Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2013, Article ID 810969, 7 pages
http://dx.doi.org/10.1155/2013/810969

Research Article

An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length

Changji Wang[1,2,3] and Jianfa Luo[1,2]

[1] *School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510006, China*
[2] *Guangdong Province Information Security Key Laboratory, Guangzhou 510006, China*
[3] *Research Center of Software Technology for Information Service, South China Normal University, Guangzhou 501631, China*

Correspondence should be addressed to Changji Wang; isswchj@mail.sysu.edu.cn

Received 21 January 2013; Accepted 16 March 2013

Academic Editor: Hai-lin Liu

There is an acceleration of adoption of cloud computing among enterprises. However, moving the infrastructure and sensitive data from trusted domain of the data owner to public cloud will pose severe security and privacy risks. Attribute-based encryption (ABE) is a new cryptographic primitive which provides a promising tool for addressing the problem of secure and fine-grained data sharing and decentralized access control. Key-policy attribute-based encryption (KP-ABE) is an important type of ABE, which enables senders to encrypt messages under a set of attributes and private keys are associated with access structures that specify which ciphertexts the key holder will be allowed to decrypt. In most existing KP-ABE scheme, the ciphertext size grows linearly with the number of attributes embedded in ciphertext. In this paper, we propose a new KP-ABE construction with constant ciphertext size. In our construction, the access policy can be expressed as any monotone access structure. Meanwhile, the ciphertext size is independent of the number of ciphertext attributes, and the number of bilinear pairing evaluations is reduced to a constant. We prove that our scheme is semantically secure in the selective-set model based on the general Diffie-Hellman exponent assumption.

1. Introduction

Cloud computing is a model for enabling ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. There are two main categories of cloud infrastructure: public cloud and private cloud. To take advantage of public clouds, data owners must upload their data to commercial cloud service providers which are usually considered to be semitrusted, that is, honest but curious [2]. That means the cloud service providers will try to find out as much secret information in the users' outsourced data as possible, but they will honestly follow the protocol in general.

Traditional access control techniques are based on the assumption that the server is in the trusted domain of the data owner, and therefore an omniscient reference monitor can be used to enforce access policies against authenticated users. However, in the cloud computing paradigm this assumption usually does not hold, and therefore these solutions are not applicable. There is a need for a decentralized, scalable, and flexible way to control access to cloud data without fully relying on the cloud service providers.

Data encryption is the most effective in regard to preventing sensitive data from unauthorized access. In traditional public key encryption or identity-based encryption systems, encrypted data is targeted for decryption by a single known user. Unfortunately, this functionality lacks the expressiveness needed for more advanced data sharing. To address these emerging needs, Sahai and Waters [3] introduced the concept of attribute-based encryption (ABE). Instead of encrypting to individual users, in ABE system, one can embed an access policy into the ciphertext or decryption key. Thus, data access is self-enforcing from the cryptography, requiring no trusted mediator.

ABE can be viewed as an extension of the notion of identity-based encryption in which user identity is generalized to a set of descriptive attributes instead of a single string specifying the user identity. Compared with identity-based encryption [4], ABE has significant advantage as it achieves flexible one-to-many encryption instead of one-to-one; it is envisioned as a promising tool for addressing the problem of secure and fine-grained data sharing and decentralized access control.

There are two types of ABE depending on which of private keys or ciphertexts that access policies are associated with.

In a key-policy attribute-based encryption (KP-ABE) system, ciphertexts are labeled by the sender with a set of descriptive attributes, while user's private key is issued by the trusted attribute authority captures an policy (also called the access structure) that specifies which type of ciphertexts the key can decrypt. KP-ABE schemes are suitable for structured organizations with rules about who may read particular documents. Typical applications of KP-ABE include secure forensic analysis and target broadcast [5]. For example, in a secure forensic analysis system, audit log entries could be annotated with attributes such as the name of the user, the date and time of the user action, and the type of data modified or accessed by the user action. While a forensic analyst charged with some investigation would be issued a private key that associated with a particular access structure. The private key would only open audit log records whose attributes satisfied the access policy associated with the private key. The first KP-ABE construction was provided by Goyal et al. [5], which was very expressive in that it allowed the access policies to be expressed by any monotonic formula over encrypted data. The system was proved selectively secure under the Bilinear Diffie-Hellman assumption. Later, Ostrovsky et al. [6] proposed a KP-ABE scheme where private keys can represent any access formula over attributes, including nonmonotone ones, by integrating revocation schemes into the Goyal et al. KP-ABE scheme.

In a ciphertext-policy attribute-based encryption (CP-ABE) system, when a sender encrypts a message, they specify a specific access policy in terms of access structure over attributes in the ciphertext, stating what kind of receivers will be able to decrypt the ciphertext. Users possess sets of attributes and obtain corresponding secret attribute keys from the attribute authority. Such a user can decrypt a ciphertext if his/her attributes satisfy the access policy associated with the ciphertext. Thus, CP-ABE mechanism is conceptually closer to traditional role-based access control method. The first CP-ABE scheme was proposed by Bethencourt et al. in [7], but its security was proved in the generic group model. Cheung and Newport [8] gave a CP-ABE construction under the Bilinear Diffie-Hellman assumption, but policies are restricted to a single AND gate. Later, Goyal et al. proposed a generic transformational approach to transform a KP-ABE scheme into a CP-ABE scheme using universal access tree in [9]. Their construction can support access structures which can be represented by a bounded size access tree with threshold gates as its nodes, and its security proof is based on the standard Decisional Bilinear Diffie-Hellman assumption. Unfortunately, in general this methodology would yield a ciphertext blowup of $O(n^{3.42})$ group elements for a Boolean formula of size n, which limits its usefulness in practice. The most efficient CP-ABE schemes in terms of ciphertext size and expressivity were proposed by Waters in [10], the size of a ciphertext depending linearly on the number of attributes involved in the specific policy for that ciphertext.

ABE has drawn extensive attention from both academia and industry, many ABE schemes have been proposed, and several cloud-based secure systems using ABE schemes have been developed [11, 12]. Most research work on ABE has focused on the design of expressive schemes, where access structures can implement as complex Boolean formulas as possible. Almost all existing ABE schemes that admit reasonably expressive decryption policies produce ciphertexts whose size depends at least linearly on the number of attributes involved in the policy. Emura et al. [13] proposed the first CP-ABE scheme with constant-size ciphertext, but policies are restricted to a single AND gate. Later, Herranz et al. [14] proposed the first CP-ABE scheme supporting threshold access structure with constant-size ciphertext. Recently, Attrapadung et al. [15] proposed a CP-ABE scheme with constant-size ciphertext for threshold access policies and where private keys remain as short as in previous systems. They also showed that a class of identity-based broadcast encryption schemes with linearity property generically yields monotonic KP-ABE systems in the selective-set model, at the expense of longer private keys of size $O(t \times n)$ elements, where n denotes the maximal number of attributes embedded in the ciphertext and t is the number of attributes in the access structure. Thus, this transformation provides us with monotonic KP-ABE schemes with constant-size ciphertexts by using identity-based broadcast encryption schemes with linearity property and constant ciphertext size. However, we notice that most of existing identity-based broadcast encryption schemes with constant-size ciphertext do not satisfy the linearity property, and it is not a necessary condition for constructing a KP-ABE schemes with constant-size ciphertext. In this paper, we propose a new KP-ABE construction with constant ciphertext size by adopting the idea of the Delerablee identity-based broadcast encryption scheme [16]. In our construction, the access policy can be expressed as any monotone access structure. Meanwhile, the ciphertext size is independent of the number of ciphertext attributes, and the number of bilinear pairing evaluations is reduced to a constant. We prove that our scheme is semantically secure in the selective-set model based on the general Diffie-Hellman exponent assumption.

The rest of this paper is organized as follows. Some necessary background knowledge about bilinear pairings, access structure and linear secret sharing scheme, and Delerablee identity-based broadcast encryption scheme are introduced in Section 2. The syntax and security notions of KP-ABE are given in Section 3. A concrete KP-ABE construction with constant-size ciphertext and its security argument will be presented in Section 4. We conclude our work and present our future work in Section 5.

2. Preliminary Works

We first introduce some notations. If $\mathbf{S}$ is a set, then $x \in_R \mathbf{S}$ denotes the operation of picking an element x uniformly random from $\mathbf{S}$. For a set $\mathbf{U}$, we define its power set as $2^{\mathbf{U}} = \{\mathbf{S} \mid \mathbf{S} \subseteq \mathbf{U}\}$. Let $\mathbf{u} = (u_1, \dots, u_k) \in \mathbf{Z}_p^k$ and $\mathbf{v} = (v_1, \dots, v_k) \in \mathbf{Z}_p^k$ be two row vectors; we denote the standard inner product by $\langle \mathbf{u}, \mathbf{v} \rangle$. A function $f(\lambda)$ is negligible if for every $c > 0$, there exists a λ_c, such that $f(\lambda) < 1/\lambda^c$ for all $\lambda > \lambda_c$.

2.1. Bilinear Pairings and the General Decisional Diffie-Hellman Exponent Assumption. Let $\mathbf{G}_1$, $\mathbf{G}_2$, and $\mathbf{G}_T$ be three cyclic groups of prime order p. Let g a generator of $\mathbf{G}_1$ and h be a generator of $\mathbf{G}_2$. A bilinear pairing $\widehat{e} : \mathbf{G}_1 \times \mathbf{G}_2 \rightarrow \mathbf{G}_T$ satisfies the following properties.

(i) Bilinearity: for $g \in_R \mathbf{G}_1$, $h \in_R \mathbf{G}_2$, and $a, b \in_R \mathbf{Z}_p$, we have $\widehat{e}(g^a, h^b) = \widehat{e}(g, h)^{ab}$.

(ii) Nondegeneracy: $\widehat{e}(g, h) \neq 1$, where 1 is the identity element of $\mathbf{G}_T$.

(iii) Computability: there is an efficient algorithm to compute $\widehat{e}(u, v)$ for $u \in_R \mathbf{G}_1$ and $v \in_R \mathbf{G}_2$.

Let $(\mathbf{G}_1, \mathbf{G}_2, \mathbf{G}_T, p, \widehat{e}$, and $g)$ be defined as above with $\mathbf{G}_1 = \mathbf{G}_2 = \mathbf{G}$. Let $g \in \mathbf{G}$ be a generator of $\mathbf{G}$, and set $g_t = \widehat{e}(g, g) \in \mathbf{G}_T$. Let s and n be positive integers; let $P \in \mathbf{Z}_p^*[X_1, \dots, X_n]^s$ and $Q \in \mathbf{Z}_p^*[X_1, \dots, X_n]^s$ be two s-tuples of n-variant polynomials over $\mathbf{Z}_p^*$. We write $P = (p_1, \dots, p_s)$ and $Q = (q_1, \dots, q_s)$ and impose that $p_1 = q_1 = 1$. For any function $h : \mathbf{Z}_p^* \rightarrow \Omega$ and vector $(x_1, \dots, x_n) \in \mathbf{Z}_p^{*n}$, $h(P(x_1, \dots, x_n))$ stands for $(h(p_1(x_1, \dots, x_n)), \dots, h(p_s(x_1, \dots, x_n))) \in \Omega^s$. We use a similar notation for the s-tuple Q. Let $f \in \mathbf{Z}_p^*[X_1, \dots, X_n]$. It is said that f depends on (P, Q), which we denote by $f \in \langle P, Q \rangle$, when there exists a linear decomposition:

$$f = \sum_{1 \le i,j \le s} a_{i,j} \cdot p_i \cdot p_j + \sum_{1 \le i \le s} b_i \cdot q_i, \quad a_{i,j}, b_i \in \mathbf{Z}_p. \tag{1}$$

As in [16], we make use of the General Decisional Diffie-Hellman Exponent (GDDHE) assumption.

Definition 1. Given the tuple $H(x_1, \dots, x_n) = (g^{P(x_1,\dots,x_n)}, g_t^{Q(x_1,\dots,x_n)}) \in \mathbf{G}^s \times \mathbf{G}_T^s$ as above and $T \in \mathbf{G}_T$, the (P, Q, f)-GDDHE problem is to decide whether T is equal to $g_t^{f(x_1,\dots,x_n)}$ or to some random element of $\mathbf{G}_T$.

2.2. Access Structure and Linear Secret Sharing Scheme

Definition 2. Let $\mathbf{P} = \{P_1, P_2, \dots, P_n\}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^{\mathbf{P}}$ is monotone if, for two sets $\mathbf{B}$ and $\mathbf{C}$, $\mathbf{B} \in \mathbb{A}$ and $\mathbf{B} \subseteq \mathbf{C}$, then $\mathbf{C} \in \mathbb{A}$. An access structure (resp., monotone access structure) is a collection (resp., monotone collection) $\mathbb{A}$ of nonempty subsets of $\mathbf{P}$. The sets in $\mathbb{A}$ are called the authorized sets, and the sets not in $\mathbb{A}$ are called the unauthorized sets.

Definition 3. Let $\mathbf{P}$ be a set of parties, $M_{\ell \times k}$ an $\ell \times k$ matrix, and $\rho : \{1, 2, \dots, \ell\} \rightarrow \mathbf{P}$ a function that maps a row to a party for labeling. A secret sharing scheme Π for access structure $\mathbb{A}$ over a set of parties $\mathbf{P}$ is a linear secret sharing scheme (LSSS) in $\mathbf{Z}_p$ and is represented by $(M_{\ell \times k}, \rho)$ if it consists of two efficient algorithms.

(i) Share$((M_{\ell \times k}, \rho), s)$: the share algorithm takes as input $s \in \mathbf{Z}_p$ which is to be shared. The dealer randomly chooses $\beta_2, \dots, \beta_k \in_R \mathbf{Z}_p$, and defines $\boldsymbol{\beta} = (s, \beta_2, \dots, \beta_k)^{\top}$. It outputs $M_{\ell \times k} \cdot \boldsymbol{\beta}$ as the vectors of ℓ shares. The share $\lambda_i = \langle \mathbf{M}_i, \beta^{\top} \rangle$ belongs to party $\rho(i)$, where $\mathbf{M}_i$ is the ith row of $M_{\ell \times k}$.

(ii) Recon$((M_{\ell \times k}, \rho), \mathbf{S})$: the reconstruction algorithm takes as input an access set $\mathbf{S} \in \mathbb{A}$. Let $\mathbf{I} = \{i \mid \rho(i) \in \mathbf{S}\}$. It outputs a set of constants $\{\mu_i\}_{i \in \mathbf{I}}$ such that $\sum_{i \in \mathbf{I}} \mu_i \cdot \lambda_i = s$.

In our context, the role of the parties is taken by the attributes. Thus, the access structure will contain the authorized sets of attributes. As in most relevant literatures [5, 6, 10], we will restrict ourselves to monotone access structures. In general, access policies can be described in terms of the monotonic Boolean formulas. There are standard techniques to convert any monotonic Boolean formula into a corresponding LSSS matrix [17].

2.3. The Delerablee Identity-Based Broadcast Encryption Scheme. Delerablee proposed the first identity-based broadcast encryption scheme with constant-size ciphertexts and private keys [16], which is described as follows.

(i) Setup$(1^{\lambda}, m)$: given the security parameter λ and an integer m, the algorithm generates a bilinear map group system $(\mathbf{G}_1, \mathbf{G}_2, \mathbf{G}_T, p, \widehat{e}, g$, and $h)$ as above and chooses a secret value $\gamma \in \mathbf{Z}_p^*$ and a cryptographic hash function $H : \{0,1\}^* \rightarrow \mathbf{Z}_p^*$. The master secret key is defined as msk $= (g, \gamma)$, and the public system parameters are defined as params $= (w, v, h, h^{\gamma}, \dots, h^{\gamma^m})$, where $w = g^{\gamma}$ and $v = \widehat{e}(g, h)$.

(ii) Extract(msk, ID): given msk $= (g, \gamma)$ and the identity ID, it outputs

$$\mathrm{sk}_{\mathrm{ID}} = g^{1/(\gamma + H(\mathrm{ID}))}. \tag{2}$$

(iii) Encrypt($\mathbf{S}$, params): assume for notational simplicity that $\mathbf{S} = \{\mathrm{ID}_j\}_{i=1}^{s}$, with $s \le m$. Given params $= (w, v, h, h^{\gamma}, \dots, h^{\gamma^m})$, the broadcaster randomly picks $k \in_R \mathbf{Z}_p^*$ and computes Hdr $= (C_1, C_2)$ and K, where

$$C_1 = w^{-k}, \qquad C_2 = h^{k \cdot \prod_{i=1}^{s} (\gamma + H(ID_i))}, \quad K = v^k. \tag{3}$$

(iv) Decrypt($\mathbf{S}$, ID_i, $\mathrm{sk}_{\mathrm{ID}_i}$, and Hdr, params): in order to retrieve the message encryption key K encapsulated in the header Hdr $= (C_1, C_2)$, user with identity ID_i and the corresponding private key $\mathrm{sk}_{\mathrm{ID}_i} = g^{1/(\gamma + H(\mathrm{ID}_i))}$ (with $\mathrm{ID}_i \in \mathbf{S}$) computes

$$K = \left(\widehat{e}\left(C_1, h^{p_{i,\mathrm{S}}(\gamma)}\right) \cdot \widehat{e}\left(\mathrm{sk}_{\mathrm{ID}_i}, C_2\right)\right)^{1/\prod_{j=1, j \neq i}^{s} H(\mathrm{ID}_j)} \tag{4}$$

with

$$p_{i,\mathrm{S}}(\gamma) = \frac{1}{\gamma} \cdot \left(\prod_{j=1, j \neq i}^{s} \left(\gamma + H\left(\mathrm{ID}_j\right)\right) - \prod_{j=1, j \neq i}^{s} H\left(\mathrm{ID}_j\right) \right). \tag{5}$$

Lemma 4. *The Delerablee identity-based broadcast encryption scheme is IND-sID-CPA secure under (f, g, F)-GDDHE assumption.*

3. Syntax and Security Notions for KP-ABE Scheme

Let $\mathbf{U} = \{\text{attr}_1, \ldots, \text{attr}_n\}$ be the universe of possible attributes, where each attr_i denotes an attribute and n is the total number of attributes. A KP-ABE scheme is parameterized by a universe of possible attributes $\mathbf{U}$ and consists of the following four polynomial-time algorithms.

(i) Setup(1^λ, $\mathbf{U}$): this probabilistic algorithm is run by the trusted attribute authority, which takes as input the security parameter λ and the attribute universe $\mathbf{U}$. It outputs some public parameters params and the master secret key msk. The trusted attribute authority publishes params and keeps msk secret.

(ii) KeyGen(params, msk, and $\mathbb{A}$): this probabilistic algorithm is run by the trusted attribute authority, which takes as input the public parameters params, the master secret key msk, and an access structure $\mathbb{A}$ which is assigned by the trusted attribute authority to the user. It outputs a decryption key $\text{SK}_{\mathbb{A}}$.

(iii) Encrypt(params, $\mathbf{W}$, and m): this probabilistic algorithm is run by the sender, which takes as input the public parameters params, a set of descriptive attributes $\mathbf{W}$, and a message $m \in \{0,1\}^*$. It outputs the ciphertext c.

(iv) Decrypt(params, c, and $\text{SK}_{\mathbb{A}}$): this deterministic algorithm is run by the recipient, which takes as input the public parameters params, the ciphertext c that was encrypted under the set of attributes $\mathbf{W}$, and the decryption key $\text{SK}_{\mathbb{A}}$ for access structure $\mathbb{A}$. It outputs the message m if $\mathbf{W} \in \mathbb{A}$.

Definition 5. A KP-ABE scheme is correct if, for any (params, msk) $\leftarrow$ Setup(1^λ, $\mathbf{U}$), any sets of attributes $\mathbf{W} \subseteq \mathbf{U}$, any message $m \in \{0,1\}^*$, and any $\text{SK}_{\mathbb{A}} \leftarrow$ KeyGen(params, msk, and $\mathbb{A}$) with $\mathbf{W} \in \mathbb{A}$, one has

$$\text{Decrypt}\left(\text{params, Encrypt}\left(\text{params, } \mathbf{W}\text{, and } m\right), \text{SK}_{\mathbb{A}}\right) = m \tag{6}$$

with probability 1 over the randomness of all the algorithms.

The property of indistinguishability for KP-ABE scheme under chosen plaintext and attribute-set attack is called selective-set model [5], which is defined in the following game between a challenger and an adversary.

(i) Initialization: the adversary declares the set of attributes $\mathbf{W}$ that he wishes to be challenged on.

(ii) Setup: the challenger runs the Setup algorithm of KP-ABE scheme and gives the public parameters to the adversary.

(iii) Phase 1: the adversary is allowed to issue queries for private keys with access structure $\mathbb{A}_j$ at most q_λ times with the restriction that $\mathbf{W} \notin \mathbb{A}_j$ for all j.

(iv) Challenge: the adversary submits two messages m_0 and m_1 with equal length. The challenger flips a random coin b and encrypts message m_b with $\mathbf{W}$. The ciphertext is then sent to the adversary.

(v) Phase 2: the same as Phase 1.

(vi) Guess: the adversary outputs his guess b' of b.

The advantage of an adversary in the above game is defined as $|\Pr[b' = b] - 1/2|$.

Definition 6. A KP-ABE scheme is secure in the selective-set model if all polynomial-time adversaries have at most a negligible advantage in the selective-set game.

The model can easily be extended to handle chosen ciphertext attacks by allowing for decryption queries in Phase 1 and Phase 2.

4. Our Construction

In this section, we present a new KP-ABE scheme with constant-size ciphertexts by adopting the idea of the Delerablee identity-based broadcast encryption scheme. The proposed KP-ABE construction is described as follows.

(i) Setup(1^λ, $\mathbf{U}$): given the security parameter λ, the trusted attribute authority chooses three cyclic groups $\mathbf{G}_1$, $\mathbf{G}_2$, and $\mathbf{G}_T$ of prime order p with a bilinear pairing $\hat{e} : \mathbf{G}_1 \times \mathbf{G}_2 \rightarrow \mathbf{G}_T$. Then the trusted attribute authority chooses two generators $g \in \mathbf{G}_1$ and $h \in \mathbf{G}_2$ as well as a secret value $\alpha \in_R \mathbf{Z}_p^*$ and a cryptographic hash function $H : \{0,1\}^* \rightarrow \mathbf{Z}_p^*$. The security analysis will view H as a random oracle. The master secret key is defined as msk $= (g, \alpha)$. The public parameters are params $= (w, v, h, h^\alpha, \ldots, h^{\alpha^n})$, where $w = g^\alpha$ and $v = \hat{e}(g, h)$.

(ii) KeyGen(params, msk, (M, ρ)): the algorithm computes a private key for an access structure that is associated with LSSS scheme $(M_{\ell \times k}, \rho)$ as follows. First, it generates shares of ℓ with the LSSS $(M_{\ell \times k}, \rho)$. Namely, it chooses a column vector $\boldsymbol{\beta} = (\beta_1, \beta_2, \ldots, \beta_k)^\top$ with $\beta_1 = s = 1$ and $\beta_2, \ldots, \beta_k \in_R \mathbf{Z}_p$. Then for each i from $i = 1$ to $i = \ell$, it calculates $\lambda_i = \langle \mathbf{M}_i, \boldsymbol{\beta}^\top \rangle$ and sets $\text{SK}_{(M,\rho)}$ as follows:

$$\text{SK}_{(M,\rho)} = \left\{D_i, \left(K_{i,j}\right)_{j=1}^{n}\right\}_{i=1}^{\ell} = \left\{g^{\lambda_i/(\alpha + H(\rho(i)))}, \left(h^{\lambda_i \alpha^j}\right)_{j=1}^{n}\right\}_{i=1}^{\ell}. \tag{7}$$

(iii) Encrypt(params, m, and $\mathbf{W}$): let t be the number of attributes included in the set of attributes $\mathbf{W}$, and denote $\mathbf{W}$ to be $\mathbf{W} = \{\omega_i\}_{i=1}^{t}$. The sender chooses $s \in_R \mathbf{Z}_p^*$ and computes the ciphertext $c = (c_0, c_1, \text{and } c_2)$, where

$$\begin{aligned} c_0 &= m \cdot v^s = m \cdot \hat{e}(g,h)^s, \\ c_1 &= w^{-s} = g^{-\alpha s}, \\ c_2 &= h^{s \cdot \prod_{i=1}^{t}(\alpha + H(\omega_i))}. \end{aligned} \tag{8}$$

(iv) Decrypt(params, c, and $\mathrm{SK}_{(M,\rho)}$): the ciphertext c labeled with the set of attributes $\mathbf{W} = \{\omega_i\}_{i=1}^{t}$ is parsed as $c = (c_0, c_1, \text{and } c_2)$. The recipient first sets $\mathbf{I} = \{i \mid \rho(i) \in \mathbf{W}\}$ and calculates the reconstruction constants $\{\mu_i\}_{i \in \mathbf{I}} = \mathrm{Recon}((M,\rho), \mathbf{W})$. The recipient's decryption key corresponding to the LSSS scheme (M,ρ) is parsed as $\mathrm{SK}_{(M,\rho)} = \{D_i, (K_{i,j})_{j=1}^{n}\}_{i=1}^{\ell}$. Then the recipient computes

$$p_{i,\mathbf{W}}(\alpha) = \frac{\lambda_i}{\alpha}\left(\prod_{j=1, j \neq i}^{t}\left(\alpha + H\left(\omega_j\right)\right) - \prod_{j=1, j \neq i}^{t} H\left(\omega_j\right)\right). \tag{9}$$

It is obvious that $p_{i,\mathbf{W}}(\alpha)$ is a polynomial on the variable α with degree $t-2$. The decrypting party can calculate $h^{p_{i,\mathrm{w}}(\alpha)}$ according to $(K_{i,j})_{j=1}^{n}$. Then the decrypting party computes

$$Y_i = \left(\hat{e}\left(c_1, h^{p_{i,\mathrm{w}}(\alpha)}\right) \cdot \hat{e}\left(D_i, c_2\right)\right)^{1/\prod_{j=1,j\neq i}^{t} H(\omega_j)} = \hat{e}(g,h)^{s\lambda_i}. \tag{10}$$

At last, the decrypting party calculates

$$Y = \prod_{i \in \mathbf{I}} Y_i^{\mu_i} = \hat{e}(g,h)^s, \qquad m = \frac{c_0}{Y}. \tag{11}$$

Theorem 7. *The proposed KP-ABE scheme is correct.*

Proof. Assume c is well formed, which means c is encrypted under the set of attributes $\mathbf{W} = \{\omega_i\}_{i=1}^{t}$; thus

$$\begin{aligned} Y_i &= \left(\hat{e}\left(c_1, h^{p_{i,\mathrm{w}}(\alpha)}\right) \cdot \hat{e}\left(D_i, c_2\right)\right)^{1/\prod_{j=1,j\neq i}^{t} H(\omega_i)} \\ &= \left(\hat{e}(g,h)^{-s\alpha(\lambda_i/\alpha)(\prod_{j=1,j\neq i}^{t}(\alpha + H(\omega_j)) - \prod_{j=1,j\neq i}^{t} H(\omega_j))}\right. \\ &\qquad \left. \cdot \hat{e}(g,h)^{s\lambda_i \prod_{i=1}^{t}(\alpha + H(\omega_j))}\right)^{1/\prod_{j=1,j\neq i}^{t} H(\omega_i)} \\ &= \left(\hat{e}(g,h)^{s\lambda_i \prod_{i=1}^{t} H(\omega_j)}\right)^{1/\prod_{j=1,j\neq i}^{t} H(\omega_i)} = \hat{e}(g,h)^{s\lambda_i}. \end{aligned} \tag{12}$$

So we have

$$Y = \prod_{i \in \mathbf{I}} Y_i^{\mu_i} = \prod_{i \in \mathbf{I}} \hat{e}(g,h)^{(s\lambda_i)\mu_i} = \hat{e}(g,h)^{s \cdot \sum_{i \in \mathbf{I}} \mu_i \cdot \lambda_i} = \hat{e}(g,h)^s. \tag{13}$$

This ends the proof. □

Theorem 8. *The proposed KP-ABE scheme is secure in the selective-set model under the (f, g, F)-GDDHE assumption.*

Proof. Suppose that there exists a polynomial-time adversary $\mathscr{A}$ that can attack the above KP-ABE scheme in the selective-set model with nonnegligible advantage. Then we can build a simulator $\mathscr{B}$ that can attack the Delerablee identity-based broadcast encryption scheme in the selective-ID model with nonnegligible advantage. The simulation proceeds as follows.

(i) Initialization: the adversary $\mathscr{A}$ chooses the set of attributes $\mathbf{W}^*$ which it wants to be challenged upon and sends $\mathbf{W}^*$ to the simulator $\mathscr{B}$. Then the simulator $\mathscr{B}$ sends this challenged attributes to the challenger $\mathscr{C}$ in the selective-ID model for the Delerablee identity-based broadcast encryption scheme. They treat each attribute as an ID in the Delerablee identity-based broadcast encryption.

(ii) Setup: the challenger $\mathscr{C}$ generates params and msk and sends params to the simulator $\mathscr{B}$; then $\mathscr{B}$ transfers them to the adversary $\mathscr{A}$.

(iii) Phase 1: the adversary $\mathscr{A}$ adaptively makes queries for private keys for access structure (M,ρ) that cannot be satisfied by $\mathbf{W}^*$. The simulator $\mathscr{B}$ picks vector $\boldsymbol{\beta} = (\beta_1, \beta_2, \ldots, \beta_k)^{\mathsf{T}}$ at random and calculates $\lambda_i = \langle \mathbf{M}_i, \boldsymbol{\beta}^{\mathsf{T}} \rangle$.

(1) If $\rho(i) \in \mathbf{W}^*$, then the simulator $\mathscr{B}$ picks $r_i \in_R \mathbf{Z}_p^*$ and submits the private key query r_i to the challenger $\mathscr{C}$. The challenger $\mathscr{C}$ will computes and returns the private key sk_{r_i} corresponding to r_i to $\mathscr{B}$. Finally, the simulator sets the private key part $D_i = (\mathrm{sk}_{r_i}^{\lambda_i}, \{h^{\lambda_i \alpha^j}\}_{j=1,\ldots,n})$.

(2) If $\rho(i) \notin \mathbf{W}^*$, then the simulator $\mathscr{B}$ submits the private key query $\rho(i)$ to the challenger $\mathscr{C}$. After the simulator $\mathscr{B}$ obtains the private key $\mathrm{sk}_{\rho(i)}$ corresponding to $\rho(i)$ from the challenger $\mathscr{C}$, the simulator sets the private key part $D_i = (\mathrm{sk}_{\rho(i)}^{\lambda_i}, \{h^{\lambda_i \alpha^j}\}_{j=1,\ldots,n})$.

(3) At last, $\mathscr{B}$ returns $\mathrm{sk}_{(M,\rho)} = \{D_i\}_{i=1,\ldots,\ell}$ to the adversary $\mathscr{A}$.

(iv) Challenge: the adversary $\mathscr{A}$ randomly chooses two messages m_0 and m_1 with equal length and sends them to the simulator $\mathscr{B}$. The simulator $\mathscr{B}$ then sends them to the challenger $\mathscr{C}$. The challenger $\mathscr{C}$ randomly encrypts m_b with the attributes set $\mathbf{W}^*$ and returns c_b to the simulator $\mathscr{B}$. Finally, the simulator $\mathscr{B}$ sends it to the adversary $\mathscr{A}$.

(v) Guess: the adversary $\mathscr{A}$ returns the guess b' to the simulator $\mathscr{B}$, and then the simulator $\mathscr{B}$ sends it to the challenger $\mathscr{C}$.

According to the observation of the attacker $\mathscr{A}$, the private keys he obtained from the simulator $\mathscr{B}$ are indistinguishable to those of obtained from the KeyGen algorithm. Thus, if the adversary $\mathscr{A}$ can attack the proposed KP-ABE scheme in the selective-set model with nonnegligible advantage, then

Table 1: Comparisons among ABE schemes with constant-size ciphertexts.

			Schemes		
	[13]	[14]	[15]-1	[15]-2	Our scheme
ABE types	CP-ABE	CP-ABE	CP-ABE	KP-ABE	KP-ABE
Access structure	AND	Threshold	Threshold	Monotone	Monotone
Private key size	$2\|\mathbf{G}\|$	$w\|\mathbf{G}_1\| + n\|\mathbf{G}_2\|$	$(n+w)\|\mathbf{G}\| + \|\mathbf{Z}_p^*\|$	$(n+1)t\|\mathbf{G}\|$	$t\|\mathbf{G}_1\| + nt\|\mathbf{G}_2\|$
Ciphertext size	$2\|\mathbf{G}\| + \|\mathbf{G}_T\|$	$\|\mathbf{G}_1\| + \|\mathbf{G}_2\| + \|\mathbf{G}_T\|$	$2\|\mathbf{G}\| + \|\mathbf{G}_T\|$	$2\|\mathbf{G}\| + \|\mathbf{G}_T\|$	$\|\mathbf{G}_1\| + \|\mathbf{G}_2\| + \|\mathbf{G}_T\|$
Encryption cost	0	0	$1p$	$1p$	$1p$
Decryption cost	$2p$	$3p$	$3p$	$2p$	$2p$

the simulator $\mathscr{B}$ can attack the Delerablee identity-based broadcast encryption scheme in the selective-ID model with nonnegligible advantage. According to Lemma 4, we can draw the conclusion that the proposed KP-ABE scheme is secure in the selective-set model under the (f, g, F)-GDDHE assumption.

This ends the proof. □

Table 1 compares efficiency among available ABE schemes with constant-size ciphertext. Attrapadung et al. [15] proposed a CP-ABE and KP-ABE scheme with constant-size ciphertexts, respectively; we denote them as [15]-1 scheme and [15]-2 scheme, respectively.

Comparisons are made in terms of private key size, ciphertext size, and the number of pairing evaluations upon encryption and decryption. In the table, we denote by n the number of attributes in the attributes universe, t the number of attributes in the access structure that describe the private key for KP-ABE scheme, w the number of attributes that describe the private key for CP-ABE scheme, and p the number of pairing evaluations.

5. Conclusion

In this paper, we have constructed a new KP-ABE scheme supporting any monotonic access structure with constant-size ciphertext and proved that the proposed scheme is semantically secure in selective-set model based on the general Diffie-Hellman exponent assumption. The downside of the proposed KP-ABE scheme is that private keys have multiple size growths in the number of attributes in the access structure. One interesting open problem would be to construct a KP-ABE scheme with constant-size ciphertexts that is secure under a more standard assumption or which achieves a stronger full security notion. Another challenging problem is to construct a KP-ABE scheme with constant ciphertext size and constant private key size.

Acknowledgments

This research is jointly funded by the National Natural Science Foundation of China (Grant no. 61173189) and the Guangdong Province Information Security Key Laboratory Project.

References

[1] P. Mell and T. Grance, "The NIST denition of cloud computing," Special Publication 800-145, 2011.

[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communication Security (ASIACCS '10)*, pp. 261–270, April 2010.

[3] A. Sahai and B. Waters, "Fuzzy identity based encryption," in *Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT '05)*, vol. 3494 of *Lecture Notes in Computer Science*, pp. 457–473, Springer, 2005.

[4] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," in *Proceedings of the Annual International Cryptology Conference (CRYPTO '01)*, vol. 2139 of *Lecture Notes in Computer Science*, pp. 213–229, Springer, 2001.

[5] 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.

[6] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pp. 195–203, November 2007.

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

[8] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pp. 456–465, November 2007.

[9] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in *Proceedings of the 35th international colloquium on Automata, Languages and Programming, Part II (ICALP '08)*, vol. 5125 of *Lecture Notes in Computer Science*, pp. 579–591, Springer, 2008.

[10] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in *Proceedings of the International Conference on Practice and Theory in Public Key Cryptography (PKC '11)*, vol. 6571 of *Lecture Notes in Computer Science*, pp. 53–70, Springer, 2011.

[11] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," *Journal of Computer Security*, vol. 18, no. 5, pp. 799–837, 2010.

[12] M. Li, S. C. Yu, Y. Zheng, K. Ren, and W. J. Lou, "Scalable and secure sharing of personal health records in cloud computing

using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.

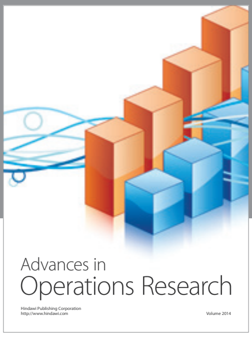
[13] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy, attribute-based encryption scheme with constant ciphertext length," in *Proceedings of the International Conference (ISPEC '09)*, vol. 5451 of *Lecture Notes in Computer Science*, pp. 13–23, Springer, 2009.

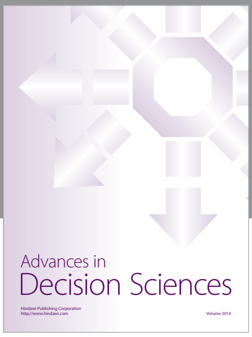
[14] J. Herranz, F. Laguillaumie, and C. Rafols, "Constant size ciphertexts in thresh-old attribute-based encryption," in *Proceedings of the 13th International Conference on Practice and Theory in Public Key Cryptography (PKC '10)*, vol. 6056 of *Lecture Notes in Computer Science*, pp. 19–34, Springer, 2010.

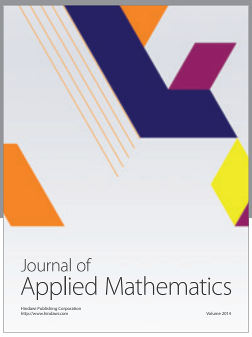
[15] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Ràfols, "Attribute-based encryption schemes with constant-size ciphertexts," *Theoretical Computer Science*, vol. 422, pp. 15–38, 2012.

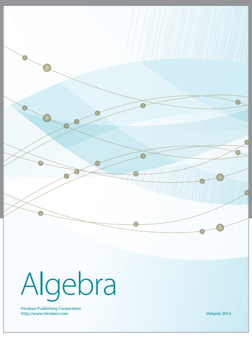
[16] C. Delerablee, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in *Proceedings of the Advances in Crypotology 13th International Conference on Theory and Application of Cryptology and Information Security (ASCIACRYPT '07)*, vol. 4833 of *Lecture Notes in Computer Science*, pp. 200–217, Springer, 2007.

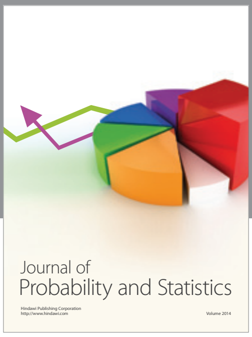
[17] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Proceedings of the 30th Annual International Conference on Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT '11)*, vol. 6632 of *Lecture Notes in Computer Science*, pp. 568–588, Springer, 2011.


Advances in
Operations Research

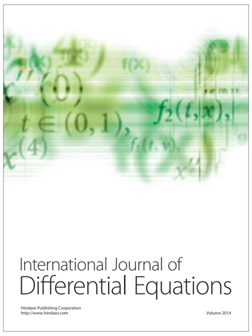

Advances in
Decision Sciences


Journal of
Applied Mathematics

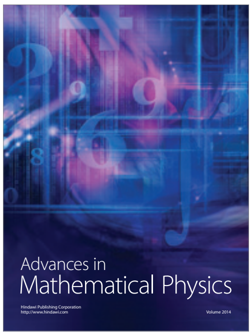

Algebra

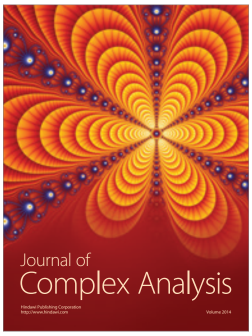

Journal of
Probability and Statistics

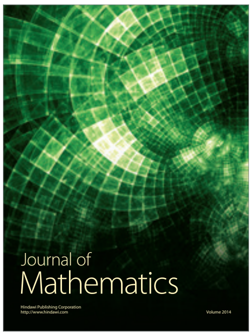
The Scientific
World Journal

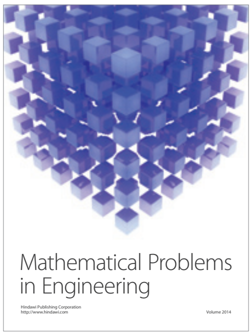

International Journal of
Differential Equations

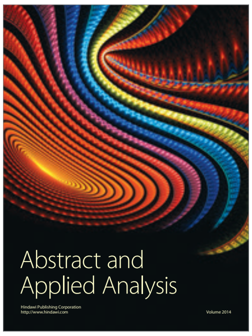
International Journal of
Combinatorics

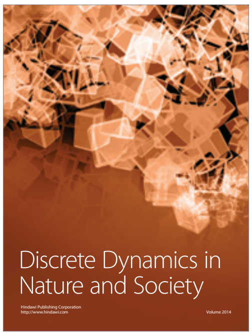

Advances in
Mathematical Physics

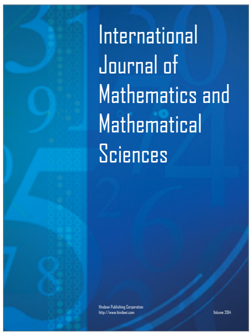

Journal of
Complex Analysis


Journal of
Mathematics


Mathematical Problems
in Engineering

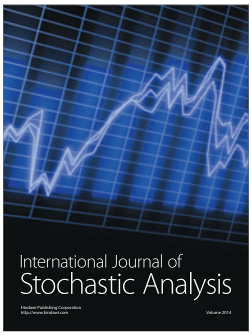

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


International Journal of
Stochastic Analysis

Journal of
Optimization