Hindawi
Security and Communication Networks
Volume 2018, Article ID 8738960, 10 pages
https://doi.org/10.1155/2018/8738960

Research Article

Two-Party Attribute-Based Key Agreement Protocol with Constant-Size Ciphertext and Key

Jiguo Li,[1,2,3] **Shengzhou Hu**,[2,4] **and Yichen Zhang**[1]

[1] *College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117, Fujian, China*
[2] *College of Computer and Information, Hohai University, Nanjing 211100, Jiangsu, China*
[3] *Jiangsu Key Laboratory of Big Data Security & Intelligent Processing, Nanjing University of Posts and Telecommunications, China*
[4] *Mathematics and Computer Science Department, Gannan Normal University, Ganzhou 341000, Jiangxi, China*

Correspondence should be addressed to Jiguo Li; ljg1688@163.com

Received 14 June 2018; Accepted 4 September 2018; Published 21 October 2018

Academic Editor: David Megias

Based on mutual authentication, the session key is established for communication nodes on the open network. In order to satisfy fine-grained access control for cloud storage, the two-party attribute-based key agreement protocol (TP-AB-KA) was proposed. However, the existing TP-AB-KA protocol is high in the cost of computation and communication and is not unfit for application in a mobile cloud setting because mobile devices are generally resource constrained. To solve the above issue, we propose a TP-AB-KA protocol with constant-size ciphertext and key. Our TP-AB-KA protocol is provable security in the standard model. The concrete proof is given under the augmented multisequence of exponents' decisional Diffie-Hellman (aMSE-DDH) hypothesis in the attribute-based BJM model (AB-BJM). Compared with the existing TP-AB-KA protocols, the computation cost and communication cost of our protocol are largely reduced.

1. Introduction

Key agreement (KA) protocol is an important component in cryptography. By establishing a session key, KA protocol provides security services of confidentiality, integrity, and availability for open communication on the network node. Recently, the two-party attribute-based key agreement protocol (TP-AB-KA) was first proposed in [1]. In TP-AB-KA protocol, the attribute-based encryption (ABE) was adopted for exchanging secret messages from two participants. This kind of protocol carries out negotiating session key based on the mutual authentication of participants' attribute information. Sahai and Waters [2] first proposed ABE, which was used for fine-grained access control for cloud storage. User identity is determined by his/her attributes. ABE is often applied in a one-to-many encryption situation, where data encrypted with certain attributes policy is correctly decrypted by any users whose attributes satisfy that access structure. TP-AB-KA protocol inherits the advantages of ABE schemes, such as using attributes to describe one user and realize the protection of user's identity. This also enables the TP-AB-KA protocols to meet the needs of some specific application scenarios where participants' attributes act as critical factor for mutual authentication.

For example, in an electronic project review system, a reviewer wants to make inquiries for some bidders. Suppose there are n attribute characters in this scene. The role information is described with certain attribute sequence $< \ldots, *_i, *_{i+1}, \ldots >$, which includes n elements in total. The subscripts $i, i+1$ stand for the corresponding locations in the sequence, where we use i location to denote "reviewer" role and $i+1$ location to denote "bidder" role. If a role U_1 is a reviewer, its attribute sequence is instantiated with $< \ldots, 0_i, 1_{i+1}, \ldots >$, where "0" shows "having" certain attribute character and "1" shows "not having". So $< \ldots, 0_i, 1_{i+1}, \ldots >$ shows that U_1 is a reviewer and not a bidder. U_1 obtains the corresponding private key generated by the trusted authority (TA) according to U_1's attribute sequence. In the same way, the authentication policy based on attributes is also described in such way. For instance, there are some qualifications about bidders, such as "A: more than 2 grade enterprise qualification", "B: more than 10 years warranty", etc. Those qualifications are written into a sequence form, that is, $< \ldots, *_j, *_{j+1}, \ldots >$ $(j \neq i)$. j, $j+1$ locations stand for A and B qualifications, respectively. If U_1 wants to talk with a bidder with A and B qualifications, U_1 gives out the corresponding authentication policy $\overline{\overline{A_{Bidder}}} =< \ldots, 0_j, 0_{j+1}, \ldots >$. Two "0" show having A and B qualifications together.

Based on above attribute description, the inquiry procedure of electronic review system is done as follows: Before voting, the reviewers need to ask some inquiry for some related bidders without revealing their real identities. Suppose that a reviewer U_1 with attribute sequence $< \ldots, 0_i, 1_{i+1}, \ldots >$ wants to inquire for bidders, such as U_2 with "A: more than 2 grade enterprise qualification" and "B: more than 10 years warranty" qualifications. If U_2 satisfies $\overline{\overline{A_{Bidder}}}$ and U_1 satisfies $\overline{\overline{A_{\mathrm{Review}}}} =< \ldots, 0_i, 1_{i+1}, \ldots >$ specified by U_2, then U_1 can consult a session key with U_2 to achieve secure communication by using a TP-AB-KA protocol.

With the increasing popularity and application of mobile devices, more and more applications are migrated from PCs to mobile devices, such as smart phones. Above example also happens in mobile environment. Since most mobile devices are resource constrained, it is more important to improve the performance of TP-AB-KA protocol by reducing computation cost and communication cost. However, the existing TP-AB-KA protocols are not so good in performance because the length of ciphertext and key grows linearly with the number of related attributes.

1.1. Our Motivation and Contribution. ABE scheme has fine-grained data access control, which can be well applied to many scenes where KA protocols are used. As shown in above example, ABE scheme was adopted for attribute authentication between the participants in the protocol and did not reveal their identities. More and more KA protocols introduce ABE schemes to construct TP-AB-KA protocols. However, the length of key and ciphertext in those TP-AB-KA protocols grows linearly with the number of attributes which participants own or are embedded in access policies. Obviously, those TP-AB-KA protocols are unfit for the lightweight applications. For example, mobile devices have become the primary devices in open cloud setting, which are resource constrained and require the protocols with high performance. In order to solve above problem, we first propose a two-party attribute-based key agreement protocol with constant-size ciphertext and key based on the CP-ABE scheme [3].

Our protocol adopts an AND-gate access structure based on the whole attribute universe. A polynomial function $\overrightarrow{f}(x, \cdot)$ embedded in the exponent location of a group element is defined to express the attribute character of one participant. One factor $x + H_1(i)$ in $\overrightarrow{f}(x, \cdot)$ is one secret value, which reflects the ith attribute of the participant, where $H_1(\cdot)$ is a hash function. The polynomial function $\overrightarrow{f}(x, \cdot) = \prod_{i \notin \Omega}(x + H_1(i))$ is used to describe all attributes of the participant, where Ω is the index set of the corresponding items in attribute sequence. Similarly, one data access policy is also described with polynomial function. When x in $\overrightarrow{f}(x, \cdot)$ is substituted with the master key of the trusted authority (TA), the polynomial functions $\overrightarrow{f}(x, \cdot)$ is computed into a constant-size value, based on which both the key and the ciphertext in our protocol can be calculated into some values, respectively, which are irrelevant to the number of corresponding attributes. By using this method, we can generate the constant-size key and ciphertext.

The proposed protocol is proved secure in AB-BJM model [4] based on the difficult problem of the augmented multisequence of exponents decisional Diffie-Hellman (aMSE-DDH) hypothesis [5] in standard model. The public key parameters and specific oracle queries $\widetilde{Send}(\cdot), \widetilde{Corrupt}(\cdot), \widetilde{Reveal}(\cdot)$ are simulated successfully. The challenge task of aMSE-DDH hypothesis is embedded in the communication ciphertexts. Compared with the existed TP-AB-KA protocols, our protocol's computation and communication costs are largely reduced. The constant-size key and chipertext improve the implementation efficiency and make our protocol be more suitable for the application of lightweight level.

1.2. Organization. The related work is introduced in Section 2. The preliminaries are introduced in Section 3. In Section 4, a TP-AB-KA protocol is proposed. TP-AB-KA protocol is proved to be secure in Section 5. Subsequently, we give the performance comparison between the protocol [4] and our protocol in Section 6. We conclude our paper in Section 7.

2. Related Work

The key agreement (KA) protocol is used to establish secure communication between two or more parties and authenticate entities in an open environment. With the emerging of identity-based cryptography, Smart [6] presented the first two-party identity-based key agreement protocol (ID-KA) which adopted the IBE scheme [7]. Since then, lots of ID-KA protocols have successively been put forward [1, 8–11]. Those ID-KA protocols were proved security in various models, respectively, such as the BJM model [12], the BR4 model, the CK model, etc. Huang and Cao [13] provided the first ID-AK protocol which was provable security in eCK [14] model. Based on the BJM model [12], Chen *et al.* [9] proposed the ID-BJM model and constructed identity-based key agreement protocols. In order to implement fine-grained access control, session keys are negotiated based on mutual authentication of participants' attribute information. many attribute-based key agreement (AB-KA) protocols [15–20] are presented. In AB-KA protocols, attribute-based encryption (ABE) plays important role in protecting secret messages used to generate session keys. ABE [21] was mainly divided into two categories called ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE). In CP-ABE, data owner chooses an access structure on attributes and encrypts data with the corresponding attribute public key. Access structure is embedded in the ciphertext, while the secret key is produced according to the attribute set of data user. If the attributes held by a user satisfy access structure embedded in the ciphertext, then he/she decrypts such ciphertext [22]. KP-ABE scheme is inverse. The encryptor selects the descriptive attributes to encrypt data. Recently, Li *et al.* [23, 24] presented two CP-ABE schemes with efficient attribute revocation, which resists the user collusion attack and supports fine-grained access control. There are some privacy-preserving decentralized CP-ABE [25–27] schemes, in which the size of the ciphertext grows linearly with the number of attributes embedded in access policy. In order to improve efficiency, Emura *et al.* [28] presented a CP-ABE scheme with constant ciphertext size. Many ABE schemes [29–38] were presented in various application domains, such as ABE with outsourced data decryption [29, 30, 37], ABE with efficient attribute revocation [31], ABE with full verifiability [30], ABE with keyword search function [29, 31], traceable ABE [32, 33], ABE with leakage resilience [34–36], auditable ABE [38], etc. In order to solve key escrow problem, Li *et al.* [39, 40] presented two certificate-based encryption schemes with leakage resilience. ABE schemes have wide application in cloud storage [41, 42], mobile social networks [43] and smart grid [44]. The original AB-AK protocol [1] gave a secret handshake mechanism based on attributes. Later, lots of AB-KA protocols [15–20] were presented. Wang *et al.* [18] presented a variant of AB-KA protocol based on ABE scheme. But this protocol did not realize mutual authentication on the basis of participants' attributes. Yoneyama [20] put forward two rounds of AB-KA protocol by using a design technique of the NAXOS protocol and gave the security proof in the modified eCK model. Recently, Wei *et al.* [4] proposed an AB-KA protocol which is proved secure in the modified BJM model under the decisional bilinear Diffie-Hellman assumption in the standard model. But the length of communication messages and decryption key in [4] increased linearly with the number of attributes and was unsuitable for the resource constrained application.

3. Preliminaries

3.1. Access Structure. Suppose that $ATT = \{att_1, att_2, \ldots, att_n\}$ includes n attributes in our system. An access structure is a nonempty subset $\mathbb{A} \subseteq 2^{\{att_1, att_2, \ldots, att_n\}} \setminus \{\varnothing\}$. In particular, for a collection $\mathbb{A}$ is monotone if $\widehat{B} \in \mathbb{A}$ and $\widehat{B} \subseteq \widehat{C}$, then $\widehat{C} \in \mathbb{A} \forall \widehat{B}, \widehat{C}$. If a user with a set in $\mathbb{A}$ then he/she is authorized to access some resources.

3.2. Bilinear Maps. $\mathbb{G}, \mathbb{G}_{\mathbb{T}}$ are two multiplicative cyclic groups with prime order p. g is the generator of $\mathbb{G}$ and e is bilinear map $e : \mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}_{\mathbb{T}}$. The bilinear map e satisfies the following properties:

(1) Bilinearity: for all $\iota, \kappa \in \mathbb{Z}_p$, $e(g^{\iota}, g^{\kappa}) = e(g, g)^{\iota\kappa}$.

(2) Nondegeneracy: $e(g, g) \neq 1$.

(3) Computability: there is an efficient algorithm to compute $e(\phi, \zeta)$ for $\forall \phi, \zeta \in \mathbb{G}$.

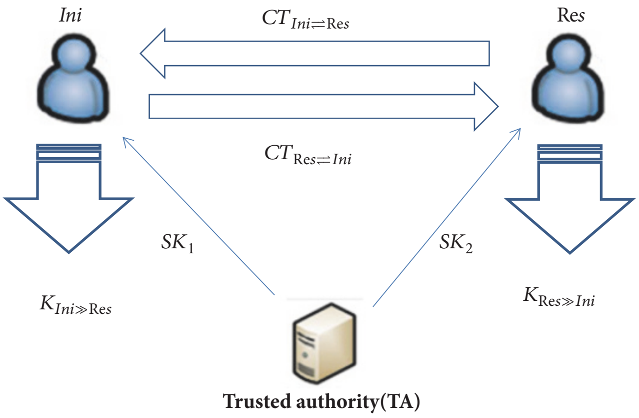

Ini
$CT_{Ini \rightleftharpoons \mathrm{Res}}$
Res
$CT_{\mathrm{Res} \rightleftharpoons Ini}$
SK_1
SK_2
$K_{Ini \gg \mathrm{Res}}$
$K_{\mathrm{Res} \gg Ini}$
Trusted authority(TA)

FIGURE 1: System model of our TP-AB-KA protocol.

3.3. aMSE-DDH Assumption [5]. The aMSE-DDH assumption is defined as follows. Let $\Gamma = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_{\mathbb{T}}, p, e\}$ be the pairing group, and let $\overrightarrow{f}(x), \overrightarrow{\vartheta}(x)$ be polynomials with coprimes. Let $\varsigma_0, \hbar_0$ be the generators of $\mathbb{G}_1, \mathbb{G}_2$, respectively. β is a random element of $\mathbb{Z}_p$ and R is selected randomly in $\mathbb{G}_{\mathbb{T}}$. Given a tuple $\overrightarrow{Y} =< \varsigma_0, \varsigma_0^{\beta}, \varsigma_0^{\beta^2}, \ldots, \varsigma_0^{\beta^{n-1}}, \varsigma_0^{\beta \overrightarrow{f}(\beta)}; \hbar_0, \hbar_0^{\beta}, \hbar_0^{\beta^2}, \ldots, \hbar_0^{\beta^n}; \hbar_0^{1/\overrightarrow{\vartheta}(\beta)}, \hbar_0^{\beta/\overrightarrow{\vartheta}(\beta)}, \hbar_0^{\beta^2/\overrightarrow{\vartheta}(\beta)}, \ldots, \hbar_0^{\beta^n/\overrightarrow{\vartheta}(\beta)}; \varsigma_0^{\xi\beta\overrightarrow{f}(\beta)}, \hbar_0^{\xi}, R >$, if no probabilistic polynomial time adversary $\mathscr{A}$ makes a distinction between $e(\varsigma_0, \hbar_0)^{\overrightarrow{f}(\beta)\xi}$ and R, then we claim that the aMSE-DDH assumption holds with the advantage $adv_{\mathscr{A}} = |\Pr[\mathscr{A}(\overrightarrow{Y}, e(\varsigma_0, \hbar_0)^{\overrightarrow{f}(\beta)\xi}) = 1] - \Pr[\mathscr{A}(\overrightarrow{Y}, R) = 1]| \leq \varepsilon$, where ε is a negligible function.

3.4. Outline of Our TP-AB-KA Protocol. We give a two-party attribute-based key agreement (TP-AB-KA) protocol. There are 3 roles, trusted authority (TA) and two participants (initiator Ini and responder Res). TA is a trusted role who monitors the participants' attributes and issue private keys for them. Two participants, Ini and Res, make key agreement as Figure 1.

$SystemSetup(\lambda) \longrightarrow MSK, MPK$. This algorithm takes as input a security parameter λ and outputs master secret key MSK and public parameters MPK.

$KeyGeneration(\overline{\overline{Ini}}) \longrightarrow SK_1$. This algorithm is implemented by trusted authority (TA). It takes as input attribute sequence $\overline{\overline{Ini}}$ of a participant Ini and outputs Ini's private key SK_1. Similarly, for another participant Res with the attribute sequence $\overline{\overline{\mathrm{Re}s}}$, TA outputs his/her private key SK_2 by calling $KeyGeneration$ algorithm.

$Encrytion(\overline{\overline{A_{\overline{\overline{\mathrm{Re}s\geq}}}}}, M_{Ini}) \longrightarrow CT_{Ini \rightleftharpoons \mathrm{Re}s}$. This algorithm takes as input the plaintext M_{Ini} and the data access policy $\overline{\overline{A_{\overline{\overline{\mathrm{Re}s\geq}}}}}$, which is proposed by Ini and the attributes of the participant Res can satisfy. This algorithm outputs the ciphertext $CT_{Ini \rightleftharpoons \mathrm{Re}s}$ according to $\overline{\overline{A_{\overline{\overline{\mathrm{Re}s\geq}}}}}$. Similarly, Re$s$ selects data access policy $\overline{\overline{A_{\overline{\overline{Ini\geq}}}}}$ of which Ini's attributes can satisfy and encrypts plaintext $M_{\mathrm{Re}s}$ into the ciphertext $CT_{\mathrm{Re}s\rightleftharpoons Ini}$ according to $\overline{\overline{A_{\overline{\overline{Ini}}\geq}}}$ by calling this algorithm.

Decrytion$(CT_{Ini\rightleftharpoons \mathrm{Re}s}, SK_1) \longrightarrow M_{Ini}$. This algorithm takes as input the ciphertext $CT_{Ini\rightleftharpoons \mathrm{Re}s}$ and Ini's private key SK_1 and outputs the message M_{Ini}. By calling this algorithm, Res decrypts $CT_{\mathrm{Re}s\rightleftharpoons Ini}$ into $M_{\mathrm{Re}s}$ by using the private key SK_2.

SessKeyGeneration$(CT_{Ini\rightleftharpoons \mathrm{Re}s}, CT_{\mathrm{Re}s\rightleftharpoons Ini}) \longrightarrow K_{Ini\gg \mathrm{Re}s}$, $K_{\mathrm{Re}s\gg Ini}$. This is an interactive procedure. Firstly, Ini sends $CT_{Ini\rightleftharpoons \mathrm{Re}s}$ to Res and Res sends $CT_{\mathrm{Re}s\rightleftharpoons Ini}$ to Ini, respectively. Secondly, Ini decrypts $CT_{\mathrm{Re}s\rightleftharpoons Ini}$ and Res decrypts $CT_{Ini\rightleftharpoons \mathrm{Re}s}$ by using *Decrytion* algorithm, respectively. Thirdly, Ini and Res compute the session key $K_{Ini\gg \mathrm{Re}s}$ and $K_{\mathrm{Re}s\gg Ini}$, respectively, where $K_{Ini\gg \mathrm{Re}s} = K_{\mathrm{Re}s\gg Ini}$.

3.5. AB-BJM Model [4]. We employ the attribute-based BJM model to prove the security of our TP-AB-KA protocol. There are many protocol participants, which are all formalized as oracles. An attacker $\widetilde{\mathscr{A}}$ can access those oracles by issuing some specified queries: $\widetilde{Send}(\cdot), \widetilde{Corrupt}(\cdot), \widetilde{Reveal}(\cdot)$. An oracle $\Pi^k_{U_1,U_2}$ represents the k-th instance of a participant U_1 involved with another participant U_2 in a session. U_1, U_2 have the corresponding attribute sequences and the private keys, respectively. Some key messages in AB-KA protocol are encrypted or decrypted based on a certain kind of ABE scheme.

The security of the protocol $\prod$ is described via a game with two phases.

(1) The First Phase. $\widetilde{\mathscr{A}}$ is allowed to launch the below queries in any order.

$\widetilde{Send}(\Pi^k_{U_1,U_2}, m)$. $\widetilde{\mathscr{A}}$ initiates a session or sends messages to the participants. On receiving the message m, oracle $\Pi^k_{U_1,U_2}$ implements the protocol and responds with an outgoing message $\widehat{m}$, or a decision to indicate accepting or rejecting the session. If $\Pi^k_{U_1,U_2}$ does not exit, it is created as an initiator if $m = \lambda$(the security parameter), or as a responder otherwise.

$\widetilde{Corrupt}(U)$. The participant U responds with its private key.

$\widetilde{Reveal}(\Pi^k_{U_1,U_2})$. If the oracle accepts, it reveals the session key; otherwise, it returns $\perp$.

(2) The Second Phase. Once $\widetilde{\mathscr{A}}$ finishes the first phase works, it begins the second phase by selecting a fresh oracle $\Pi^k_{U_1,U_2}$ and launching the $\widetilde{Test}(\Pi^k_{U_1,U_2})$ query. The fresh oracle $\Pi^k_{U_1,U_2}$ and $\widetilde{Test}(\cdot)$ query are defined as below.

Definition 1 (fresh oracle). An oracle $\Pi^k_{U_1,U_2}$ is fresh if (1) $\Pi^k_{U_1,U_2}$ has been accepted; (2) $\Pi^k_{U_1,U_2}$ is not opened (not being submitted the $\widetilde{Reveal}(\cdot)$ query); (3) U_1, U_2 is not corrupted (not being submitted the $\widetilde{Corrupt}(\cdot)$ query); (4) There is no opened oracle $\Pi^j_{U_2,U_1}$, which has matched a conversation to $\Pi^k_{U_1,U_2}$.

$\widetilde{Test}(\Pi^k_{U_1,U_2})$. If $\Pi^k_{U_1,U_2}$ is fresh, $\widetilde{\mathscr{B}}$ randomly chooses $\tau \in \{0,1\}$. It responds with the session key if $\tau = 0$, otherwise, a random sample from the distribution of the session keys.

$\widetilde{\mathscr{A}}$ continues to query the oracles except that it does not reveal the test oracle $\Pi^k_{U_1,U_2}$ or its session participant $\Pi^j_{U_2,U_1}$ (if it exists), and it does not corrupt the participant U_2.

At last the adversary outputs a guess τ' for τ. If $\tau = \tau'$, we claim that the adversary wins. The advantage of the adversary is defined as $Adv^{\widetilde{\mathscr{A}}}(k) = \max\{0, \Pr[\widetilde{\mathscr{A}}\ \ wins] - 1/2\}$.

A secure key agreement protocol $\prod$ is defined as below.

Definition 2. Protocol $\prod$ is a secure key agreement protocol if (1) the adversary faithfully conveys messages. Both $\Pi^k_{U_1,U_2}$ and $\Pi^j_{U_2,U_1}$ are always accepted and hold the same session key which is distributed uniformly on $\{0,1\}^k$; (2) $Adv^{\widetilde{\mathscr{A}}}(k)$ is negligible.

4. TP-AB-KA Protocol

A TP-AB-KA protocol with constant-size key and ciphertext is first given in this paper. We embed the ABE scheme [3] into the key agreement protocol. Two parties in our protocol make agreement of the session key based on the exchanged secret messages. Suppose that two participants U_1,U_2 encrypt their own secret messages into the ciphertexts according to the access policies proposed by each other, respectively. U_1 acts as an initiator and U_2 acts as a responder. So long as the attributes of U_1, U_2 satisfy mutual access policies, they can obtain the partner's secret messages, respectively. U_1, U_2 use the corresponding secret messages to calculate the same session key. The protocol is showed in Figure 2. Our TP-AB-KA protocol includes three stages: *SystemSetup*, *KeyGeneration* and *KeyExchange*. The concrete construction is described as below.

SystemSetup. Suppose that λ is the security parameter. Let $\mathbb{G}$ and $\mathbb{G}_{\mathbb{T}}$ be multiplicative cyclic groups with prime order p. A trusted authority (TA) selects generators g, h from $\mathbb{G}$ and keeps g secret. Suppose that there is an attribute universe $[\![U]\!] =< att_1, att_2, \ldots, att_n >$ including n attributes. For each attribute att_i, TA randomly selects $\beta, \sigma_1, \sigma_2 \in \mathbb{Z}_p$ and calculates $\widetilde{H_i} = h^{\beta^i}$, $\widetilde{Q_i} = h^{\sigma_1\beta^i}$, $\widetilde{E_i} = h^{\sigma_2\beta^i}$, $i \in \{0,1,\ldots,n\}$. TA keeps $MSK = \{g,\beta,\sigma_1,\sigma_2\}$ secret. This algorithm chooses 3 cryptographic hash functions: $H_1 : \{0,1\}^* \longrightarrow \mathbb{Z}_p$, $H_2 : \{0,1\}^* \longrightarrow \mathbb{Z}_p$, $H_3 : \mathbb{G}_{\mathbb{T}} \longrightarrow \mathbb{G}$. For the attribute sequence $\overline{\overline{U}} =< z_1, z_2, \ldots, z_n >$ of one participant U, we define a polynomial function $\overrightarrow{f}(x, \overline{\overline{U}}) = \prod_{i=1}^{n}(x + H_1(i))^{1-z_i}$ to describe U's attribute character. Here, "$z_i = 0$" denotes "having the ith attribute value" and "$z_i = 1$" denotes "not having the ith attribute value". We use $\overline{\overline{A_{\overline{\overline{U}}\geq}}} =< z'_1, z'_1, \ldots, z'_n >$ to denote the attribute sequence which the attributes of U can satisfy. Any participant can compute a polynomial function $\overrightarrow{f}(x, \overline{\overline{A_{\overline{\overline{U}}\geq}}}) = \prod_{i=1}^{n}(x + H_1(i))^{1-z'_i}$ to describe a kind of data access policy. Here, z'_i has the same

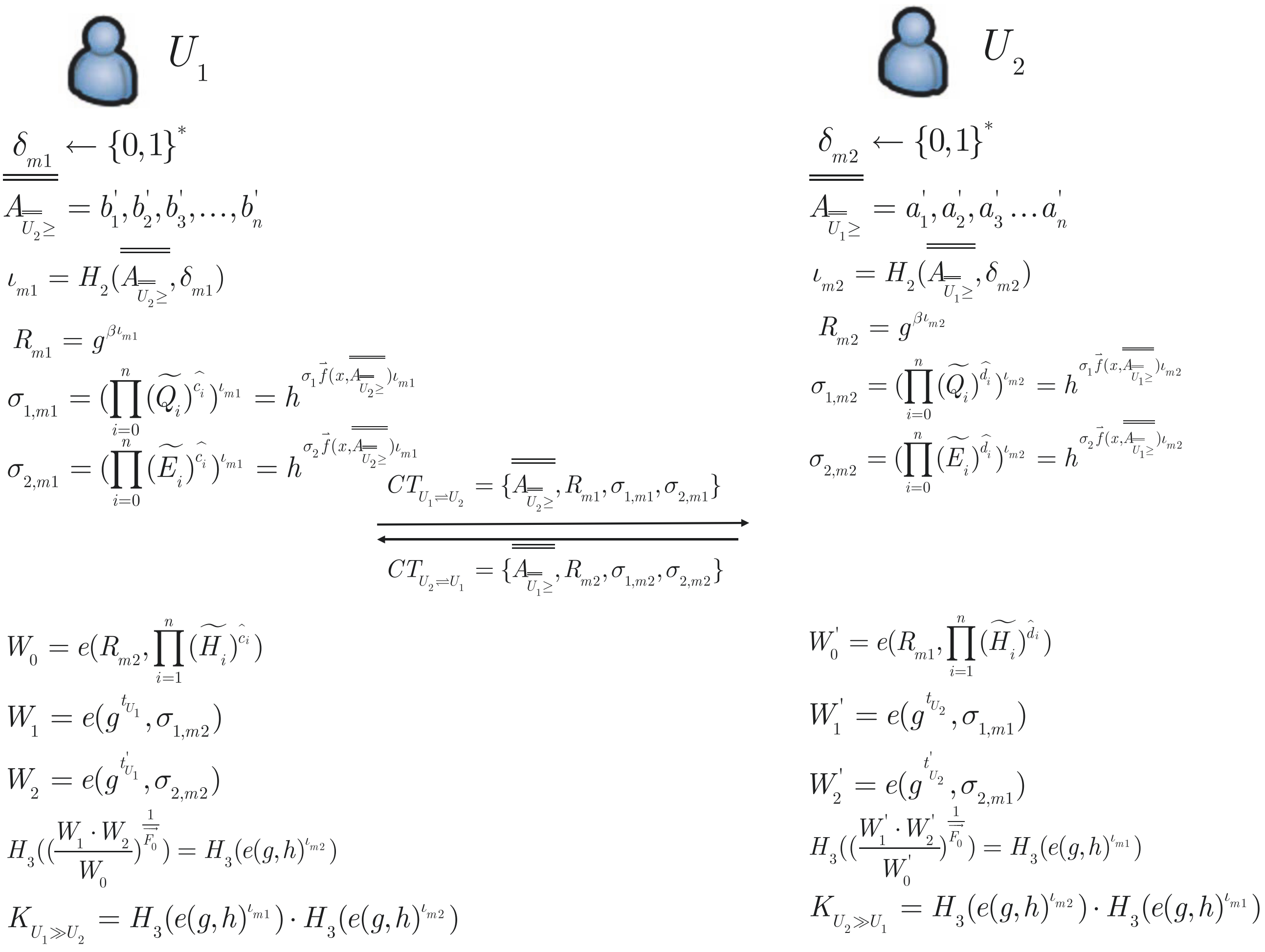

U_1
U_2
$\delta_{m1} \leftarrow \{0,1\}^*$
$\overline{\overline{A}}_{\overline{\overline{U_2}}\geq} = b'_1, b'_2, b'_3, \ldots, b'_n$
$\iota_{m1} = H_2(\overline{\overline{A}}_{\overline{\overline{U_2}}\geq}, \delta_{m1})$
$R_{m1} = g^{\beta\iota_{m1}}$
$\sigma_{1,m1} = (\prod_{i=0}^{n}(\widetilde{Q}_i)^{\widehat{c}_i})^{\iota_{m1}} = h^{\sigma_1 \overrightarrow{f}(x, \overline{\overline{A}}_{\overline{\overline{U_2}}\geq})\iota_{m1}}$
$\sigma_{2,m1} = (\prod_{i=0}^{n}(\widetilde{E}_i)^{\widehat{c}_i})^{\iota_{m1}} = h^{\sigma_2 \overrightarrow{f}(x, \overline{\overline{A}}_{\overline{\overline{U_2}}\geq})\iota_{m1}}$
$\delta_{m2} \leftarrow \{0,1\}^*$
$\overline{\overline{A}}_{\overline{\overline{U_1}}\geq} = a'_1, a'_2, a'_3 \ldots a'_n$
$\iota_{m2} = H_2(\overline{\overline{A}}_{\overline{\overline{U_1}}\geq}, \delta_{m2})$
$R_{m2} = g^{\beta\iota_{m2}}$
$\sigma_{1,m2} = (\prod_{i=0}^{n}(\widetilde{Q}_i)^{\widehat{d}_i})^{\iota_{m2}} = h^{\sigma_1 \overrightarrow{f}(x, \overline{\overline{A}}_{\overline{\overline{U_1}}\geq})\iota_{m2}}$
$\sigma_{2,m2} = (\prod_{i=0}^{n}(\widetilde{E}_i)^{\widehat{d}_i})^{\iota_{m2}} = h^{\sigma_2 \overrightarrow{f}(x, \overline{\overline{A}}_{\overline{\overline{U_1}}\geq})\iota_{m2}}$
$CT_{U_1 \rightleftharpoons U_2} = \{\overline{\overline{A}}_{\overline{\overline{U_2}}\geq}, R_{m1}, \sigma_{1,m1}, \sigma_{2,m1}\}$
$CT_{U_2 \rightleftharpoons U_1} = \{\overline{\overline{A}}_{\overline{\overline{U_1}}\geq}, R_{m2}, \sigma_{1,m2}, \sigma_{2,m2}\}$
$W_0 = e(R_{m2}, \prod_{i=1}^{n}(\widetilde{H}_i)^{\widehat{c}_i})$
$W_1 = e(g^{t_{U_1}}, \sigma_{1,m2})$
$W_2 = e(g^{t'_{U_1}}, \sigma_{2,m2})$
$H_3((\frac{W_1 \cdot W_2}{W_0})^{\frac{1}{\overline{\overline{F_0}}}}) = H_3(e(g,h)^{\iota_{m2}})$
$K_{U_1 \gg U_2} = H_3(e(g,h)^{\iota_{m1}}) \cdot H_3(e(g,h)^{\iota_{m2}})$
$W'_0 = e(R_{m1}, \prod_{i=1}^{n}(\widetilde{H}_i)^{\widehat{d}_i})$
$W'_1 = e(g^{t_{U_2}}, \sigma_{1,m1})$
$W'_2 = e(g^{t'_{U_2}}, \sigma_{2,m1})$
$H_3((\frac{W'_1 \cdot W'_2}{W'_0})^{\frac{1}{\overline{\overline{F_0}}}}) = H_3(e(g,h)^{\iota_{m1}})$
$K_{U_2 \gg U_1} = H_3(e(g,h)^{\iota_{m2}}) \cdot H_3(e(g,h)^{\iota_{m1}})$

FIGURE 2: TP-AB-KA protocol.

definition as z_i. The algorithm finally outputs the public parameters $MPK = \{e(g,h), g^{\beta}, \widetilde{H_i}, \widetilde{Q_i}, \widetilde{E_i}, H_1, H_2, H_3\}$.

KeyGeneration. For a participant U_1 with attribute sequence $\overline{\overline{U_1}} =< a_1, a_2, a_3, \ldots, a_n >$, TA calculates $\overrightarrow{f}(\beta, \overline{\overline{U_1}}) = \prod_{i=1}^{n}(\beta + H_1(i))^{1-a_i}$, which is a polynomial formula with n-degree at most. TA randomly selects $t_{U_1} \in \mathbb{Z}_p$ and computes $t'_{U_1} = (1/\sigma_1)(1/\overrightarrow{f}(\beta, \overline{\overline{U_1}}) - \sigma_2 t_{U_1})$. TA computes U_1's private key $SK_1 = \{g^{t_{U_1}}, g^{t'_{U_1}}\}$.

For another participant U_2 with $\overline{\overline{U_2}} =< b_1, b_2, b_3, \ldots, b_n >$, TA randomly selects $t_{U_2} \in \mathbb{Z}_p$ and computes $t'_{U_2} = (1/\sigma_1)(1/\overrightarrow{f}(\beta, \overline{\overline{U_2}}) - \sigma_2 t_{U_2})$ by using the similar approach. TA computes U_2's private key $SK_2 = \{g^{t_{U_2}}, g^{t'_{U_2}}\}$.

Encrytion. U_1 chooses a data access policy $\overline{\overline{A}}_{\overline{\overline{U_2}}\geq} =< b'_1, b'_2, b'_3, \ldots, b'_n >$ which U_2's attributes can satisfy. U_1 generates the corresponding $\overrightarrow{f}(x, \overline{\overline{A}}_{\overline{\overline{U_2}}\geq}) = \prod_{i=1}^{n}(x + H_1(i))^{1-b'_i}$. Let $\widehat{c_i}$ be the coefficient of x^i in $\overrightarrow{f}(x, \overline{\overline{A}}_{\overline{\overline{U_2}}\geq})$. U_1 randomly selects $\delta_{m1} \in \{0,1\}^*$ and computes $\iota_{m1} = H_2(\overline{\overline{A}}_{\overline{\overline{U_2}}\geq}, \delta_{m1})$, $e(g,h)^{\iota_{m1}}$, $R_{m1} = g^{\beta\iota_{m1}}$, $\sigma_{1,m1} = (\prod_{i=0}^{n}(\widetilde{Q_i})^{\widehat{c_i}})^{\iota_{m1}} = h^{\sigma_1 \overrightarrow{f}(x, \overline{\overline{A}}_{\overline{\overline{U_2}}\geq})\iota_{m1}}$, $\sigma_{2,m1} = (\prod_{i=0}^{n}(\widetilde{E_i})^{\widehat{c_i}})^{\iota_{m1}} = h^{\sigma_2 \overrightarrow{f}(x, \overline{\overline{A}}_{\overline{\overline{U_2}}\geq})\iota_{m1}}$. U_1 generates $CT_{U_1 \rightleftharpoons U_2} = \{\overline{\overline{A}}_{\overline{\overline{U_2}}\geq}, R_{m1}, \sigma_{1,m1}, \sigma_{2,m1}\}$. Similarly, U_2 completes the following work successively by using the same way. U_2 chooses a data access policy $\overline{\overline{A}}_{\overline{\overline{U_1}}\geq} =< a'_1, a'_2, a'_3, \ldots, a'_n >$ which U_2's attributes can satisfy. U_2 generates the corresponding $\overrightarrow{f}(x, \overline{\overline{A}}_{\overline{\overline{U_1}}\geq}) = \prod_{i=1}^{n}(x + H_1(i))^{1-a'_i}$. Let $\widehat{d_i}$ be the coefficient of x^i in $\overrightarrow{f}(x, \overline{\overline{A}}_{\overline{\overline{U_1}}\geq})$. Then U_2 randomly selects $\delta_{m2} \in \{0,1\}^l$ and computes $\iota_{m2} = H_2(\overline{\overline{A}}_{\overline{\overline{U_1}}\geq}, \delta_{m2})$, $e(g,h)^{\iota_{m2}}$, $R_{m2} = g^{\beta\iota_{m2}}$, $\sigma_{1,m2} = (\prod_{i=0}^{n}(\widetilde{Q_i})^{\widehat{d_i}})^{\iota_{m2}} = h^{\sigma_1 \overrightarrow{f}(x, \overline{\overline{A}}_{\overline{\overline{U_1}}\geq})\iota_{m2}}$ and $\sigma_{2,m2} = (\prod_{i=0}^{n}(\widetilde{E_i})^{\widehat{d_i}})^{\iota_{m2}} = h^{\sigma_2 \overrightarrow{f}(x, \overline{\overline{A}}_{\overline{\overline{U_1}}\geq})\iota_{m2}}$. U_2 generates $CT_{U_2 \rightleftharpoons U_1} = \{\overline{\overline{A}}_{\overline{\overline{U_1}}\geq}, R_{m2}, \sigma_{1,m2}, \sigma_{2,m2}\}$.

Decrytion. Assume that U_1 has the attribute sequence $\overline{\overline{U_1}}$ and the corresponding private key SK_1, U_2 with $\overline{\overline{U_2}}$ has SK_2. U_1 generates the share secret by using the following calculation steps after receiving $CT_{U_2 \rightleftharpoons U_1}$. For $\overline{\overline{U_1}} =<$

$a_1, a_2, a_3, \ldots, a_n >$ and $\overline{\overline{A_{\overline{\overline{U_1}}\geq}}} =< a_1', a_2', a_3', \ldots, a_n' >$, U_1 computes $\Delta_i = a_i' - a_i$, $i \in \{0, 1, \cdots, n\}$ and $\overrightarrow{F}(x) = \overrightarrow{F_{AU}}(x, \overline{\overline{A_{\overline{\overline{U_1}}\geq}}}, \overline{\overline{U_1}}) = \prod_{i=1}^{n}(x + H_1(i))^{\Delta_i}$. $\overline{\overline{U_1}}$ satisfies $\overline{\overline{A_{\overline{\overline{U_1}}\geq}}}$, $\overrightarrow{F}(x)$ is the $(n - |\overline{\overline{U_1}}|)$-degree at most polynomial function, where $\overrightarrow{F}_i$ the coefficient of x^i and $\overrightarrow{F}_0 \neq 0$. U_1 computes $\widetilde{W_0} = e(R_{m2}, \prod_{i=1}^{n}\widetilde{H_i}^{\widehat{c_i}}) = e(g^{\beta\iota_{m2}}, \prod_{i=1}^{n}h^{\beta^{i-1}\widehat{c_i}}) = e(g,h)^{\beta\iota_{m2}\sum_{i=1}^{n|}\beta^{i-1}\widehat{c_i}} = e(g,h)^{\iota_{m2}(\overrightarrow{F}(\beta)-\widehat{c_0})} = e(g, h)^{\iota_{m2}(\overrightarrow{F}(\beta)-\overrightarrow{F}(0))}$, $\widetilde{W_1} = e(g^{t_{U_1}'}, \sigma_{1,m2}) = e(g,h)^{\sigma_1\overrightarrow{f}(\beta,\overline{\overline{A_{\overline{\overline{U_1}}\geq}}})\iota_{m2}t_{U_1}'}$, $\widetilde{W_2} = e(g^{t_{U_1}}, \sigma_{2,m2}) = e(g,h)^{\sigma_2\overrightarrow{f}(\beta,\overline{\overline{A_{\overline{\overline{U_1}}\geq}}})\iota_{m2}t_{U_1}}$, $\widetilde{W}_1 \cdot \widetilde{W}_2 = e(g,h)^{\overrightarrow{f}(\beta,\overline{\overline{A_{\overline{\overline{U_1}}\geq}}})\iota_{m2}(\sigma_1 t_{U_1}' + \sigma_2 t_{U_1})} = e(g,h)^{\iota_{m2}\overrightarrow{F}(\beta)}$, $((\widetilde{W}_1 \cdot \widetilde{W}_2)/\widetilde{W_0})^{1/\widehat{c_0}} = e(g,h)^{\iota_{m2}}$. At last, U_1 obtains secret $H_3(e(g,h)^{\iota_{m2}})$. By using the similar approach, U_2 computes $\Delta_i' = b_i' - b_i$ and $\overrightarrow{F'}(x) = \overrightarrow{F_{AU}}(x, \overline{\overline{A_{\overline{\overline{U_2}}\geq}}}, \overline{\overline{U_2}}) = \prod_{i=1}^{n}(x + H_1(i))^{\Delta_i'}$. $\overrightarrow{F'}(x)$ is the $(n - |\overline{\overline{U_2}}|)$-degree at most polynomial function, where $\overrightarrow{F_i'}$ is denoted by the coefficient of x^i and $\overrightarrow{F_0'} \neq 0$. U_2 obtains $H_3(e(g,h)^{\iota_{m1}})$ from the received ciphertext $CT_{U_1 \rightleftharpoons U_2}$.

SessKeyGeneration. Firstly, U_1 sends $CT_{U_1 \rightleftharpoons U_2}$ to U_2 and U_2 sends $CT_{U_2 \rightleftharpoons U_1}$ to U_1, respectively. Secondly, U_1, U_2 decrypt $CT_{U_2 \rightleftharpoons U_1}$, $CT_{U_1 \rightleftharpoons U_2}$ by calling *Decrytion* algorithms, respectively. Thirdly, U_1 and U_2 compute the session key $K_{U_1 \gg U_2} = H_3(e(g,h)^{\iota_{m1}}) \cdot H_3(e(g,h)^{\iota_{m2}})$ and $K_{U_2 \gg U_1} = H_3(e(g,h)^{\iota_{m2}}) \cdot H_3(e(g,h)^{\iota_{m1}})$, respectively.

5. Security Analysis

Theorem 3. *Provided that the augmented multisequence of exponents decisional Diffie-Hellman (aMSE-DDH) [5] assumption holds, our protocol TP-AB-KA protocol is secure in the AB-BJM model. In detail, if there is an adversary* $\widetilde{\mathscr{A}}$ *who attacks our protocol successfully at the advantage* ε *under the condition involving* N_U *participants and* Q_S *sessions, a simulator* $\widetilde{\mathscr{B}}$ *can be constructed to solve the aMSE-DDH problem at the advantage* $\varepsilon/(N_U^2 \cdot Q_S)$.

Proof. Suppose an adversary $\widetilde{\mathscr{A}}$ involves N_U participants in the protocol and establishes Q_S sessions. $\widetilde{\mathscr{B}}$ chooses $k^* \in (0, Q_S)$ and two participants U_1, U_2 arbitrarily. $\widetilde{\mathscr{B}}$ guesses that $\widetilde{\mathscr{A}}$ launches the $\widetilde{Test}(\cdot)$ query to the participant $\Pi_{U_1,U_2}^{k^*}$. $\widetilde{\mathscr{A}}$ provides the access policies $\widetilde{\overline{\overline{A_{U_1,U_2}^{*}}}} = \{\overline{\overline{A^{*}_{\overline{\overline{U_2}}\geq}}}, \overline{\overline{A^{*}_{\overline{\overline{U_1}}\geq}}}\}$. Let $\overline{\overline{A^{*}_{\overline{\overline{U_2}}\geq}}} = \overline{\overline{A_{\overline{\overline{U_2}}\geq}}} =< b_1', b_2', b_3' \ldots b_n' >$ where $b_i' = 0$ denotes "having the ith attribute value" and $b_i' = 1$ denotes "not having the ith attribute value". $\widetilde{\mathscr{B}}$ sets $\widehat{\vartheta}(x) = \overrightarrow{f}(x, \overline{\overline{A^{*}_{\overline{\overline{U_2}}\geq}}}) = \prod_{i=1}^{n}(x + H_1(i))^{1-b_i'}$, $\widehat{f}(x) = \prod_{i=1}^{n}(x + H_1(i))^{b_i'}$. Here, $\widehat{f}(x)$ is $|\overline{\overline{A_{\overline{\overline{U_2}}\geq}}}|$-degree polynomial and $\widehat{\vartheta}(x)$ is $(n - |\overline{\overline{A_{\overline{\overline{U_2}}\geq}}}|)$-degree polynomial. Let $\widehat{c_i}$ be the coefficient of x^i in $\widehat{f}(x)$. $|\overline{\overline{A_{U_2}}}|$ denotes the number of nonzero items in $\overline{\overline{A_{U_2}}}$. R is randomly selected in $\mathbb{G}_{\mathbb{T}}$. Let $\overrightarrow{Y} =< \varsigma_0, \varsigma_0^{\beta}, \varsigma_0^{\beta^2}, \ldots, \varsigma_0^{\beta^{n-1}}, \varsigma_0^{\beta\widehat{f(\beta)}}; \hbar_0, \hbar_0^{\beta}, \hbar_0^{\beta^2}, \ldots, \hbar_0^{\beta^n}; \hbar_0^{1/\widehat{\vartheta(\beta)}}, \hbar_0^{\beta/\widehat{\vartheta(\beta)}}, \hbar_0^{\beta^2/\widehat{\vartheta(\beta)}}, \ldots, \hbar_0^{\beta^n/\widehat{\vartheta(\beta)}}; \varsigma_0^{\xi\beta\widehat{f(\beta)}}, \hbar_0^{\xi}, R >$. $\widetilde{\mathscr{B}}$ receives the challenge $(e, p, \mathbb{G}, \mathbb{G}_{\mathbb{T}}, \overrightarrow{Y}, e(\varsigma_0, \hbar_0)^{\widehat{f(\beta)}\xi}, R, \widehat{f}(x), \widehat{\vartheta}(x), \widetilde{\overline{\overline{A_{U_1,U_2}^{*}}}})$ and the task of $\widetilde{\mathscr{B}}$ is to differentiate $e(\varsigma_0, \hbar_0)^{\widehat{f(\beta)}\xi}$ from R.

SystemSetup. $\widetilde{\mathscr{B}}$ implicitly sets β as the master key which is used in the aMSE-DDH challenge instance. $\widetilde{\mathscr{B}}$ simulates the public parameters as below. $\widetilde{\mathscr{B}}$ randomly chooses $\varpi_1, \varpi_2 \in \mathbb{Z}_p$ and implicitly sets $\sigma_1 = \varpi_1/\widehat{\vartheta}(\beta), \sigma_2 = \varpi_2/\widehat{\vartheta}(\beta)$. Then $\widetilde{\mathscr{B}}$ sets $h = \hbar_0$, $h_i = \hbar_0^{\beta^i}$, $g^{\beta} = \varsigma_0^{\beta\widehat{f(\beta)}}$, $\widetilde{Q_i} = (\hbar_0^{\beta^i/\widehat{\vartheta(\beta)}})^{\varpi_1}$, $\widetilde{E_i} = (\hbar_0^{\beta^i/\widehat{\vartheta(\beta)}})^{\varpi_2}$, $e(g,h) = e(\varsigma_0, \hbar_0)^{\widehat{f(\beta)}}$. $h, \widetilde{Q_i}, \widetilde{E_i}$ is computed from the challenge instance $\overrightarrow{Y}$. $e(g,h)$ is calculated from $\varsigma_0, \varsigma_0^{\beta}, \varsigma_0^{\beta^2}, \ldots, \varsigma_0^{\beta^{n-1}}, \varsigma_0^{\beta\widehat{f(\beta)}}$ and $\hbar_0, \hbar_0^{\beta}, \widehat{f}(x)$. That is, $e(\prod_{i=0}^{n-1}(\varsigma_0^{\beta^i})^{\widehat{c_{i+1}}}, \hbar_0^{\beta}) \cdot e(\varsigma_0^{\widehat{c_0}}, \hbar_0) = e(\varsigma_0^{\sum_{i=-1}^{n-1}\widehat{c_{i+1}}\beta^{i+1}}, \hbar_0) = e(\varsigma_0, \hbar_0)^{\widehat{f(\beta)}} = e(g,h)$. $\widetilde{\mathscr{A}}$ obtains public parameter set $PK = \{\mathbb{G}, e(g,h), g^{\beta}, \widetilde{Q_i}, \widetilde{E_i}, \widetilde{H_i}\}$ from $\widetilde{\mathscr{B}}$.

$\widetilde{Corrupt}(U)$. Assume there is a participant U with $\overline{\overline{U}} =< z_1, z_2, \ldots, z_n >$, where $\overline{\overline{U}}$ does not satisfy $\overline{\overline{A^{*}_{\overline{\overline{U_1}}\geq}}}$ and $\overline{\overline{A^{*}_{\overline{\overline{U_2}}\geq}}}$, z_i is the same definition as b_i. $\widetilde{\mathscr{B}}$ sets $\overrightarrow{f}(\beta, \overline{\overline{U}}) = \prod_{i=1}^{n}(\beta + H_1(i))^{1-\chi_i}$. $\widetilde{\mathscr{B}}$ randomly chooses $\nu \in \mathbb{Z}_p$ and implicitly sets $r_U = \sigma_1\nu\beta/\sigma_2$ and $s_U = 1/\sigma_1 \cdot (1/\overrightarrow{f}(\beta, \overline{\overline{U}}) - \sigma_2 r_U)$. $\widetilde{\mathscr{B}}$ computes $g^{r_U} = (g_0^{\beta\widehat{f(\beta)}})^{\varpi_1\nu/\varpi_2}$. Without loss of generality, for $\overline{\overline{A^{*}_{\overline{\overline{U_2}}\geq}}}$, $\widetilde{\mathscr{B}}$ generates $\overleftrightarrow{f(x)} = 1/\varpi_1 \cdot (\widehat{\vartheta}(x) \cdot \widehat{f}(x))/\overrightarrow{f}(x, \overline{\overline{U}})$, where $\widehat{\vartheta}(x) = \overrightarrow{f}(x, \overline{\overline{A^{*}_{\overline{\overline{U_2}}\geq}}}) = \prod_{i=1}^{n}(x + H_1(i))^{1-b_i'}$, $\widehat{f}(x) = \prod_{i=1}^{n}(x + H_1(i))^{b_i'}$. $\overleftrightarrow{f(x)}$ is a polynomial with at most $n-1$ degree since $\overline{\overline{U}}$ does not satisfy $\overline{\overline{A^{*}_{\overline{\overline{U_2}}\geq}}}$. So, $\widetilde{\mathscr{B}}$ computes $\varsigma_0^{\overleftrightarrow{f(\beta)}}$ from $\varsigma_0, \varsigma_0^{\beta}, \varsigma_0^{\beta^2}, \ldots, \varsigma_0^{\beta^{n-1}}$, $\overleftrightarrow{f(x)}$ and sets $g^{s_U} = \varsigma_0^{\overleftrightarrow{f(\beta)}}(g_0^{\beta\widehat{f(\beta)}})^{-\nu}$. At last, $\widetilde{\mathscr{A}}$ obtains $K_U = \{s_U, r_U\}$ from $\widetilde{\mathscr{B}}$.

$\widetilde{Send}(\Pi_{U_1,U_2}^{k}, m)$. This enquiry denotes that after receiving a message m, oracle Π_{U_1,U_2}^{k} executes the protocol and responds with an outgoing message $\widehat{m}$. If Π_{U_1,U_2}^{k} is the initiator of this session, we stipulate that the received message m is the security parameter λ. $\widetilde{\mathscr{B}}$ establishes a initialized list $L_k = (\bot_1, \bot_2, \bot_3, \bot_4, \bot_5, \bot_6)$ as empty list, where $\bot_1, \bot_2, \ldots, \bot_6$ mean empty values. In our protocol, $\widetilde{\mathscr{B}}$ maintains a list that saves the following information $L_k = (\Pi_{U_1,U_2}^{k}, \widehat{x}, m, \widehat{m}, Key_{U_1U_2}, K_{U_1 \gg U_2})$. Here, $\widehat{x}$ is a random value selected by Π_{U_1,U_2}^{k}. $\widehat{m}$ is generated by Π_{U_1,U_2}^{k} in response when Π_{U_1,U_2}^{k} receives the message m. $Key_{U_1U_2}$ is the secret share from U_1 and $K_{U_1 \gg U_2}$ is the session key. When $\widetilde{\mathscr{B}}$ receives the message m, the following works are done in turn.

(1) If m is the security parameter λ, $\Pi^{k}_{U_1,U_2}$ is the initiator of this session. There are 2 cases listed as follows:

(a) If $k = k^{*}$, then $\widetilde{\mathscr{B}}$ does the following works. According to the challenging access structure $\overline{\overline{A_{\overline{\overline{U_2\geq}}}}} =< b'_1, b'_2, b'_3, \ldots, b'_n >$, $\widetilde{\mathscr{B}}$ implicitly sets $\iota_{m1} = \xi$ and $R_{m1} = \varsigma_0^{\beta \widehat{f(\beta)\xi}}$, $\sigma_{1,m1} = h_0^{\varpi_1 \xi}$, $\sigma_{2,m1} = h_0^{\varpi_2 \xi}$, and $\widehat{m} = \{\overline{\overline{A_{\overline{\overline{U_2\geq}}}}}, R_{m1}, \sigma_{1,m1}, \sigma_{2,m1}\}$. $\widetilde{\mathscr{B}}$ creates the record $(\widehat{\Pi^{k}_{U_1,U_2}}, \perp_2, \perp_3, \widehat{m}, \perp_5, \perp_6)$ in list L_k. Here, $\widetilde{\mathscr{B}}$ denotes ξ with $\perp_2$ in L_k since $\widetilde{\mathscr{B}}$ does not know ξ.

(b) If $k \neq k^{*}$, then $\widetilde{\mathscr{B}}$ carries out according to the specification of the protocol and updates the list L_k.

(2) If m is not the security parameter λ, there are 3 cases listed as follows.

(a) If there is no record $(\Pi^{k}_{U_1,U_2}, \xi', m, \widehat{m}, Key_{U_1U_2}, K_{U_1 \gg U_2})$ in list L_k, where ξ' is an arbitrary value belonged to $\mathbb{Z}_p$, $\Pi^{k}_{U_1,U_2}$ is the responder of the protocol. $\widetilde{\mathscr{B}}$ selects one random value $\iota_{m2} \in \mathbb{Z}_p$, and computes $\xi' = H_2(\overline{\overline{A_{\overline{\overline{U_1\geq}}}}}, \delta_{m2}), \widehat{m}$, $Key_{U_1U_2}, K_{U_1 \gg U_2}$ according to the protocol and updates the list L_k.

(b) If there is the record $(\Pi^{k}_{U_1,U_2}, \perp_2, \perp_3, \widehat{m}, \perp_4, \perp_5)$ in list L_k, $\Pi^{k}_{U_1,U_2}$ is just the object for test query and $k = k^{*}$. For the received m, $\widetilde{\mathscr{B}}$ computes $Key_{U_1U_2} = e(g,h)^{\iota_{m2}}$ and the session key $K_{U_1 \gg U_2} = H_3(e(\varsigma_0, \hbar_0)^{\widehat{f(\beta)\xi}}) \cdot H_3(e(g,h)^{\iota_{m2}})$ according to the protocol. Then $\widetilde{\mathscr{B}}$ updates the list L_k.

(c) If there is the record $(\Pi^{k}_{U_1,U_2}, \xi', \perp_3, \widehat{m}, \perp_4, \perp_5)$ in list L_k, where ξ' is an arbitrary value belonged to $\mathbb{Z}_p$, $\Pi^{k}_{U_1,U_2}$ is the sponsor. $\widetilde{\mathscr{B}}$ carries out according to the specification of the protocol and updates the list L_k.

$\widetilde{Test}(\Pi^{k}_{U_1,U_2})$. $\widetilde{\mathscr{A}}$ selects a fresh protocol participant $\Pi^{k}_{U_1,U_2}$ for test query.

If $\Pi^{k}_{U_1,U_2}$ is not the protocol participant guessed by $\widetilde{\mathscr{B}}$ during the initialization phase, then $\widetilde{\mathscr{B}}$ terminates the simulation. Otherwise, $\widetilde{\mathscr{B}}$ returns the session key $K_{U_1 \gg U_2} = H_3(e(\varsigma_0, \hbar_0)^{\xi \widehat{f(\beta)}}) \cdot H_3(e(g,h)^{\iota_{m2}})$.

$\widetilde{Reveal}(\Pi^{k}_{U_1,U_2})$. If $\Pi^{k}_{U_1,U_2}$ or the matched protocol participants having sessions with participant $\Pi^{k}_{U_1,U_2}$ do not be issued the $\widetilde{Test}(\cdot)$ query to, $\widetilde{\mathscr{B}}$ terminates simulation. Otherwise, $\widetilde{\mathscr{B}}$ returns the corresponding session key value through accessing the query list L_k.

Output. when $\widetilde{\mathscr{A}}$ completes all inquiries in Phase 1, $\widetilde{\mathscr{A}}$ continues to ask the 3 inquiries: $\widetilde{Corrupt}(\cdot)$, $\widetilde{Reveal}(\cdot)$, $\widetilde{Send}(\cdot)$, which are not allowed to break the freshness of participants receiving the test inquiry. Once $\widetilde{\mathscr{A}}$ decides to complete the inquiry, $\widetilde{\mathscr{A}}$ outputs a bit κ' as the stochastic value of the session key which is a conjecture and is used by $\widetilde{\mathscr{B}}$ to distinguish $e(\varsigma_0, \hbar_0)^{\xi \widehat{f(\beta)}}$ from R.

Analysis. In the whole simulation process, the simulator $\widetilde{\mathscr{B}}$ does not terminate the simulation with the probability of at least $1/(N_U^2 \cdot Q_S)$. When the simulation of $\widetilde{\mathscr{B}}$ is not terminated, $\widetilde{\mathscr{A}}$ does not distinguish the security game simulated by $\widetilde{\mathscr{B}}$ from the real security game. Therefore, if the advantage of guessing for $\widetilde{\mathscr{A}}$ is ε, then that of guessing for $\widetilde{\mathscr{B}}$ in the simulated security game is $\varepsilon/(N_U^2 \cdot Q_S)$.

If $R = e(\varsigma_0, \hbar_0)^{\xi \widehat{f(\beta)}}$, the security game simulated by $\widetilde{\mathscr{B}}$ is perfect. We get $|\Pr[\widetilde{\mathscr{B}}(\overrightarrow{Y}, e(\varsigma_0, \hbar_0)^{\widehat{f(\beta)\xi}}) = 0] - \Pr[\widetilde{\mathscr{B}}(\overrightarrow{Y}, R) = 0]| = \varepsilon/(N_U^2 \cdot Q_S)$.

According to the above analysis, we construct a simulator $\widetilde{\mathscr{B}}$ solving aMSE-DDH problem with a nonnegligible advantage $\varepsilon/(N_U^2 \cdot Q_S)$, if an attacker $\widetilde{\mathscr{A}}$ wins the security game with advantage ε. Since it is inconsistent with the hypothesis of aMSE-DDH, our protocol satisfies the conditions shown in Definition 2 (2).

Besides, we suppose there exists a benign adversary $\widetilde{\mathscr{A}}$ who faithfully conveys messages. If U_1, U_2 execute the protocol in accordance with the protocol, they correctly receive messages from each other. Therefore, the two participants in the protocol finally calculate the same session key distributed over the key space uniformly. So it satisfies the conditions shown in Definition 2 (1). □

6. Efficiency Analysis

6.1. Theoretical Analysis. We give a performance comparison between attribute-based key agreement protocols in [4] and our protocol. Some symbols are defined as follow: n_A is denoted by the number of the attributes, which are involved in the system. $T\widehat{E}_{\mathbb{G}_{\mathbb{T}}}$, $T\widehat{E}_{\mathbb{G}}$ are exponentiation operation time on an element in group $\mathbb{G}_{\mathbb{T}}$ and that in group $\mathbb{G}$, respectively. $\widehat{TP}$ is the pairing operation time. $\widehat{l_{\overline{\overline{A}}}}$ is the number of the related attributes in the data access policy. $\widehat{l_U}$ is the number of the related attributes in the private key. The comparison of computation cost is given in Table 1.

Our protocol has better performance in the *KeyGeneration* algorithm than that of [34]. The comparison of communication cost is given in Table 2.

In the protocols, we denote $|\widetilde{\overline{\overline{A^{*}_{U_1,U_2}}}}|$ as the length of all data access structures, which are supposed to be 16 bits for every protocol. If $\widehat{l_{\overline{\overline{A}}}} \geq 3$, our protocol has better performance in communication cost than that of [4].

6.2. Experimental Simulation. We conduct a simulation experiments on Windows 7 system with Intel(R) Core(TM) i7 CPU at 2.3GHZ and 4 GB RAM. The protocol is implemented by using the pairing-based cryptography library(PBC) library [45]. We use a symmetric elliptic curve a-curve, where the base field size is 512-bit. The a-curve has a 160-bit group order, i.e., p is a 160-bit length prime.

To compare above protocol in actual operation, we run each protocol ten times, respectively, and compute the average values. We code all the algorithms by using c language under the default condition that each protocol contains

Table 1: The comparison of computation cost.

Protocol	*KeyGeneration*	*SessKeyGeneration* (Encryption)	*SessKeyGeneration* (Decryption)
Protocol [4]	$(2 + 2\,\widehat{l_U})\,\widehat{TE}_{\mathbb{G}}$	$\widehat{TE}_{\mathbb{G}_{\mathbb{T}}} + (1 + 2\,\widehat{l_{\overline{\overline{A}}}})\,\widehat{TE}_{\mathbb{G}}$	$\widehat{TE}_{\mathbb{G}_{\mathbb{T}}} + (2\,\widehat{l_U} + 1)\,\widehat{TP}$
Our protocol	$2\,\widehat{TE}_{\mathbb{G}}$	$\widehat{TE}_{\mathbb{G}_{\mathbb{T}}} + (1 + 2\,\widehat{l_{\overline{\overline{A}}}})\,\widehat{TE}_{\mathbb{G}}$	$(n_A - \widehat{l_U})\,\widehat{TE}_{\mathbb{G}} + 3\,\widehat{TP} + \widehat{TE}_{\mathbb{G}_{\mathbb{T}}}$

Table 2: The comparison of communication cost.

Protocol	Communication cost
Protocol [4]	$2(\widehat{l_{\overline{\overline{A}}}} + 1)\lvert\mathbb{G}\rvert + \lvert\widetilde{\overline{\overline{A^*_{U_1,U_2}}}}\rvert$
Our protocol	$6\lvert\mathbb{G}\rvert + \lvert\widetilde{\overline{\overline{A^*_{U_1,U_2}}}}\rvert$

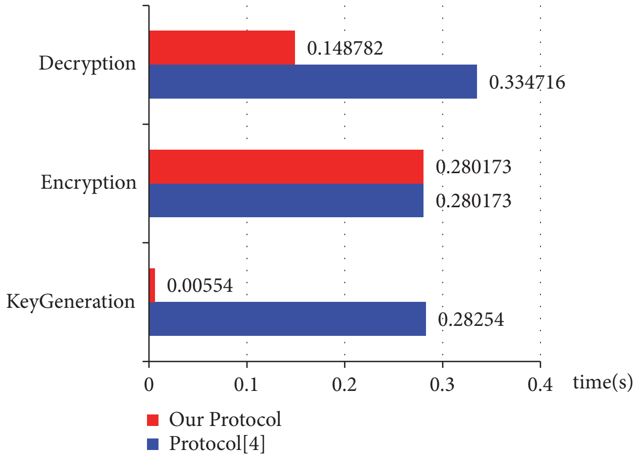


Figure 3: Running time of each algorithm in both protocols.

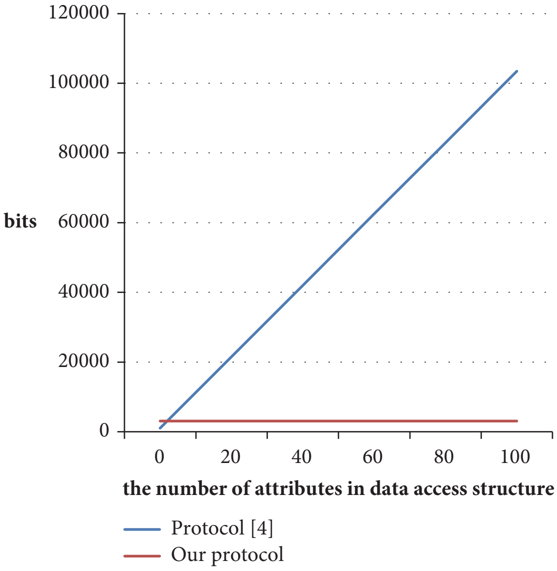


Figure 4: Communication costs of both protocols.

100 attributes in total, 50 attributes in access policy, 50 attributes in participants' attribute set. The running results are shown in Figure 3, from which we find out that the computation performance of our protocol being better than that of protocol in [4] overall. From Figure 4, our protocol has obvious advantage in the performance of communication if the number of attributes in data access structure is bigger than 3 (demarcation point). Our protocol is more practical in the resource constrained smart media and mobile environments. The theoretical analysis and simulation results are consistent, and our protocol achieves a high performance with good properties.

7. Conclusion

Compared with protocol [4], our protocol has advantages in security and efficiency. The constant-size key and ciphertext make our protocol be more suitable for the application of lightweight level. We design the key agreement protocol between two principals based on attribute-based encryption. We prove its security under the AB-BJM model in the standard model. Our protocol has better computation and communication performance than that of existed protocols.

A future research is trying to weaken the security assumption that the attacker is passive in AB-BJM model. Namely, one attacker does not have to execute the protocol faithfully to provide the messages for satisfying the requirement of the honest participator in a running of protocol. Such scene is closer to the true environment. In addition, it is an interesting topic to research the relation between the ABE and broadcast encryption [46, 47].

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (U1736112, 61772009, and 61672207), Jiangsu Provincial Natural Science Foundation of China (BK20161511), the Fundamental Research Funds for the Central Universities (2016B10114), Jiangsu Key Laboratory of Big Data Security & Intelligent Processing, NJUPT, the Key Research and Development Project of Science Department in

Jiangxi Province (20171BBE50065), and Anhui University of Natural Science Research Project (KJ2018A0398).

References

[1] G. Ateniese, J. Kirsch, and M. Blanton, "Secret handshakes with dynamic and fuzzy matching," in *Proceedings of the NDSS 2007*, W. Arbaugh, Ed., pp. 159–177, San Diego, Calif, USA, 2007.

[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings of the 24th International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT '05)*, pp. 457–473, Aarhus, Denmark, 2005.

[3] V. Odelu, A. K. Das, Y. S. Rao, S. Kumari, M. K. Khan, and K.-K. R. Choo, "Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment," *Computer Standards & Interfaces*, vol. 54, pp. 3–9, 2017.

[4] J. Wei, W. Liu, and X. Hu, "Provable secure attribute based authenticated key exchange protocols in the standard model," *Journal of Software*, vol. 25, no. 10, pp. 2397–2408, 2014.

[5] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE with constant-size keys for lightweight devices," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 763–771, 2014.

[6] N. Smart, "An ID-based authenticated key agreement protocol based on the Weil pairing," *Electronics Letters*, vol. 38, no. 13, pp. 630–632, 2002.

[7] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *Advances in Cryptology*, vol. 32, no. 3, pp. 213–229, 2001.

[8] C. Boyd, Y. Cliff, J. G. Nieto, and K. G. Paterson, *Efficient One-Round Key Exchange in the Standard Model, Information Security and Privacy*, Springer, Berlin, Heidelberg, 2008.

[9] L. Chen, Z. Cheng, and N. P. Smart, "Identity-based key agreement protocols from pairings," *International Journal of Information Security*, vol. 6, no. 4, pp. 213–241, 2007.

[10] K. Shim, "Efficient ID-based authenticated key agreement protocol based on Weil pairing," *IEEE Electronics Letters*, vol. 39, no. 8, pp. 653-654, 2003.

[11] S. Wang, Z. Cao, K. R. Choo, and L. Wang, "An improved identity-based key agreement protocol and its security proof," *Information Sciences*, vol. 179, no. 3, pp. 307–318, 2009.

[12] S. Blake-Wilson, D. Johnson, and A. Menezes, *Key Agreement Protocols and Their Security Analysis, Crytography and Coding*, Springer, Berlin, Heidelberg, 1997.

[13] H. Huang and Z. Cao, "An ID-based authenticated key exchange protocol based on bilinear Diffie-Hellman problem," in *Proceedings of the 4th International ACM Symposium on Information, Computer and Communications Security (ASIACCS '09)*, pp. 333–342, Sydney, Australia, March 2009.

[14] B. Lamacchia, K. Lauter, and A. Mityagin, "Stronger security of authenticated key exchange," in *Proceedings of the 1st International Conference on Provable Security (ProvSec '07)*, pp. 1–16, Wollongong, Australia, 2007.

[15] M. Bayat and M. Aref, "An attribute based key agreement protocol resilient to KCI attack," *International Journal of Electronics & Information Engineering*, vol. 2, no. 1, pp. 10–20, 2015.

[16] Z. Eslami, N. Pakniat, and M. Noroozi, "Cryptanalysis of an attribute-based key agreement protocol," *International Journal of Computer & Information Technologies*, vol. 2, pp. 351–358, 2014.

[17] Y. Wang, J. Song, H. Qiang, and Z. Liu, "An attribute-based key agreement protocol," *Computer Engineering*, vol. 40, no. 2, pp. 134–139, 2014.

[18] H. Wang, Q. Xu, and T. Ban, "A provably secure two-party attribute-based key agreement protocol," in *Proceedings of the Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP '09)*, H. Sakano, Ed., pp. 1042–1045, Kyoto, Japan, September 2009.

[19] H. Wang, Q. Xu, and X. Fu, "Two-party attribute-based key agreement protocol in the standard model," in *Proceedings of the International Symposium on Information Processing (ISIP '09)*, pp. 325–328, Huangshan, China, 2009.

[20] K. Yoneyama, "Strongly secure two-pass attribute-based authenticated key exchange," in *Proceedings of the Paring 2010*, M. Joye, Ed., pp. 147–166, Yamanaka Hot Spring, Japan, 2010.

[21] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 89–98, November 2006.

[22] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, Berkeley, Calif, USA, May 2007.

[23] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, "User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage," *IEEE Systems Journal*, vol. 12, no. 2, pp. 1767–1777, 2018.

[24] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 785–796, 2017.

[25] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 11, pp. 2150–2162, 2012.

[26] H. Qian, J. Li, Y. Zhang, and J. Han, "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation," *International Journal of Information Security*, vol. 14, no. 6, pp. 487–497, 2015.

[27] J. Han, W. Susilo, Y. Mu, J. Zhou, and M. H. A. Au, "Improving privacy and security in decentralized ciphertext-policy attribute-based encryption," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 665–678, 2015.

[28] K. Emura, A. Miyaji, K. Omote, A. Nomura, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," *International Journal of Applied Cryptography*, vol. 2, no. 1, pp. 46–59, 2010.

[29] J. Li, X. Lin, Y. Zhang, and J. Han, "KSF-OABE:outsourced attribute-based encryption with keyword search function for cloud storage," *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 715–725, 2017.

[30] J. Li, Y. Wang, Y. Zhang, and J. Han, "Full Verifiability for Outsourced Decryption in Attribute Based Encryption," *IEEE Transactions on Services Computing*, 2017.

[31] J. Li, Y. Shi, and Y. Zhang, "Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage," *International Journal of Communication Systems*, vol. 30, no. 1, 2017.

[32] J. Ning, Z. Cao, X. Dong, and L. Wei, "White-box traceable CP-ABE for cloud storage service: how to catch people leaking their access credentials effectively," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 883–897, 2018.

[33] J. Ning, X. Dong, Z. Cao, L. Wei, and X. Lin, "White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1274–1288, 2015.

[34] J. Li, Q. Yu, Y. Zhang, and J. Shen, "Key-Policy Attribute-Based Encryption against Continual Auxiliary Input Leakag," *Information Sciences*, 2018.

[35] J. Li, Q. Yu, and Y. Zhang, *Hierarchical Attribute Based Encryption with Continuous Leakage-Resilience*, Information Sciences, 2018.

[36] Y. Guo, J. Li, Y. Zhang, and J. Shen, "Hierarchical attribute-based encryption with continuous auxiliary inputs leakage," *Security and Communication Networks*, vol. 9, no. 18, pp. 4852–4862, 2016.

[37] C. Zuo, J. Shao, G. Wei, M. Xie, and M. Ji, "CCA-secure ABE with outsourced decryption for fog computing," *Future Generation Computer Systems*, vol. 78, pp. 730–738, 2018.

[38] J. Ning, Z. Cao, X. Dong, K. Liang, H. Ma, and L. Wei, "Auditable σ-time outsourced attribute-based encryption for access control in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 94–105, 2018.

[39] J. Li, Y. Guo, Q. Yu, Y. Lu, Y. Zhang, and F. Zhang, "Continuous leakage-resilient certificate-based encryption," *Information Sciences*, vol. 355-356, pp. 1–14, 2016.

[40] Y. Guo, J. Li, Y. Lu, Y. Zhang, and F. Zhang, "Provably secure certificate-based encryption with leakage resilience," *Theoretical Computer Science*, vol. 711, pp. 1–10, 2018.

[41] J. Li, H. Yan, and Y. Zhang, "Certificateless public integrity checking of group shared data on cloud storage," *IEEE Transactions on Services Computing*, 2017.

[42] H. Yan, J. Li, J. Han, and Y. Zhang, "A Novel Efficient Remote Data Possession Checking Protocol in Cloud Storage," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 78–88, 2017.

[43] H. Li, H. Zhu, S. Du, X. Liang, and X. Shen, "Privacy leakage of location sharing in mobile social networks: attacks and defense," *IEEE Transactions on Dependable and Secure Computing*, no. 99, 2016.

[44] Y. Liu, W. Guo, C. Fan, L. Chang, and C. Cheng, "A practical privacy-preserving data aggregation (3PDA) scheme for smart grid," *IEEE Transactions on Industrial Informatics*, 2018.

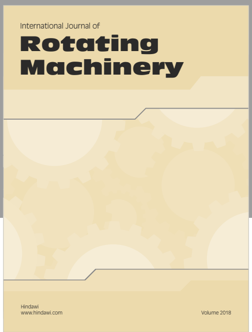
[45] B. Lynn, "Pairing-Based Cryptography (PBC) Library," 2013, http://crypto.stanford.edu/pbc.

[46] J. Li, L. Chen, Y. Lu, and Y. Zhang, "Anonymous certificate-based broadcast encryption with constant decryption cost," *Information Sciences*, vol. 454/455, pp. 110–127, 2018.

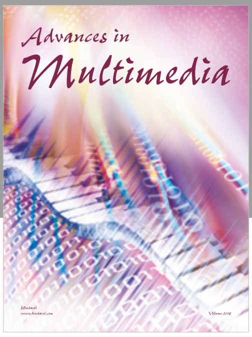
[47] J. Li, Q. Yu, and Y. Zhang, "Identity-based broadcast encryption with continuous leakage resilience," *Information Sciences*, vol. 429, pp. 177–193, 2018.

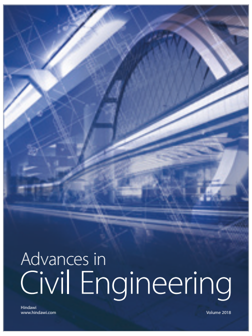
Journal of
Engineering

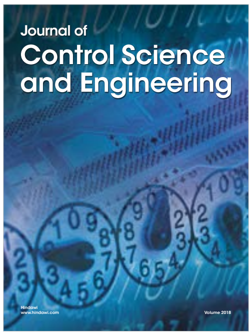
The Scientific
World Journal


International Journal of
Rotating
Machinery

Journal of
Sensors

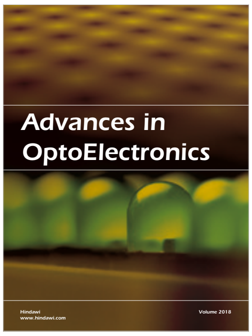

Advances in
Multimedia


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

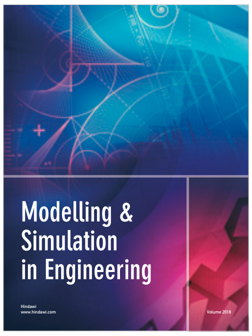
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

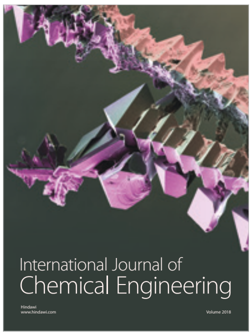

Advances in
OptoElectronics

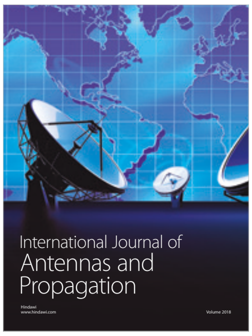
VLSI Design

International Journal of
Navigation and
Observation

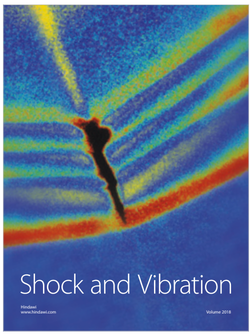

Modelling &
Simulation
in Engineering

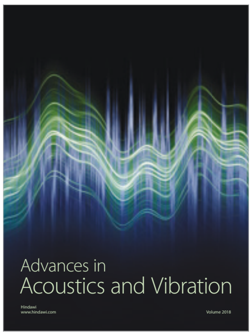
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration