The Computer Journal Advance Access published June 7, 2012

doi:10.1093/comjnl/bxs061

Attribute-Based Oblivious Access Control

Jinguang Han[1,3]*, Willy Susilo[1], Yi Mu[1] and Jun Yan[2]

[1] *Centre for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW 2522, Australia*
[2] *School of Information Systems and Technology, University of Wollongong, Wollongong, NSW 2522, Australia*
[3] *College 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 $S_{\text{A}} = \{\text{European}, \text{Married}, \text{Adult}, \text{Student}\}$ and $S_{\text{B}} = \{\text{European}, \text{Adult}, \text{Vegetarian}, \text{Student}\}$, 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 $S \subseteq S_{\text{A}}$ and $S \subseteq S_{\text{B}}$. 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 encrypter 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 computing 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 $\mathsf{Aggregate}$ introduced in [35]. As mentioned in [35], the running time of the algorithm $\mathsf{Aggregate}$ is about $(\gamma(\gamma-1)/2)T_{\mathrm{exp}}$, where γ 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 $S_{\mathrm{A}} = \{\text{European, Student}\}$, and Bob holds a set of attributes $S_{\mathrm{B}} = \{\text{American, Adult}\}$. If Alice and Bob collude, they can collaborate to get attributes $\mathrm{S} = \{\text{European, Adult, Student}\}$ 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 cihpertext 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_k^m) is a protocol where the sender and the receiver have a set of messages $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ 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 $(\mathrm{OT}_{k\times 1}^m)$ 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 $O(\gamma n)$, respectively, where n is the number of the attributes listed in the access policies, and γ 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.

Coull *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 $|S_{C_i}|$ denote that the number of the attributes required by the ith 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 $\mathcal{O}(\sum_{i=1}^{k} |S_{C_{\sigma_i}}|)$ and $\mathcal{O}(m)$, respectively.

Zhang *et al.* [49] proposed a new AC-OT scheme which is based on the CP-ABE scheme [28] and OT_k^m 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_k^m 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 $\mathcal{O}(\sum_{i=1}^{k} |S_{C_{\sigma_i}}|)$ and $\mathcal{O}(\sum_{i=1}^{m} |S_{C_i}|)$, 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 size 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 $\mathcal{O}(\sum_{i=1}^{k} |S_{C_{\sigma_i}}|)$ and $\mathcal{O}(\sum_{i=1}^{m} |S_{C_i}|)$, respectively.

1.2. Our contribution

An ABE scheme is more efficient and it can express a fine-gained 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 $a \overset{R}{\leftarrow} A$, we denote that a is selected uniformly from A, if A is a finite set. By $R \overset{\Phi}{\leftarrow} S$ and $R \overset{\Phi}{\rightarrow} S$, we denote that party S sends Φ to party R and party R sends Φ 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 $|\epsilon(x)| < 1/x^z$ for all $x > k$. By ℓ and 1^ℓ, we denote a security parameter and the string of ℓ ones. We denote $\mathcal{KG}(1^\ell)$ as a key generator which takes as input 1^ℓ 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* $\mathbb{A} \subset 2^{\{P_1,P_2,\ldots,P_n\}}$ *is monotone, if* $S_1 \in \mathbb{A}$ *and* $S_1 \subseteq S_2$ *implies* $S_2 \in \mathbb{A}$. *An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection)* $\mathbb{A}$ *of non-empty subsets of* $\{P_1, P_2, \ldots, P_n\}$, *namely* $\mathbb{A} \subset 2^{\{P_1,P_2,\ldots,P_n\}} \setminus \{\phi\}$, *where* ϕ *is the empty set. A set* S *is called authorized set, if* $S \in \mathbb{A}$*; 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^ℓ as inputs, and outputs the public key PK and the master key MK, where $(\mathrm{PK}, \mathrm{MK}) \leftarrow \mathcal{KG}(1^\ell)$.
(ii) Key Generation. The key generation algorithm takes the master key MK and a set of attributes S_U as inputs, and outputs a secret key SK_U for S_U.
(iii) Encryption. The encryption algorithm takes an access structure $\mathbb{A}$, 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 S_U if $S_U \in \mathbb{A}$.
(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 first ABE scheme which can achieve full security and can be reduced to the subgroup decision assumptions in composite order bilinear groups. They used the dual system encryption [53] technology to prove their scheme. Before the proof, two additional algorithms are constructed, namely semi-functional key algorithm and semi-functional ciphertext algorithm.

In this paper, we consider the selective-attribute model which is slightly stronger than the selective-set model introduced in [23]. This model is analogous to the selective-ID model in IBE [17]. We describe this model as follows:

Initiation. The adversary $\mathcal{A}$ submits a set of attributes $S^* = \{\text{attr}^*\}$ that she wants to be challenged with.

Setup. The challenger runs the setup algorithm, and sends the public key PK to the adversary $\mathcal{A}$.

Phase 1. The adversary $\mathcal{A}$ can query secret keys on the sets of attributes $S_1, S_2, \ldots, S_{q_1}$, where $S^* \not\subseteq S_i$, for $i = 1, 2, \ldots, q_1$. The challenger responds with the corresponding secret keys.

Challenge. The adversary submits two equal length messages M_0 and M_1. The challenger flips an unbiased coin from $\{0, 1\}$, and obtains $b \in \{0, 1\}$. It chooses a set of attributes S, and encrypts M_b under S, where $S^* \subseteq S$. The ciphertext C^* is responded to the adversary $\mathcal{A}$.

Phase 2. The adversary $\mathcal{A}$ can query secret keys on the sets of attributes $S_{q_1+1}, S_{q_1+2}, \ldots, S_q$. The only constraint is $S^* \not\subseteq S_j$, for $j = q_1 + 1, q_1 + 2, \ldots, q$. The challenger responds as in Phase 1.

Guess. The adversary $\mathcal{A}$ outputs his guess b' on b.

DEFINITION 2.2. *An ABE is (T, q, ϵ)-semantically secure (CPA-ABE), if no probabilistic polynomial-time adversary $\mathcal{A}$ making at most q secret key queries has the advantage*

$$\text{Adv}_{\mathcal{A}}^{\text{ABE}}(\ell) = |\Pr[b' = b] - \tfrac{1}{2}| > \epsilon(\ell)$$

in the selective-attribute model.

2.2. Attribute-based oblivious access control

An ABOAC scheme consists of the following four algorithms:

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

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

(iii) Commitment. The sender generates his secret-public key pairs $(\text{SSK}, \text{SPK}) \leftarrow \mathcal{KG}(1^\ell)$. To commit messages $M_1, M_2, \ldots, M_m$ under the corresponding access structures $\mathbb{A}_1, \mathbb{A}_2, \ldots, \mathbb{A}_m$, the commitment algorithm takes as input SSK, $(M_1, \mathbb{A}_1), (M_2, \mathbb{A}_2), \ldots, (M_m, \mathbb{A}_m)$, 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 $S \in \mathbb{A}_i$, for $i = 1, 2, \ldots, m$.

(iv) Transfer. The sender inputs his secret key SSK. The receiver inputs his choices $\mathcal{C} = \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$ and his secret key SK_U, where $S_U \in \mathbb{A}_{\sigma_i}$, 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.

2.2.1. *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 $\sigma_1, \sigma_2, \ldots, \sigma_k \in \{1, 2, \ldots, m\}$, 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 $\hat{R}$ in the ideal world such that the outputs of R and $\hat{R}$ are indistinguishable.

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

2.3. Complexity assumptions

Let $\mathbb{G}$ and $\mathbb{G}_\tau$ be two multiplicative cyclic groups with prime order p, and g be a generator of $\mathbb{G}$. A bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow$

$\mathbb{G}_\tau$ is a map with the following properties:

(1) Bilinearity: for all $\mu, \nu \in \mathbb{G}$ and $x, y \in \mathbb{Z}_p$, $e(\mu^x, \nu^y) = e(\mu, \nu)^{xy}$.
(2) Non-degeneracy: $e(g, g) \neq 1$, where 1 is the identity in $\mathbb{G}_\tau$.
(3) Computability: there exists an efficient algorithm to compute $e(\mu, \nu)$, for all $\mu, \nu \in \mathbb{G}$.

Let $\mathcal{GG}(1^\ell)$ be a bilinear group generator that takes as input 1^ℓ and outputs the description of groups $\mathbb{G}$ and $\mathbb{G}_\tau$ with prime order p and a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_\tau$. Let $\mathcal{G}(1^\ell)$ be a group generator which takes as input 1^ℓ and output the description of group $\mathbb{G}$ with prime order p.

DEFINITION 2.3. (Decisional Bilinear Diffie-Hellman (DBDH) Assumption) [17]. *Let* $a, b, c, \overset{R}{\leftarrow} \mathbb{Z}_p$, *and* g *be the generator of* $\mathbb{G}$. *The DBDH assumption holds in the bilinear group* $(e, \mathbb{G}, \mathbb{G}_\tau) \leftarrow \mathcal{GG}(1^\ell)$, *if no probabilistic polynomial-time adversary* $\mathcal{A}$ *can distinguish* $(A, B, C, Z) = (g^a, g^b, g^c, e(g, g)^{abc})$ *from* $(A, B, C, Z) = e(g^a, g^b, g^c, e(g, g)^z)$ *with the advantage*

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

where the probability is over the random choice of $a, b, c, z \overset{R}{\leftarrow} \mathbb{Z}_p$ *and the random bits consumed by the adversary* $\mathcal{A}$.

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

$$\mathrm{Adv}_{\mathcal{A}}^{\text{CT-CDH}} = \Pr[\{(\theta_{\rho+1}, i_{\rho+1}), \ldots, (\theta_1, i_1)\} \leftarrow \mathcal{A}^{T_{\mathbb{G}}(\cdot), H_{\mathbb{G}}(\cdot)}(p, \mathcal{H}, g, g^x)] > \epsilon(\ell),$$

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

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 $\mathcal{A}$ queries the help oracle on the elements of $\mathbb{G}$ for q_H times, she cannot compute a new element of $\mathbb{G}$ 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 $\mathbb{G}$. We will prove that the proposed XCT-CD assumption and the CT-CDH assumption are equivalent.

DEFINITION 2.5 (E𝕏tended XCT-CDH Assumption). *Let* g *be a generator of the group* $\mathbb{G} \leftarrow \mathcal{G}(1^\ell)$ *with prime order* p, *and* $x \overset{R}{\leftarrow} \mathbb{Z}_p$. $H_{\mathbb{G}}(\cdot)$ *is a help oracle, which takes as input* $g_i \in \mathbb{G}$, *and outputs* $g_i^x \in \mathbb{G}$. *Given the* $(\rho + 1)$*-tuple* $(g^{a_1}, g^{a_2}, \ldots, g^{a_{\rho+1}})$, *the XCT-CDH assumption holds in* $\mathbb{G}$, *if no probabilistic polynomial-time adversary* $\mathcal{A}$

$$\mathrm{Adv}_{\mathcal{A}}^{\text{XCT-CDH}} = \Pr[g^{xa_{j_{\rho+1}}} \leftarrow \mathcal{A}^{H_{\mathbb{G}}(\cdot)}(p, g, g^x, g^{a_{j_1}}, g^{a_{j_2}}, \ldots, g^{a_{j_\rho}})] > \epsilon(\ell),$$

where $a_{j_l} \in \{a_1, a_2, \ldots, a_{\rho+1}\} \subseteq \mathbb{Z}_p^{\rho+1}$, *for* $l = 1, 2, \ldots, \rho+1$.

THEOREM 2.1. *XCT-CDH assumption and CT-CDH assumption are equivalent.*

Proof. Given the $(\rho + 1)$-tuple $\{g^{a_1}, g^{a_2}, \ldots, g^{a_{\rho+1}}\}$, we define $\mathcal{H} : l \to g^{a_{i_l}} \in \mathbb{G}$, where $a_{i_l} \in \{a_1, a_2, \ldots, a_{\rho+1}\}$, for $l = 1, 2, \ldots, \rho + 1$; otherwise $\mathcal{H} : l \to g^{b_l}$, where $b_l \overset{R}{\leftarrow} \mathbb{Z}_p$. So, $\mathcal{H}(\cdot)$ is a cryptographic hash function.

On the one hand, if $\mathcal{A}$ can break the XCT-CDH assumption, we will show that there exists an algorithm $\mathcal{B}$ that can use $\mathcal{A}$ to break the CT-CDH assumption. When $\mathcal{A}$ queries help oracle on $\{g^{a_{i_1}}, g^{a_{i_2}}, \ldots, g^{a_{i_\rho}}\}$, the challenger queries the help oracle $H_{\mathbb{G}}(\cdot)$ in CT-CDH assumption, and responds with $\{g^{xa_{i_1}}, g^{xa_{i_2}}, \ldots, g^{xa_{i_\rho}}\}$, where $\rho = q_H$. If $\mathcal{A}$ can output $g^{xa_{i_{\rho+1}}}$, $\mathcal{B}$ can compute $\theta_{\rho+1} = g_{i_{\rho+1}}^x$, where $\mathcal{H}(\rho + 1) = g_{i_{\rho+1}} = g^{a_{i_{\rho+1}}}$ and $\rho + 1 = q_H + 1 > q_H$. So, $\mathcal{B}$ can break the CT-CDH assumption.

On the other hand, if the adversary $\mathcal{A}$ can break the CT-CDH assumption, we will show that there exists an algorithm $\mathcal{B}$, who can use $\mathcal{A}$ to break the XCT-CDH assumption. Given $\{g^{a_1}, g^{a_2}, \ldots, g^{a_{\rho+1}}\}$, for q_T $(q_T \leq \rho + 1)$ target oracle queries, the challenger responds with $g^{a_{i_1}}, g^{a_{i_2}}, \ldots, g^{a_{i_{q_T}}}$, where $a_{i_j} \in \{a_1, a_2, \ldots, a_{\rho+1}\}$, for $j = 1, 2, \ldots, q_T$. For q_H $(q_H \leq \rho)$ help oracle queries, the challenger queries the help oracle $H_{\mathbb{G}}(\cdot)$ in the XCT-CDH assumption, and responds with $\{g^{xa_{i_1}}, g^{xa_{i_2}}, \ldots, g^{xa_{i_{q_H}}}\}$, where $a_{i_l} \in \{a_1, a_2, \ldots, a_{\rho+1}\}$, for $l = 1, 2, \ldots, q_H$. If $\mathcal{A}$ can compute $\theta_{\rho+1} = g_{i_{\rho+1}}^x$, $\mathcal{B}$ can compute $g^{xa_{i_{\rho+1}}} = g_{i_{\rho+1}}^x$, where $\mathcal{H}(\rho + 1) = g_{i_{\rho+1}} = g^{a_{i_{\rho+1}}}$. So, $\mathcal{B}$ can break the XCT-CDH assumption.

Therefore, the XCT-CDH assumption is equivalent to the CT-CDH assumption. □

Note that the XCT-CDH assumption is the computational Diffie-Hellman (CDH) assumption, if the help oracle $H_{\mathbb{G}}(\cdot)$ in the XCT-CDH assumption is canceled.

Indistinguishability. We define that two distribution families $\Omega_1(\ell)$ and $\Omega_2(\ell)$ are (statistically) indistinguishable, if

$$\sum_y |\Pr_{x \in \Omega_1(\ell)}[x = y] - \Pr_{x \in \Omega_2(\ell)}[x = y]| \leq \epsilon(\ell).$$

Setup. Taking as input 1^ℓ, this algorithm responds with a bilinear group $(e, p, \mathbb{G}, \mathbb{G}_\tau) \leftarrow \mathcal{GG}(1^\ell)$ with prime order p, where $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_\tau$. Let g, g_2, h be the generators of $\mathbb{G}$. Suppose that the set of universal attributes $\mathcal{U} = \{attr_1, attr_2, \cdots, attr_n\} \subseteq \{0,1\}^n$. For each $attr_j \in \mathcal{U}$, it chooses $A_j \overset{R}{\leftarrow} \mathbb{G}$. It generates a master secret-public key pair $(\alpha, g_1) \leftarrow \mathcal{KG}(1^\ell)$, where $\alpha \overset{R}{\leftarrow} \mathbb{Z}_p$ and $g_1 = g^\alpha$. The public key is

$$(e, p, \mathbb{G}, \mathbb{G}_\tau, g, g_1, g_2, h, A_1, A_2, \cdots, A_n)$$

Key Generation. To generate a private key for a set of attributes $S_U = \{attr_{i_1}, attr_{i_2}, \cdots, attr_{i_\gamma}\} \subseteq \mathcal{U}$, this algorithm chooses $r_U \overset{R}{\leftarrow} \mathbb{Z}_p$, and computes

$$a_U = g^{r_U},\ b_U = g_2^\alpha h^{r_U},\ s_{i_1} = A_{i_1}^{r_U},\ s_{i_2} = A_{i_2}^{r_U}, \cdots,\ s_{i_\gamma} = A_{i_\gamma}^{r_U}$$

The secret key for the set of attributes S_U is $SK_U = \{a_U, b_U, s_{i_1}, s_{i_2}, \cdots, s_{i_\gamma}\}$.
These secret keys can be verified as follows:

$$e(g, b_U) = e(g_1, g_2)e(a_U, h)$$

and

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

for $j = 1, 2, \cdots, \gamma$.

Encryption. Let $\mathbb{A}$ be a monotonic access structure and $S_C \in \mathbb{A}$ be the minimal set in $\mathbb{A}$ [57][a]. To encrypt a message $M \in \mathbb{G}_\tau$ under $S_C = \{attr_{c_1}, attr_{c_2}, \cdots, attr_{c_t}\} \in \mathbb{A}$, this algorithm chooses $\omega \overset{R}{\leftarrow} \mathbb{Z}_p$, and computes

$$C_1 = g^w,\ C_2 = (h \prod_{j=1}^{t} A_{c_j})^\omega,\ C_3 = e(g_1, g_2)^\omega \cdot M$$

The ciphertext is $C = (C_1, C_2, C_3)$.

Decryption. To decrypt the ciphertext $C = (C_1, C_2, C_3)$, the following steps are proceeded.

1. Compute $s_c = b_U \prod_{j=1}^{t} s_{c_j}$, where $s_{c_j} \in SK_U$ and $S_C \subseteq S_U \in \mathbb{A}$.
2. Compute
$$C_3 \cdot \frac{e(a_U, C_2)}{e(s_c, C_1)} = M$$

[a] By $S_C \in \mathbb{A}$ is the minimal set of $\mathbb{A}$, we mean that $S_C \subseteq S$ if $S \in \mathbb{A}$.

FIGURE 1. ABE with constant cost.

3. EFFICIENT ABE WITH CONSTANT COST

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.

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

$$= e(g, h)^{r_U \omega} \prod_{j=1}^{t} e(g, A_{c_j})^{r_U \omega}, \qquad (1)$$

$$s_c = b_U \prod_{j=1}^{t} s_{c_j} = g_2^\alpha h^{r_U} \prod_{j=1}^{t} A_{c_j}^{r_U} \qquad (2)$$

$$e(C_1, s_c) = e\left(g^\omega, g_2^\alpha h^{r_U} \prod_{j=1}^{t} A_{c_j}^{r_U}\right)$$

$$= e(g^\alpha, g_2)^\omega e(g, h)^{r_U \omega} \prod_{j=1}^{t} e(g, A_{c_j})^{r_U \omega}$$

$$= e(g_1, g_2)^\omega e(a_U, C_2) \qquad (3)$$

and

$$
\begin{aligned}
C_3 \cdot \frac{e(a_U, C_2)}{e(C_1, s_c)} &= M \cdot e(g_1, g_2)^{\omega} \cdot \frac{e(a_U, C_2)}{e(g_1, g_2)^{\omega} e(a_U, C_2)} \\
&= M \cdot e(g_1, g_2)^{\omega} \cdot \frac{1}{e(g_1, g_2)^{\omega}} \\
&= M. \qquad (4)
\end{aligned}
$$

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

$$T' = T + (|\mathcal{U}| + 4(q+1) + 3(|S_1| + |S_2| + \cdots + |S_q|))T_{\exp}$$

and

$$\epsilon'(\ell) = \frac{\epsilon(\ell)}{2}.$$

$T_{\exp}$ denotes the running time of one exponentiation, $\mathcal{U}$ 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 $\mathcal{A}$ who can (T, q, ϵ) break our ABE in the selective-attribute model, we will show that there exists an algorithm $\mathcal{B}$ who can (T', ϵ') break the decisional bilinear Diffie-Hellman assumption as follows.

The challenger generates the bilinear group $(e, p, \mathbb{G}, \mathbb{G}_\tau) \leftarrow \mathcal{GG}(1^\lambda)$, and chooses a generator $g \in \mathbb{G}$. It flips an unbiased coin μ from $\{0, 1\}$. If $\mu = 0$, the challenger sends $(A, B, C, Z) = (g^a, g^b, g^c, e(g, g)^{abc})$ to $\mathcal{B}$; otherwise, the challenger sends $(A, B, C, Z) = (g^a, g^b, g^c, e(g, g)^z)$ to $\mathcal{B}$, where $z \overset{R}{\leftarrow} \mathbb{Z}_p$. $\mathcal{B}$ will output his guess μ' on μ. $\mathcal{B}$ sets $g_1 = g^a$, $g_2 = g^b$ and $g_3 = g^c$.

Initialization. The adversary submits an attribute $S^* = \{\mathrm{attr}_i\}$.

Setup. $\mathcal{B}$ selects n random integers $e_1, e_2, \ldots, e_n \overset{R}{\leftarrow} \mathbb{Z}_p$, and computes $A_i = g_1^{e_i}$ and $A_j = g^{e_j}$, for $j \in \{1, 2, \ldots, n\} \setminus \{i\}$. $\mathcal{B}$ chooses $\gamma \overset{R}{\leftarrow} \mathbb{Z}_p$, and sets $h = g_1^{-e_i} g^{\gamma}$.

$\mathcal{B}$ sends $\mathcal{A}$ the public parameters

$$(e, \mathbb{G}, \mathbb{G}_\tau, g, g_1, g_2, h, A_1, A_2, \ldots, A_n).$$

Phase 1. $\mathcal{A}$ queries secret keys on the set of attributes $S_\sigma = \{\mathrm{attr}_{\sigma_1}, \mathrm{attr}_{\sigma_2}, \ldots, \mathrm{attr}_{\sigma_\rho}\}$, where $\sigma = 1, 2, \ldots, q_1$, $\sigma_\rho < n$ and $S^* \not\subseteq S_{\sigma_i}$, for $i = 1, 2, \ldots, q_1$. $\mathcal{B}$ chooses $r_\sigma \overset{R}{\leftarrow} \mathbb{Z}_p$, and computes

$$a_\sigma = g^{-r_\sigma} g_2^{1/e_i}, \quad b_\sigma = g_2^{\gamma/e_i} h^{-r_\sigma}, \quad s_{\sigma_j} = (g^{-r_\sigma} g_2^{1/e_i})^{e_{\sigma_j}}$$

for $j = 1, 2, \ldots, \sigma_\rho$, and $\sigma = 1, 2, \ldots, q_1$.

We claim that $\{a_\sigma, b_\sigma, (s_{\sigma_j})_{j=1}^{\rho}\}$ are correctly distributed. Because, we have

$$
\begin{aligned}
g_2^{\gamma/e_i} h^{-r_\sigma} &= g_1^{b\gamma/ae_i} (g_1^{-e_i+\gamma/a})^{-r_\sigma} \\
&= (g_1^{-e_i+\gamma/a})^{b/e_i} g_1^{b} (g_1^{-e_i+\gamma/a})^{-r_\sigma} \\
&= g_1^{b} (g_1^{-e_i+\gamma/a})^{-r_\sigma+b/e_i} \\
&= g_2^{a} (g_1^{-e_i} g^{\gamma})^{-r_\sigma+b/e_i} \\
&= g_2^{a} h^{-r_\sigma+b/e_i}.
\end{aligned}
$$

Let $\hat{r}_\sigma = -r_\sigma + b/e_i$, we have

$$
\begin{aligned}
g_2^{\gamma/e_i} h^{-r_\sigma} &= g_2^{a} h^{\hat{r}_\sigma}, \\
g^{-r_\sigma} g_2^{1/e_i} &= g^{-r_\sigma+b/e_i} = g^{\hat{r}_\sigma}
\end{aligned}
$$

and

$$(g^{-r_\sigma} g_2^{1/e_i})^{e_{\sigma_j}} = (g^{-r_\sigma+b/e_i})^{e_{\sigma_j}} = (g^{\hat{r}_\sigma})^{e_{\sigma_j}} = A_{\sigma_j}^{\hat{r}_\sigma}.$$

Challenge. $\mathcal{A}$ sends $\mathcal{B}$ two messages M_0 and M_1. $\mathcal{B}$ flips an unbiased coin from $\{0, 1\}$, and gets back with $\hat{\mu} \in \{0, 1\}$. $\mathcal{B}$ chooses $S = \{\mathrm{attr}_i, \mathrm{attr}_{\lambda_1}, \mathrm{attr}_{\lambda_2}, \ldots, \mathrm{attr}_{\lambda_\pi}\} \subseteq \mathcal{U}$, and computes

$$C_1^* = g_3, \quad C_2 = g_3^{\gamma + \sum_{j=1}^{\pi} e_{\lambda_j}}, \quad C_3^* = Z \cdot M_{\hat{\mu}},$$

where $S^* \subseteq S$.

$\mathcal{B}$ responds with the challenge ciphertext $C^* = (C_1^*, C_2^*, C_3^*)$. So, $C^* = (g^c,\ (hA_i \prod_{j=1}^{\pi} A_{\lambda_j})^c,\ Z \cdot M_{\hat{\mu}})$ is a valid encryption of $M_{\hat{u}}$ with the correct distribution whenever $Z = e(g, g)^{abc}$.

Phase 2. $\mathcal{A}$ can query secret keys for sets of attributes $S_{q_1+1}, S_{q_1+2}, \ldots, S_q$, where the only constraint is $S^* \not\subseteq S_\sigma$, for $\sigma = 1, 2, \ldots, q$. $\mathcal{B}$ responds as Phase 1.

Guess. $\mathcal{A}$ outputs his guess $\tilde{\mu}$ on $\hat{\mu}$. If $\tilde{\mu} = \hat{\mu}$, $\mathcal{B}$ outputs $\mu' = 0$; otherwise $\mathcal{B}$ 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 $\mathcal{B}$ 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, $\mathcal{A}$ can output $\tilde{\mu} = \hat{\mu}$ with advantage at least $\epsilon(\ell)$, namely $\Pr[\tilde{\mu} = \hat{\mu} | \mu = 0] \geq \frac{1}{2} + \epsilon(\ell)$. Since $\mathcal{B}$ guesses $\mu' = 0$ when $\tilde{\mu} = \hat{\mu}$, we have $\Pr[\mu' = \mu | \mu = 0] \geq \frac{1}{2} + \epsilon(\ell)$.

If $\mu = 1$, $\mathcal{A}$ can obtain no information about $\hat{\mu}$. Therefore, $\mathcal{A}$ can output $\tilde{\mu} \neq \hat{\mu}$ with no advantage, namely $\Pr[\tilde{\mu} \neq \hat{\mu} | \mu = 1] = \frac{1}{2}$. Since $\mathcal{B}$ guesses $\mu' = 1$ when $\tilde{\mu} \neq \hat{\mu}$, we have $\Pr[\mu' = \mu | \mu = 1] = \frac{1}{2}$

So, the advantage that $\mathcal{B}$ can break the DBDH assumption is

$$
\begin{aligned}
&\tfrac{1}{2}\Pr[\mu' = \mu | \mu = 0] + \tfrac{1}{2}\Pr[\mu' = \mu | \mu = 1] - \tfrac{1}{2}| \\
&\quad \geq \tfrac{1}{2} \times (\tfrac{1}{2} + \epsilon(\ell)) + \tfrac{1}{2} \times \tfrac{1}{2} - \tfrac{1}{2} = \tfrac{\epsilon(\ell)}{2}.
\end{aligned}
$$

□

TABLE 1. The comparison of computation cost.

Schemes	Setup	Key generation	Encryption	Decryption
SW [21]	$(\|\mathcal{U}\| + 1)E$	$\|S_U\|E$	$\|S_C\|E$	$\|S_C\|E + \|S_C\|P$
GPSW [23]	$(\|\mathcal{U}\| + 1)E$	$\|S_U\|E$	$\|S_C\|E$	$\|S_C\|E + \|S_C\|P$
OSW [24]	$2(\|\mathcal{U}\| + 1)E$	$3\|S_U\|E$	$2(\|S_C\| + 1)E$	$\|S_C\|E + \|S_C\|P$
BSW [25]	$3E$	$2(\|S_U + 1\|)E$	$2(\|(S_C\| + 1)\|E$	$\|S_C\|E + \|S_C\|P$
CN [26]	$(3\|\mathcal{U}\| + 1)E$	$(\|\mathcal{U}\| + \|S_U\|)E$	$(\|\mathcal{U}\| + 2)E$	$\|\mathcal{U}\|P$
HLR [27]	$2(\|\mathcal{U} + 1\|)E$	$(\|\mathcal{U}\| + \|S_U\|)E$	$3E$	$(\frac{\|S_C\|(\|S_C\|-1)}{2} + 2)E + 3P$
LOSTW [28]	$(\|\mathcal{U}\| + 2)E$	$(\|S_U\| + 2)E$	$(3\|S_C\| + 2)E$	$\|S_C\|E + (2\|S_C\| + 1)P$
Waters [29]	$3E$	$(\|S_U\| + 2)E$	$2(\|S_C\| + 1)E$	$\|S_C\|E + (2\|S_C\| + 1)P$
ZH [36]	$6\|\mathcal{U}\|E$	$(\|S_U\| + 1)E$	$3E$	$(2\|S_C\| + 1)P$
EMONS [37]	$(\|\mathcal{U}\| + 1)E$	$4E$	$3E$	$2P$
ALP [38]	$(2\|\mathcal{U}\| + 1)E$	$(5\|S_U\| - 2)E$	$4E$	$(2\|\mathcal{U}\| - 1)E + 2\|S_C\|P$
CZF [39]	$2\|\mathcal{U}\|(E + P)$	$\|S_U\|E$	$3E$	$2P$
Our scheme	$2E$	$(\|S_U\| + 2)E$	$3E$	$2P$

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

Schemes	KP/CP-ABE	Access structure	Security model	Length of ciphertext
SW [21]	KP-ABE	Monotonic	Selective-set	$\|S_C\|E_{\mathbb{G}} + E_{\mathbb{G}_\tau}$
GPSW [23]	KP-ABE	Monotonic	Selective-set	$\|S_C\|E_{\mathbb{G}} + E_{\mathbb{G}_\tau}$
OSW [24]	KP-ABE	Non-monotonic	Selective-set	$(\|S_C\| + 1)E_{\mathbb{G}} + E_{\mathbb{G}_\tau}$
BSW [25]	CP-ABE	Monotonic	Full security	$(\|S_C\| + 2)E_{\mathbb{G}} + E_{\mathbb{G}_\tau}$
CN [26]	CP-ABE	Non-monotonic	Selective-set	$(\|S_C\| + 1)E_{\mathbb{G}} + E_{\mathbb{G}_\tau}$
HLR [27]	CP-ABE	Monotonic	Selective-set	$2E_{\mathbb{G}} + 2E_{\mathbb{G}_\tau}$
LOSTW [28]	CP-ABE	Monotonic	Full security	$(2\|S_C\| + 1)E_{\mathbb{G}} + E_{\mathbb{G}_\tau}$
Waters [29]	CP-ABE	Monotonic	Selective-set	$(2\|S_C\| + 1)E_{\mathbb{G}} + E_{\mathbb{G}_\tau}$
ZH [36]	CP-ABE	Non-monotonic	Selective-set	$2E_{\mathbb{G}} + E_{\mathbb{G}_\tau}$
EMONS [37]	CP-ABE	Monotonic	Selective-set	$2E_{\mathbb{G}} + E_{\mathbb{G}_\tau}$
ALP [38]	KP-ABE	Non-monotonic	Selective-set	$3E_{\mathbb{G}} + E_{\mathbb{G}_\tau}$
CZF [39]	KP-ABE	Non-monotonic	Selective-set	$2E_{\mathbb{G}} + E_{\mathbb{G}_\tau}$
Our scheme	CP-ABE	Monotonic	Selective-attribute	$2E_{\mathbb{G}} + E_{\mathbb{G}_\tau}$

Comparison. We compare our scheme with previous schemes in Tables 1 and 2. By $\mathcal{U}$, S_U and S_C, we denote the set of universal attributes, the set of attributes which the user holds and the set of attributes which the ciphertext requires, respectively. By E and P, we denote one exponentiation and one pairing, respectively. By $E_{\mathbb{G}}$ and $E_{\mathbb{G}_\tau}$, we denote one element in $\mathbb{G}$ and one element in $\mathbb{G}_\tau$, respectively.

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.

Setup. Taking as input 1^{ℓ} , this algorithm responds with bilinear group $(e, p, \mathbb{G}, \mathbb{G}_{\tau}) \leftarrow \mathcal{GG}(1^{\ell})$ with prime order p, where $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_{\tau}$. Let g, g_2, h be the generators of $\mathbb{G}$, and the set of universal attributes $\mathcal{U} = \{attr_1, attr_2, \cdots, attr_n\} \subseteq \{0,1\}^n$.

The issuer generates his master secret-public key pair $(\alpha, g_1) \leftarrow \mathcal{KG}(1^{\ell})$, where $\alpha \overset{R}{\leftarrow} \mathbb{Z}_p$ and $g_1 = g^{\alpha}$. For each $attr_j \in \mathcal{U}$, he chooses $A_j \overset{R}{\leftarrow} \mathbb{G}$. The public key is

$$(e, p, \mathbb{G}, \mathbb{G}_{\tau}, g, g_1, g_2, h, A_1, A_2, \cdots, A_n).$$

Key Generation. To generate a private key for a set of attributes $S_U = \{attr_{i_1}, attr_{i_2}, \cdots, attr_{i_{\gamma}}\} \subseteq \mathcal{U}$, The issuer chooses $r_U \overset{R}{\leftarrow} \mathbb{Z}_p$, and computes

$$a_U = g^{r_U},\ b_U = g_2^{\alpha} h^{r_U},\ s_{i_1} = A_{i_1}^{r_U},\ s_{i_2} = A_{i_2}^{r_U}, \cdots,\ s_{i_{\gamma}} = A_{i_{\gamma}}^{r_U}$$

The secret keys for the set of attributes S_U is $SK_U = \{a_U, b_U, s_{i_1}, s_{i_2}, \cdots, s_{i_{\gamma}}\}$.
These secret keys can be verified as follows:

$$e(g, b_U) = e(g_1, g_2) \cdot e(a_U, h)$$

and

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

for $j = 1, 2, \cdots, \gamma$.

Commitment Phase. Suppose that the sender has m messages $\mathcal{M} = \{M_1, M_2, \cdots, M_m\} \in \mathbb{G}_{\tau}^m$. Let $\mathbb{A}_i$ be monotonic access structure and $S_{C_i} \in \mathbb{A}_i$ be the minimal set in $\mathbb{A}_i$ [57][a].

1. The sender generates his secret-public pair $(\vartheta, \mathfrak{g}) \leftarrow \mathcal{KG}(1^{\ell})$, where $\vartheta \overset{R}{\leftarrow} \mathbb{Z}_p$ and $\mathfrak{g} = e(g_1, g_2)^{\vartheta}$.
2. To commit a message M_j under the attribute set $S_{C_j} = \{attr_{j_1}, attr_{j_2}, \cdots, attr_{j_t}\} \in \mathbb{A}_j$, the sender chooses $\omega_j \overset{R}{\leftarrow} \mathbb{Z}_p$, and computes

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

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

Transfer Phase.

1. R adaptively chooses $\sigma_z \in \{1, 2, \cdots, m\}$, and computes $s_z = b_U \prod_{j=1}^{|S_{C_{\sigma_z}}|} s_{\sigma_{z_j}}$, where $s_{\sigma_{z_j}} \in SK_U$ and $S_{C_{\sigma_z}} \subseteq S_U \in \mathbb{A}_{\sigma_z}$. He computes $\Gamma_z = \frac{e(C_{\sigma_{z_1}}, s_z)}{e(a_U, C_{\sigma_{z_2}})}$. The receiver chooses $x_z \overset{R}{\leftarrow} \mathbb{Z}_p$, and computes $\Theta_z = \Gamma_z^{x_z}$, for $z = 1, 2, \cdots, k$.
2. $R \xrightarrow{\Theta_z} S$. The receiver sends Θ_z to the sender.
3. $R \xleftarrow{\Phi_z} S$. The sender computes $\Phi_z = \Theta_z^{\vartheta}$, and sends Φ_z to the receiver.
4. The receiver computes $\Psi_z = \Phi_z^{x_z^{-1}}$ and $M_{\sigma_z} = \frac{C_{\sigma_{z3}}}{\Psi_z}$, for $z = 1, 2, \cdots, k$.

[a] By $S_{C_i} \in \mathbb{A}_i$ be the minimal set of $\mathbb{A}_i$, we mean that $S_C \subseteq S$ if $S \in \mathbb{A}_i$.

FIGURE 2. Attribute-based oblivious access control.

Correctness. From Equations (1)–(3) in Section 3, we have

$$\Gamma_z = \frac{e(C_{\sigma_{z_1}}, s_z)}{e(a_U, C_{\sigma_{z_2}})} = \frac{e(g_1, g_2)^{\omega_{\sigma_z}} e(a_U, C_{\sigma_{z_2}})}{e(a_U, C_{\sigma_{z_2}})} = e(g_1, g_2)^{\omega_{\sigma_z}}, \tag{5}$$

$$\Theta_z = \Gamma_z^{x_z} = e(g_1, g_2)^{\omega_{\sigma_z} x_z}, \tag{6}$$

$$\Phi_z = \Theta_z^{\vartheta} = e(g_1, g_2)^{\vartheta \omega_{\sigma_z} x_z}, \tag{7}$$

$$\Psi_z = \Phi_z^{x_z^{-1}} = e(g_1, g_2)^{\vartheta \omega_{\sigma_z}} \tag{8}$$

and

$$\frac{C_{\sigma_{z_3}}}{\Psi_z} = \frac{e(g_1, g_2)^{\vartheta \omega_{\sigma_z}} \cdot M_{\sigma_z}}{e(g_1, g_2)^{\vartheta \omega_{\sigma_z}}} = M_{\sigma_z}. \tag{9}$$

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

Proof. For any Θ_j received by the sender from the receiver, there exists an x_i such that

$$\Theta_j = e(g_1, g_2)^{\omega_{\sigma_j} x_j} = e(g_1, g_2)^{\omega_{\sigma_i} x_i} = \Theta_i,$$

namely $x_i = \omega_{\sigma_j} x_j / \omega_{\sigma_i} \bmod p$. Therefore, from the view of the sender, whether Θ_j is computed from C_{σ_j} or C_{σ_i} 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 $\mathbb{G}_\tau$.*

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 $C_i^* \xleftarrow{R} \mathbb{G}^2 \times \mathbb{G}_\tau$.
(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 $(\Gamma_j^*, \Theta_j^*) \xleftarrow{R} \mathbb{G}^2$, 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 $H_{\mathbb{G}_\tau}(\cdot)$ on $\{\Theta_1^*, \Theta_2^*, \ldots, \Theta_k^*\}$, and gets back with $\{\Phi_1^*, \Phi_2^*, \ldots, \Phi_k^*\}$, where $\Phi_j^* = (\Theta_j^*)^{\vartheta^*}$, for $j = 1, 2, \ldots, k$.
(5) If $\hat{R}$ can output Ψ_j, $\hat{R}^*$ sends σ_j to Charlie. Charlie responds with $C_{\sigma_{j3}}^* / M_{\sigma_j}$.
(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 Ψ_j, for $j = 1, 2, \ldots, k+1$. Therefore, after receiving $(e(g_1, g)^{\omega_{\sigma_1}})^{\vartheta}, (e(g_1, g)^{\omega_{\sigma_2}})^{\vartheta}, \ldots, (e(g_1, g)^{\omega_{\sigma_k}})^{\vartheta}$, $\hat{R}$ can compute $(e(g_1, g)^{\omega_{\sigma_{k+1}}})^{\vartheta}$. This will contradict the XCT-CDH assumption. So, $\hat{R}$ can obtain at most k messages.

$\{\Gamma_1, \Gamma_2, \ldots, \Gamma_k\}$ and $\{\Theta_1, \Theta_2, \ldots, \Theta_k\}$ are random elements in $\mathbb{G}_\tau$. $\{C_1, C_2, \ldots, C_m\}$ are random elements in $\mathbb{G}^2 \times \mathbb{G}_\tau$. $\{\Phi_1, \Phi_2, \ldots, \Phi_k\}$ and $\{\Phi_1^*, \Phi_2^*, \ldots, \Phi_k^*\}$ 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 $\mathbb{G}_\tau$.*

Proof. There are two kinds of adversaries:

Type-I. The adversary can compute Γ_j from the ciphertext (C_{j_1}, C_{j_2}), then acts as a legal receiver to interact with the sender.
Type-II. The adversary can compute M_j from $(C_{j_1}, C_{j_2}, C_{j_3})$.

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 $\mathcal{A}$ is Type-I adversary, he can compute Γ_j from the ciphertext (C_{j_1}, C_{j_2}). There exists an algorithm $\mathcal{B}$ who can use $\mathcal{A}$ 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 $C'_j = (C'_{j_1}, C'_{j_2}, C'_{j_3})$, where $C'_{j_i} = C_{j_i}$, for $i = 1, 2$. $\mathcal{B}$ sends (C'_{j_1}, C'_{j_2}) to $\mathcal{A}$. If $\mathcal{A}$ can compute Γ_j, $\mathcal{B}$ can compute $M_j = \frac{C'_{j_3}}{\Gamma_j}$. This will contradict Theorem 1.
Type-II. Suppose $\mathcal{A}$ is Type-II adversary, he can compute the M_j from $(C_{j_1}, C_{j_2}, C_{j_3})$. There exists an algorithm $\mathcal{B}$ who can use $\mathcal{A}$ to break the XCT-CDH assumption as follows. Given $e(g_1, g_2)^{\vartheta}, e(g_1, g)^{\omega_j}$, $e(g_1, h \prod_{\mathrm{attr}_i \in S_j} A_i)^{\omega_j}$, the aim of $\mathcal{B}$ is to compute $(e(g_1, g_2)^{\vartheta})^{\omega_i}$. $\mathcal{B}$ sends $C_j = (C_{j_1}, C_{j_2}, C_{j_3})$ to $\mathcal{A}$. If $\mathcal{A}$ can output M_j, $\mathcal{B}$ can compute $(e(g_1, g_2)^{\vartheta})^{\omega_j} = \frac{C_{j3}}{M_j}$. So $\mathcal{B}$ can use $\mathcal{A}$ 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 $E_{\mathbb{G}}$ and $E_{\mathbb{G}_\tau}$, we denote one element in $\mathbb{G}$ and one element in $\mathbb{G}_\tau$, respectively.

TABLE 3. The computation cost of Our ABOAC.

	Computation cost					
	Setup	Key generation		Commitment	Transfer	
Scheme	I	I	R	S	R	S
ABOAC	$2E$	$(\lvert S_U\rvert + 2)E$	$(2(\lvert S_U\rvert + 1)P$	$3mE$	$2kE + 2 + kP$	kE

TABLE 4. The communication cost of our ABOAC.

	Communication cost			
	Key generation	Commitment	Transfer	
Scheme	I → R	S → R	R → S	R ← S
ABOAC	$(\lvert S_U\rvert + 2)E_{\mathbb{G}}$	$2mE_{\mathbb{G}} + mE_{\mathbb{G}_\tau}$	$kE_{\mathbb{G}_\tau}$	$kE_{\mathbb{G}_\tau}$

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

[1] NCSC-TG-003-87 (1987) *A Guide to Understanding Discretionary Access Control in Trusted Systems*. National Computer Security Center, Maryland, USA.

[2] DoD-5200.28-STD (1985) *Department of Defense Trusted Computer System Evaluation Criteria*. Department of Defense Standard, USA.

[3] Blaze, M., Feigenbaum, J. and Lacy, J. (1996) Decentralized Trust Management. *Proc. S&P 1996*, Oakland, CA, USA, May 6–8, pp. 164–173. IEEE, Washington, DC, USA.

[4] Bobba, R., Fatemieh, O., Khan, F., Gunter, C.A. and Khurana, H. (2006) Using Attribute-based Access Control to Enable Attribute-based Messaging. *Proc. ACSAC 2006*, Miami, FL, USA, December 11–15, pp. 403–413. IEEE, Washington, DC, USA.

[5] Frikken, K., Atallah, M. and Li, J. (2006) Attribute-based access control with hidden policies and hidden credentials. *IEEE Trans. Comput.*, **55**, 1259–1270.

[6] Pirretti, M., Traynor, P., McDaniel, P. and Waters, B. (2006) Secure Attribute Based Systems. *Proc. CCS 2006*, Alexandria, VA, USA, October 30–November 3, pp. 99–112. ACM, New York, NY, USA.

[7] Yuan, E. and Tong, J. (2005) Attributed Based Access Control (abac) for Web Services. *Proc. ICWS 2005*, Orlando, Florida, USA, July 11–15, pp. 561–569. IEEE Washington, DC, USA.

[8] Li, N. and Mitchell, J.C. (2003) RT: A Role-based Trust-management Framework. *Proc. DISCEX 2003*, Washington, DC, USA, April 22–24, pp. 201–212. IEEE, Washington, DC, USA.

[9] Sandhu, R.S., Coyne, E.J., Feinstein, H.L. and Youman, C.E. (1996) Role-based access control models. *IEEE Comput.*, **29**, 38–47.

[10] Li, N. and Tripunitara, M.V. (2006) Security analysis in role-based access control. *ACM Trans. Inf. Syst. Secur.*, **9**, 391–420.

[11] Byun, J.-W., Bertino, E. and Li, N. (2005) Purpose Based Access Control of Complex Data for Privacy Protection. *Proc. SACMAT 2005*, Stockholm, Sweden, June 1–3, pp. 102–110. ACM, New York, NY, USA.

[12] Byun, J.-W. and Li, N. (2008) Purpose based access control for privacy protection in relational database systems. *VLDB J.*, **17**, 603–619.

[13] Zhao, S. and Raychaudhuri, D. (2009) Scalability and performance evaluation of hierarchical hybrid wireless networks. *IEEE/ACM Tran. Netw.*, **17**, 1536–1549.

[14] Sun, Y. and Liu, K.J.R. (2007) Hierarchical group access control for secure multicast communications. *IEEE/ACM Trans. Netw.*, **15**, 1514–1526.

[15] Akyildiz, I.F. and Kasimoglu, I.H. (2004) Wireless sensor and actor networks: research challenges. *Ad Hoc Netw.*, **2**, 351–367.

[16] Nguyen, H.L. and Nguyen, U.T. (2008) A study of different types of attacks on multicast in mobile ad hoc networks. *Ad Hoc Netw.*, **6**, 32–46.

[17] Boneh, D. and Franklin, M.K. (2001) Identity-based Encryption from the Weil Pairing. *Proc. CRYPTO 2001*, Santa Barbara, CA, USA, August 19–23, Lecture Notes in Computer Science 2139, pp. 213–229. Springer, Berlin.

[18] Gentry, C. (2006) Practical Identity-based Encryption Without Random Oracles. *Proc. EUROCRYPT 2006*, Petersburg, Russia, May 28–June 1, Lecture Notes in Computer Science 4004, pp. 445–464. Springer, Berlin.

[19] Shamir, A. (1984) Identity-based Cryptosystems and Signature Schemes. *Proc. CRYPTO 1984*, Santa Barbara, CA, USA, August 19–22, Lecture Notes in Computer Science 196, pp. 47-53. Springer, Berlin.

[20] Waters, B. (2005) Efficient Identity-based Encryption Without Random Oracles. *Proc. EUROCRYPT 2005*, Aarhus, Denmark, May 22–26, Lecture Notes in Computer Science 3494, pp. 114–127. Springer, Berlin.

[21] Sahai, A. and Waters, B. (2005) Fuzzy Identity-based Encryption. *Proc. EUROCRYPT 2005*, Aarhus, Denmark, May 22–26, Lecture Notes in Computer Science 3494, pp. 457–473. Springer, Berlin.

[22] Shamir, A. (1979) How to share a secret. *Commun. ACM*, **22**, 612–613.

[23] Goyal, V., Pandey, O., Sahai, A. and Waters, B. (2006) Attribute-based Encryption for Fine-grained Access Control of Encrypted Data. *Proc. CCS 2006*, Alexandria, VA, USA, October 30–November 3, pp. 89–98. ACM, New York, NY, USA.

[24] Ostrovsky, R., Sahai, A. and Waters, B. (2007) Attribute-based Encryption with Non-monotonic Access Structures. *Proc. CCS 2007*, Alexandria, VA, USA, October 28–31, pp. 195–203. ACM, New York, NY, USA.

[25] Bethencourt, J., Sahai, A. and Waters, B. (2007) Ciphertext-Policy Attribute-based Encryption. *Proc. S&P 2007*, Oakland, CA, USA, May 20–23, pp. 321–34. IEEE, Washington, DC, USA.

[26] Cheung, L. and Newport, C. (2007) Provably Secure Ciphertext Policy ABE. *Proc. CCS 2007*, Alexandria, VA, USA, October 28–31, pp. 456–465. ACM, New York, NY, USA.

[27] Herranz, J., Laguillaumie, F. and Ràfols, C. (2010) Constant Size Ciphertexts in Threshold Attribute-based Encryption. *Proc. PKC 2010*, Paris, France, May 26–28, Lecture Notes in Computer Science 6065, pp. 19–34. Springer, Berlin.

[28] Lewko, A., Okamoto, T., Sahai, A., Takashima, K. and Waters, B. (2010) Fully Secure Functional Encryption: Attribute-based Encryption and (hierarchical) Inner Product Encryption. *Proc. EUROCRYPT 2010*, Riviera, French, May 30–June 3, Lecture Notes in Computer Science 6110, pp. 62–91. Springer, Berlin.

[29] Waters, B. (2011) Ciphertext-Policy Attribute-based Encryption: An Expressive, Efficient, and Provably Secure Realization. *Proc. PKC 2011*, Aormina, Italy, March 6–9, Lecture Notes in Computer Science 6571, pp. 53–70. Springer, Berlin.

[30] Goyal, V., Jain, A., Pandey, O. and Sahai, A. (2008) Bounded Ciphertext Policy Attribute Based Encryption. *Proc. ICALP 2008*, Reykjavik, Iceland, July 7–11, Lecture Notes in Computer Science 5126, pp. 579–591. Springer, Berlin.

[31] Liang, X., Cao, Z. and Lin, H. (2009) Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption. *Proc. ASIACCS 2009*, Sydney, Australia, March 10–12, pp. 343–352. ACM, New York, NY, USA.

[32] Attrapadung, N. and Imai, H. (2009) Dual-Policy Attribute Based Encryption. *Proc. ACNS 2009*, Paris-Rocquencourt, France, June 2–5, Lecture Notes in Computer Science 5536, pp. 168–185. Springer, Berlin.

[33] Chase, M. (2007) Multi-authority Attribute Based Encryption. *Proc. TCC 2007*, Amsterdam, The Netherlands, February 21–24, Lecture Notes in Computer Science 4392, pp. 515–534. Springer, Berlin.

[34] Delerablèe, C. and Pointcheval D. (2008) Dynamic Threshold Public-key Encryption. *Proc. CRYPTO 2008*, Santa Barbara, CA, USA, August 17–21, Lecture Notes in Computer Science 5157, pp. 317–334. Springer, Berlin.

[35] Delerablèe, C., Paillier, P. and Pointcheval, D. (2007) Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys. *Proc. Pairing 2007*, Tokyo, Japan, July 2–4, Lecture Notes in Computer Science 4575, pp. 39–59. Springer, Berlin.

[36] Zhou, Z. and Huang, D. (2010) On Efficient Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption. *Proc. CCS 2010*, Chicago, IL, USA, October 4–8, pp. 753–755. ACM, New York, NY, USA.

[37] Emura, K., Miyaji, A., Nomura, A., Omote, K. and Soshi, M. (2009) A Ciphertextpolicy Attribute-based Encryption Scheme with Constant Ciphertext Length. *Proc. ISPEC 2009*, Xi'an, China, April 13–15, Lecture Notes in Computer Science 5451, pp. 13–23. Springer, Berlin.

[38] Attrapadung, N., Libert, B. and Panafieu, E. (2011) Expressive Key-Policy Attribute-based Encryption with Constant-Size Ciphertexts. *Proc. PKC 2011*, Taormina, Italy, March 6–9, Lecture Notes in Computer Science 6571, pp. 90–108. Springer, Berlin.

[39] Chen, C., Zhang, Z. and Feng, D. (2011) Efficient Ciphertext Policy Attribute-based Encryption with Constant-Size Ciphertext and Constant Computation-Cost. *Proc. ProvSec 2011*, Xi'an, China, October 16–18, Lecture Notes in Computer Science 6980, pp. 84–101. Springer, Berlin.

[40] Ishai, Y., Kushilevitz, E., Ostrovsky, R. and Sahai, A. (2006) Cryptography from Anonymity. *Proc. FOCS 2006*, Berkeley, CA, USA, October 21–24, pp. 239–248. IEEE, Los Alamitos, CA, USA.

[41] Tr-81 Rabin, M.O. (1981) *How to Exchange Secrets by Oblivious Transfer*. Aiken Computation Laboratory, Harvard University.

[42] Naor, M. and Pinkas, B. (1999) Oblivious Transfer and Polynomial Evaluation. *Proc. STOC 1999*, Atlanta, GA, USA, May 1–4, pp. 245–254. ACM, New York, NY, USA.

[43] Naor, M. and Pinkas, B. (1999) Oblivious Transfer with Adaptive Queries. *Proc. CRYPTO 1999*, Santa Barbara, CA, USA, August 15–19, Lecture Notes in Computer Science 1666, pp. 573–590. Springer, Berlin.

[44] Aiello, B., Ishai, Y. and Reingold, O. (2001) Priced Oblivious Transfer: How to Sell Digital Goods. *Proc. EUROCRYPT 2001*, Innsbruck, Austria, May 6–10, Lecture Notes in Computer Science 2045, pp. 119–135. Springer, Berlin.

[45] Coull, S., Green, M. and Hohenberger, S. (2009) Controlling Access to an Oblivious Database Using Stateful Anonymous Credentials. *Proc. PKC 2009*, Irvine, CA, USA, March 18–20, Lecture Notes in Computer Science 5443, pp. 501–520. Springer, Berlin.

[46] Camenisch, J., Dubovitskaya, M. and Neven, G. (2009) Oblivious Transfer with Access Control. *Proc. CCS 2009*, Chicago, IL, USA, November 9–13, pp. 131–140. ACM New York, NY, USA.

[47] Paillier, P. (1999) Public-key Cryptosystems Based on Composite Degree Residuosity Classes. *Proc. EUROCRYPT 1999*, Prague, Czech Republic, May 2–6, Lecture Notes in Computer Science 1592, pp. 223–238. Springer, Berlin.

[48] Freedman, M.J., Nissim, K. and Pinkas, B. (2004) Efficient Private Matching and Set Intersection. *Proc. EUROCRYPT 2004*, Interlaken, Switzerland, May 2–6, Lecture Notes in Computer Science 3027, pp. 1–19. Springer, Berlin.

[49] Zhang, Y., Au, M.H., Wong, D.S., Huang, Q., Mamoulis, N., Cheung, D.W. and Yiu, S.-M. (2010) Oblivious Transfer with Access Control: Realizing Disjunction Without Duplication. *Proc. Pairing 2010*, Yamanaka Hot Spring, Japan, December 13–15, Lecture Notes in Computer Science 6487, pp. 96–115. Springer, Berlin.

[50] Camenisch, J., Neven, G. and Shelat, A. (2007) Simulatable Adaptive Oblivious Transfer. *Proc. EUROCRYPT 2007*, Barcelona, Spain, May 20–24, Lecture Notes in Computer Science 4515, pp. 573–590. Springer, Berlin.

[51] Rial, A. and Preneel, B. (2010) Blind Attribute-based Encryption and Oblivious Transfer with Fine-grained Access Control. *Proc. WISSec 2010*, Nijmegen, Netherlands, November 29–30, pp. 1–20. http://www.cosic.esat.kuleuven.be/publications/article-1419.pdf

[52] Beimel, A. (1996) Secure Schemes for Secret Sharing and Key Distribution. PhD Thesis, Israel Institute of Technology, Technion, Haifa, Israel.

[53] Waters, B. (2009) Dual System Encryption: Realizing Fully Secure IBE and HIBE Under Simple Assumptions. *Proc. CRYPTO 2009*, Santa Barbara, CA, USA, August 16–20, Lecture Notes in Computer Science 5677, pp. 619–636. Springer, Berlin.

[54] Boldyreva, A. (2003) Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie–Hellman-Group Signature Scheme. *Proc. PKC 2003*, Miami, FL, USA, January 6–8, Lecture Notes in Computer Science 2567, pp. 31–46. Springer, Berlin.

[55] Bellare, M., Namprempre, C., Pointcheval, D. and Semanko, M. (2001) The Power of RSA Inversion Oracles and the Security of Chaum's RSA-based Blind Signature Scheme. *Proc. FC 2001*, Grand Cayman, British West Indies, February 19–22, Lecture Notes in Computer Science 2339, pp. 309–328. Springer, Berlin.

[56] Boyen, X. and Waters, B. (2006) Compact Group Signatures Without Random Oracles. *Proc. EUROCRYPT 2006*, St. Petersburg, Russia, May 28–June 1, Lecture Notes in Computer Science 4004, pp. 427–444. Springer, Berlin.

[57] Damgärd, I. and Thorbek, R. (2007) Non-interactive Proofs for Integer Multiplication. *Proc. EUROCRYPT 2007*, Barcelona, Spain, May 20–24, Lecture Notes in Computer Science 4515, pp. 412–429. Springer, Berlin.