $A_j$ $∈$ $G$. The public key is

$$(e, p, G, G_r, g, g_1, g_2, h, A_1, A_2, \ldots, A_n).$$

Key Generation. To generate a private key for a set of attributes $SU = \{\text{attr}_{i_1}, \text{attr}_{i_2}, \ldots, \text{attr}_{i_γ}\} \subseteq U$, The issuer chooses $r_U$ $∈$ $\mathbb{Z}_p$, and computes

$$a_U = g^{r_U}, \quad b_U = g_2^{r_U}, \quad s_{i_1} = A_{i_1}^{r_U}, \quad s_{i_2} = A_{i_2}^{r_U}, \ldots, \quad s_{i_γ} = A_{i_γ}^{r_U}.$$ 

The secret keys for the set of attributes $SU$ is $SK_U = \{a_U, b_U, s_{i_1}, \ldots, s_{i_γ}\}$. These secret keys can be verified as follows:

$$e(g, b_U) = e(g, g_2) \cdot e(a_U, h)$$

and

$$e(g, s_{i_j}) = e(a_U, A_{i_j})$$

for $j = 1, 2, \ldots, γ$.

Commitment Phase. Suppose that the sender has $m$ messages $M = \{M_1, M_2, \ldots, M_m\} \subseteq \mathbb{G}_r^*$. Let $A_i$ be monotonic access structure and $S_{C_i}$ $∈$ $A_i$ be the minimal set in $A_i$ [57].

1. The sender generates his secret-public pair $(θ, g) ← K(1^λ)$, where $θ$ $∈$ $\mathbb{Z}_p$ and $g = e(g_1, g_2)^θ$.
2. To commit a message $M_j$ under the attribute set $S_{C_j} = \{\text{attr}_{j_1}, \text{attr}_{j_2}, \ldots, \text{attr}_{j_{γ_j}}\} \subseteq A_j$, the sender chooses $ω_j$ $∈$ $\mathbb{Z}_p$, and computes

$$C_{j_1} = g^{ω_j}, \quad C_{j_2} = (h \prod_{i=1}^{t} A_{j_i})^{ω_j}, \quad C_{j_3} = e(g_1, g_2)^{ω_j} \cdot M_j$$

The sender sends the receiver $\{C_1, C_2, \ldots, C_m\}$, where $C_j = (C_{j_1}, C_{j_2}, C_{j_3})$, for $j = 1, 2, \ldots, m$.

Transfer Phase.

1. $R$ adaptively chooses $σ_z \in \{1, 2, \ldots, m\}$, and computes $s_z = b_U \prod_{j=1}^{l} s_{σ_j}$, where $s_{σ_j} \in SK_U$ and $S_{C_{σ_j}} \subseteq SU \in A_{σ_j}$. He computes $Γ_z = e(g_{σ_z}, s_z)^{ω_z}$. The receiver chooses $x_z$ $∈$ $\mathbb{Z}_p$, and computes $Θ_z = Γ_z^{x_z}$, for $z = 1, 2, \ldots, k$.
2. $R$ $\xrightarrow{Θ_z} S$. The receiver sends $Θ_z$ to the sender.
3. $R$ $\xrightarrow{s_{σ_z}} S$. The sender computes $Φ_z = Θ_z^{s_{σ_z}}$, and sends $Φ_z$ to the receiver.
4. The receiver computes $Ψ_z = Φ_z^{x_z}$ and $M_{σ_z} = C_{σ_z} Ψ_z^{ω_z}$, for $z = 1, 2, \ldots, k$.

*By $S_{C_i} \subseteq A_i$ be the minimal set of $A_i$, we mean that $S_{C_i} \subseteq S$ if $S \in A_i$.*

FIGURE 2. Attribute-based oblivious access control.
Correctness. From Equations (1)–(3) in Section 3, we have

\[
\Gamma_z = \frac{e(C_{\sigma_1}, s_z)}{e(aU, C_{\sigma_2})} = \frac{e(g_1, g_2)^{s_{\omega_\sigma j} x_j}}{e(aU, C_{\sigma_2})} = e(g_1, g_2)^{s_{\omega_\sigma j} x_j},
\]

(5)

\[
\Theta_z = \Gamma_z^\tau = e(g_1, g_2)^{s_{\omega_\sigma j} x_j},
\]

(6)

\[
\Phi_z = \Theta_z^\tau = e(g_1, g_2)^{s_{\omega_\sigma j} x_j},
\]

(7)

\[
\Psi_z = \Phi_z^{\tau^{-1}} = e(g_1, g_2)^{s_{\omega_\sigma j} x_j},
\]

(8)

and

\[
\frac{C_{\sigma_2}}{\Psi_z} = \frac{e(g_1, g_2)^{s_{\omega_\sigma j} x_j}, M_{\sigma_2}}{e(aU, C_{\sigma_2})} = M_{\sigma_2}.
\]

(9)

**Theorem 4.1.** ABOAC is unconditionally receiver-secure.

**Proof.** For any \(\Theta_j\) received by the sender from the receiver, there exists an \(x_i\) such that

\[
\Theta_j = e(g_1, g_2)^{s_{\omega_\sigma j} x_j} = e(g_1, g_2)^{s_{\omega_\sigma j} x_j} = \Theta_i,
\]

namely \(x_i = s_{\omega_\sigma j} x_j \mod p\). Therefore, from the view of the sender, whether \(\Theta_j\) is computed from \(C_{\sigma_2}\) or \(C_{\sigma_1}\) is identically distributed. So, ABOAC is unconditionally receiver-secure.

**Theorem 4.2.** ABOAC is sender secure, if the extended chosen-target Diffie-Hellman assumption holds in \(\mathbb{G}_z\).

**Proof.** For any probabilistic polynomial-time adversary \(\hat{R}\) in the real world, we will show that there exists a probabilistic polynomial-time adversary \(\hat{R}^*\) in the ideal world such that the outputs of \(\hat{R}\) and \(\hat{R}^*\) are indistinguishable. The real-world and ideal-world paradigms are processed as follows:

1. The sender S sends his messages \(\{M_1, M_2, \ldots, M_m\}\) to the TTP Charlie.
2. \(\hat{R}^*\) sends \(\{C^*_1, C^*_2, \ldots, C^*_m\}\) to Charlie, where \(C^*_j \xleftarrow{} \mathbb{G}_z^\times \mathbb{G}_z\).
3. \(\hat{R}^*\) monitors the outputs of \(\hat{R}\). If \(\hat{R}\) can output \((\Gamma_1, \Theta_1), (\Gamma_2, \Theta_2), \ldots, (\Gamma_k, \Theta_k)\), \(\hat{R}^*\) outputs \((\Gamma^*_1, \Theta^*_1), (\Gamma^*_2, \Theta^*_2), \ldots, (\Gamma^*_k, \Theta^*_k)\), where \((\Gamma^*_j, \Theta^*_j) \xleftarrow{} \mathbb{G}_z^\times \mathbb{G}_z\), for \(j = 1, 2, \ldots, k\).
4. When \(\hat{R}\) submits \([\Theta_1, \Theta_2, \ldots, \Theta_k]\) to obtain \([\Phi_1, \Phi_2, \ldots, \Phi_k]\), \(\hat{R}^*\) queries the help oracle \(H_{\omega_\sigma j}()\) on \([\Theta^*_1, \Theta^*_2, \ldots, \Theta^*_k]\), and gets back with \([\Phi^*_1, \Phi^*_2, \ldots, \Phi^*_k]\), where \(\Phi^*_j = (\Theta^*_j)^{\omega_\sigma j}\), for \(j = 1, 2, \ldots, k\).
5. If \(\hat{R}\) can output \(\Psi_j\), \(\hat{R}^*\) sends \(s_j\) to Charlie. Charlie responds with \(C^*_j/M_{\sigma_2}\).
6. \(\hat{R}^*\) outputs \([\Gamma^*_1, \Gamma^*_2, \ldots, \Gamma^*_k, \Theta^*_1, \Theta^*_2, \ldots, \Theta^*_k, \Phi^*_1, \Phi^*_2, \ldots, \Phi^*_k, C^*_1, C^*_2, \ldots, C^*_m]\).

If \(\hat{R}\) obtains \(k + 1\) messages, \(\hat{R}^*\) does not know which \(k\) indices have been selected by \(\hat{R}\), the simulation fails. Otherwise, we will show that \(\hat{R}\) can obtain no more than \(k\) messages under the XCT-CDH assumption. If \(\hat{R}\) can obtain \(k + 1\) messages, he can compute \(\Psi_j\), for \(j = 1, 2, \ldots, k + 1\). Therefore, after receiving \((e(g_1, g)^{s_{\omega_\sigma j}})^\varphi, (e(g_1, g)^{s_{\omega_\sigma j}})^\varphi, \ldots, (e(g_1, g)^{s_{\omega_\sigma j}})^\varphi\), \(\hat{R}\) can compute \((e(g_1, g)^{s_{\omega_\sigma k+1}})^\varphi\). This will contradict the XCT-CDH assumption. So, \(\hat{R}\) can obtain at most \(k\) messages.

\begin{align*}
\{\Gamma_1, \Gamma_2, \ldots, \Gamma_k\} & \text{ and } \{\Theta_1, \Theta_2, \ldots, \Theta_k\} \text{ are random elements in } \mathbb{G}_z, \\
\{C^*_1, C^*_2, \ldots, C^*_m\} & \text{ are random elements in } \mathbb{G}_z \times \mathbb{G}_z, \quad \{\Phi^*_1, \Phi^*_2, \ldots, \Phi^*_k\}\end{align*}

are identically distributed.

Hence, the outputs of \(\hat{R}\) and \(\hat{R}^*\) are indistinguishable.

**Theorem 4.3.** ABOAC is semantically secure, if the extended chosen-target Diffie-Hellman assumption holds in \(\mathbb{G}_z\).

**Proof.** There are two kinds of adversaries:

**Type-I.** The adversary can compute \(\Gamma_j\) from the ciphertext \((C_j, C_j)\), then acts as a legal receiver to interact with the sender.

**Type-II.** The adversary can compute \(M_j\) from \((C_j, C_j, C_j)\).

We will show that Type-I adversary can break the semantically secure ABE proposed in Section 2, and Type-II adversary can break the XCT-CDH assumption.

**Type-I.** Suppose \(A\) is Type-I adversary, he can compute \(\Gamma_j\) from the ciphertext \((C_j, C_j, C_j)\). There exists an algorithm \(B\) who can use \(A\) to break the semantic security of the proposed ABE. Suppose that \(M_j\) is encrypted under the same set of attributes \(S_j\) in the proposed ABE and the ciphertext is \(C'_j = (C_j^*, C_j^*, C_j^*)\), where \(C_k^* = C_k\), for \(i = 1, 2, B\) sends \((C_j^*, C_j^*)\) to \(A\). If \(A\) can compute \(\Gamma_j\), \(B\) can compute \(M_j = \frac{C_k^*}{M_{\sigma_2}}\). This will contradict Theorem 1.

**Type-II.** Suppose \(A\) is Type-II adversary, he can compute the \(M_j\) from \((C_j, C_j, C_j)\). There exists an algorithm \(B\) who can use \(A\) to break the XCT-CDH assumption as follows. Given \((e(g_1, g_2)^\varphi, e(g_1, g)^{\varphi_1}, e(g_1, g)^{\varphi_2})\), the aim of \(B\) is to compute \((e(g_1, g_2)^{\varphi_1, \varphi_2})^{\varphi_3}\). \(B\) sends \(C_j = (C_j, C_j, C_j)\) to \(A\). If \(A\) can output \(M_j\), \(B\) can compute \(e(g_1, g_2)^{\varphi_1, \varphi_2} = \frac{C_j}{M_{\sigma_2}}\). So \(B\) can use \(A\) to break the XCT-CDH assumption.

**Complexity.** We list the computation cost and communication cost of our ABOAC scheme in Tables 3 and 4, respectively. By \(S_U\), we denote the set of attributes held by the user \(U\). By \(\#m\) and \(\#k\), we denote the total number of the messages and the number of the transferred messages. Additionally, by \(E_G\) and \(E_{G_2}\), we denote one element in \(\mathbb{G}\) and one element in \(\mathbb{G}_2\), respectively.
TABLE 3. The computation cost of Our ABOAC.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Setup</th>
<th>Key generation</th>
<th>Commitment</th>
<th>Transfer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>I</td>
<td>I</td>
<td>S</td>
<td>R</td>
</tr>
<tr>
<td>ABOAC</td>
<td>$2E$</td>
<td>$(</td>
<td>S_U</td>
<td>+ 2)E$</td>
</tr>
</tbody>
</table>

TABLE 4. The communication cost of our ABOAC.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Key generation</th>
<th>Commitment</th>
<th>Transfer</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABOAC</td>
<td>$(</td>
<td>S_U</td>
<td>+ 2)E_G$</td>
</tr>
</tbody>
</table>

5. CONCLUSION

In this paper, we first proposed a new ABE scheme, where the ciphertext can be constant. Both the encryption and the decryption algorithms in our ABE scheme are very efficient. Based on the proposed ABE, we proposed an ABOAC scheme, where both the attributes of the receiver and the actions performed by him can be hidden. The sender knows the number of the services selected by the receiver if his attributes satisfy the public access policies. The receiver does not release anything about the selected services and his attributes to the sender, even the number and a superset of his attributes. Hence, our ABOAC scheme provides an intuitive and novel solution to privacy-enhanced attribute-based access control. Notably, the computing cost and communication cost in our ABOAC scheme are independent of the required attributes. So, our ABOAC can be exploited in the systems where both the bandwidth and the computing ability are limited, such as WSANs [15], MANETS [16], etc.

FUNDING

The first author was supported by PhD scholarships of Smart Services Cooperative Research Centre (CRC) and University of Wollongong. The second author was supported by ARC Future Fellowship FT0991397.

REFERENCES


