Scalable Attribute-Based Encryption Under the Strictly Weaker Assumption Family

Yuqiao Deng[a], Ge Song[b]

[a] *School of Mathematics And Statistics, Guangdong University of Finance and Economics, Guangzhou, China*
[b] *College of Mathematics And Informatics, South China Agricultural University, Guangzhou, China*

Abstract

Attribute-Based Encryption (ABE) is a special type of public key encryption that allows users to share sensitive data efficiently through fine-grained access control. The security involved in existing ABE systems is currently insufficient. These systems are usually built on the Decisional Bilinear Diffie-Hellman (DBDH) assumption or the q-type DBDH assumption, which is stronger than the DBDH assumption. However, once the DBDH assumption is unsecure, all concerned ABEs become vulnerable to threats. To address this problem, the k-BDH assumption family proposed by Benson et al. is adopted. Any assumption in the k-BDH assumption family is associated with parameter k and becomes strictly weaker as k increased. We propose a framework to implement Ciphertext-Policy Attribute Based Encryption (CP-ABE) under the arbitrary assumption in the k-BDH assumption family. When the k'-BDH assumption in the k-BDH assumption family becomes unsecure, where k'-BDH is the assumption on which our ABE relies, the scheme can be shifted to rely on the l'-BDH assumption instead, where $l' > k'$. This condition guarantees security as the underlying assumption of our scheme becomes weaker. In addition, we define the formal security model of our schemes and prove the security of CP-ABE in the selective attribute model.

Keywords: KP-ABE, CP-ABE, k-BDH assumption family, selective security model, strictly weaker

1. Introduction

Attribute Based Encryption (ABE), as presented by Sahai and Waters [1], is an influential paradigm for embedding a complex access policy into encrypted data. Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) are commonly used ABE schemes [2]. In KP-ABE, ciphertext is associated with the attribute set, and the private key is associated with the access policy. In the case of CP-ABE, ciphertext is associated with the access policy, and the private key is associated with the attribute set.

In recent years, interest in ABEs has grown because of their new functionalities [3, 4] or better performance [5, 6, 7]; *however, they often suffer from two undetectable security problems as described below*:

(1) *q-type DBDH assumptions may not guarantee ABE security when encountering Cheon's attack [8].* Most proposed ABEs are reduced to "q-type DBDH" assumptions [3, 9, 7, 10, 2]. Nevertheless, Cheon [8] claimed that q-type assumptions and the associated ABEs may be vulnerable to special attacks. Consider the well-known q-Decisional Bilinear Diffie-Hellman Exponent Assumption (q-DBDHE). This assumption is often used by all kinds of ABEs [10][11]; we briefly describe it as follows:

Definition 1 (q-DBDHE)[10][11]) Let $\mathbb{G}$ be a group of prime order p, g be a generator of $\mathbb{G}$, and $a, s \overset{R}{\leftarrow} Z_p$ be two integers. Given tuples:

$$\vec{X} = (\mathbb{G}, p, g, g^a, ..., g^{a^q}, g^{a^{q+2}}, ..., g^{a^{2q}}).$$

The adversary is unable to distinguish element $g^{a^{q+1}}$ from a random element R in group $\mathbb{G}$.

Most ABEs are reduced to q-DBDHE to enforce security, where parameter q denotes the number of attributes. However, security may be threatened as the number of attributes increases. In [8], Cheon formulated the following theorem:

Theorem 1 *A cyclic group G with prime order p is chosen, and g is an element of G. Let d be a positive divisor of $p-1$. Let $g, g_1 = g^{\alpha}$ and $g_d = g^{\alpha^d}$, then one can use $O(max\{\sqrt{p-1/d}, \sqrt{d}\})$ memory to compute α in $O(\log p(\sqrt{p-1/d} + \sqrt{d}))$ group operations.*

Theorem 1 implies that ABE security decreases when the attribute number (i.e., d) increases. Cheon pointed out that, compared with the

DBDH assumption, the q-type DBDH assumption has computational complexity reduced by $\sqrt{d}$.

(2) *Any single assumption may be compromised when new attacks against the assumption are found.* Most ABE frameworks are built to adapt to one assumption, but the above frameworks fail to provide a "scalable" property, i.e., when the current assumption becomes compromised, existing ABEs cannot provide a "plug and play" mechanism to shift to a new framework that is based on a more secure assumption. In other words, the existing ABE framework is relatively "fixed" for *one assumption.*

We simultaneously overcome the above two problems by employing a new *scalable* ABE framework that can flexibly "switch" the based assumption to a more secure assumption in an assumption series defined as Ł, with the limitation that it must satisfy the following three conditions. First, each assumption in Ł is weaker than q-type DBDH assumptions. Second, each assumption is associated with a parameter κ, and we denote this assumption as AS_{κ}. Third, the assumption AS_{κ} in Ł becomes progressively weaker as κ increases.

While utilizing the assumption series Ł, an ABE framework that can accommodate an arbitrary assumption in Ł can be constructed so that the two secure problems mentioned above may be addressed. First, since any assumption in Ł is weaker than a q-type DBDH assumption, this improved ABE is more secure than the existing schemes based on q-type assumptions. The method for addressing the second secure problem is intuitive: when the current assumption AS_{κ_1} becomes unsecure, we switch to an *even weaker assumption*, AS_{κ_2} where $\kappa_1 < \kappa_2$, which replaces AS_{κ_1} and guarantees the security of the scheme (according to the property of Ł, assumption AS_{κ_2} is weaker than assumption AS_{κ_1}).

The remaining problem is that a series of assumptions, Ł, must be formulated, and a suitable framework for Ł must be constructed. Recently, Benson et al. [12] have proposed a proper assumption family, k-BDH. This assumption family satisfies all properties of assumption series Ł. We provide a brief introduction to the k-BDH assumption family below.

1.1. k-BDH Assumption Family

The k-BDH assumption family, first proposed in [12], is a decisional assumption family. We describe the k-BDH assumption as

A group $\mathbb{G}$ with prime order p be chosen. Let $x, y, r_1, ..., r_k$ be chosen at random and $g, v_1, ..., v_k$ be generators of $\mathbb{G}$. The adversary must distinguish the target element $e(g,g)^{xy(r_1+\cdots+r_k)}$ from a random element $T \in \mathbb{G}_T$.

Formally, if an adversary $\mathcal{B}$ is given:

$$\vec{z} = (g, g^x, g^y, v_1, ..., v_k, v_1^{r_1}, ..., v_k^{r_k}).$$

it is difficult for it to distinguish $K = e(g,g)^{xy(r_1+\cdots+r_k)}$ from a random element in $\mathbb{G}_T$.

The advantage ε of Algorithm $\mathcal{B}$ in solving the k-BDH assumption in $\mathbb{G}$ is defined as

$$|Pr[\mathcal{B}(\vec{z}, T = K) = 0] - Pr[\mathcal{B}(\vec{z}, T = R) = 0]| \geq \varepsilon.$$

Each k-BDH assumption is associated with a parameter k. When $k = 1$, the 1-BDH assumption is given $(g, g^x, g^y, v_1, v_1^{r_1})$, distinguish $T = e(g,g)^{xyr_1}$ from a random element in $\mathbb{G}_T$. Benson et al. [12] proved that the 1-BDH assumption is equivalent to the DBDH assumption. They also proved that assumptions in the k-BDH assumption family become progressively weaker when k increases (Section 4 in [12]). For example, the 2-BDH assumption is weaker than the 1-BDH assumption, 3-BDH is weaker than 2-BDH, and so on.

We demonstrate that the k-BDH assumption family satisfies three properties of Ł. First, considering that the DBDH assumption is weaker than the q-type DBDH assumption, the 1-BDH assumption is equivalent to the DBDH assumption, and the l-BDH assumption is weaker than 1-BDH $(l > 1)$, we can deduce that the k-BDH assumptions $(k \geq 1)$ are weaker than the q-type DBDH assumption. Second, the k-BDH assumption family satisfies the second property of Ł because each k-BDH assumption is associated with a parameter k . Finally, the k-BDH assumption family satisfies the third property of Ł in that assumptions in the k-BDH assumption family become progressively weaker. Therefore, the k-BDH assumption family meets the requirements of the assumption series Ł.

1.2. Contributions

The contributions of this paper are multifold. First, considering that trivial ABE scheme may become vulnerable to severe attacks and unable to shift to a new assumption, we propose a ABE framework that can flexibly ”generate” an ABE scheme on an arbitrary assumption in an assumption series that becomes progressively weaker. Our framework serves the benefit of simply adding some public parameters and system switches to rely on a new assumption, thus making redesigning a new system unnecessary. Second, we demonstrate the implementation of the above mentioned framework. A CP-ABE scheme is proposed. The CP-ABE scheme is built by adapting to the k-BDH assumption family, and it can be constructed on an arbitrary assumption in the same assumption family. This scheme is capable of easily switching between based assumptions in the k-BDH assumption when the relied-on assumption is attacked instead of redesigning the whole scheme. Third, we formally prove the security of the proposed scheme and analyze its performance in terms of computational and storage overhead.

1.3. Related Work

The first work on Identity-Based Encryption (IBE) [13] was proposed by Boneh-Franklin a decade ago. Several works that focused different types of IBE schemes are presented [14][15][16].

Benson, Shacham and Waters [12] proposed an IBE system based on an arbitrary assumption in the k-BDH assumption, proving that the assumption can generalize the DBDH assumption. Their work strengthens the security of IBE because one can create a scheme reduced to a weak enough assumption in the k-BDH assumption family as needed.

Research on IBE has also been conducted by Sahai and Waters [1]. They proposed a Fuzzy IBE scheme that provides a mechanism for provider to control how data are shared within the encryption algorithm. Basing on this scheme, Sahai and Waters [1] presented ABE.

Most existing ABE schemes are based on the DBDH or q-type DBDH assumption. For example, in terms of KP-ABE, Goyal, Pandey, Sahai, and Waters [2] proposed an expressive KP-ABE scheme that uses fine-grained access control based on the DBDH assumption. Attrapadung et al. [17] proposed another scheme with constant-size ciphertexts based on the q-DBDHE assumption (q-Decisional Bilinear Diffie-Hellman Exponent, a type of q-type DBDH), while Ostrovsky et al. [9] proposed one with a non-monotonic access structure where secret keys are associated with a set of attributes including positive and negative attributes based on the DBDH assumption. Rouselakis and Waters [18] proposed a KP-ABE scheme with a large universe using a new proving method under the assumption called "q-2", which belongs to a q-type DBDH assumption.

In terms of CP-ABE, Bethencourt et al. [19] uses a monotonic access tree as access structure to propose the first CP-ABE construction in 2007. However, the security of their scheme is limited, and their system is secure only in the generic group model. Waters [10] proposed three CP-ABE schemes that express the access structure using the Linear Secret Sharing Scheme (LSSS); the three CP-ABEs are based on the q-parallel DBDHE assumption (q-parallel Bilinear Diffie-Hellman Exponent problem, a type of q-type DBDH), the q-DBDHE assumption, and the DBDH assumption. CP-ABE has attracted increasing interest. For example, Goyal et al. proposed a bounded CP-ABE on the DBDH assumption, Chase [3] proposed multi-authority CP-ABE on the DBDH assumption, Rouselakis and Waters [18] proposed a CP-ABE with a large universe on the so-called "q-1" assumption, which is a type of q-type DBDH assumption.

Most recently, Zhou et al. proposed an efficient privacy-preserving CP-ABE[20]; Boyen proposed ABE based on lattices [21]. Zhang et al. proposed multi-authority ABE from lattices [22]. Takashima proposed a new proof techniques for DLIN-Based adaptively secure ABE [23]. Rahulamathavan proposed a novel user collusion avoidance Scheme for KP-ABE [24]. Crampton et al. proposed ABE for Access Control Using Elementary Operations [25]. GIACON et al. proposed a proof of security for a KP-RS-ABE scheme [26]. Fu proposed unidirectional proxy re-encryption for access structure transformation in ABE [27].

2. Background

Bilinear maps, access structures, and LSSS are first defined. Finally, the security definitions of CP-ABE are formulated.

2.1. Bilinear Maps

Two multiplicative cyclic groups $\mathbb{G}$ and $\mathbb{G}_T$ with prime order p be chosen. Generator g of $\mathbb{G}$ be chosen, and let e be such a bilinear map that $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ and

1. Bilinearity: assuming u, v are elements of $\mathbb{G}$ and $a, b \in \mathbb{Z}_p$, then it holds that $e(u^a, v^b) = e(u, v)^{ab}$.

2. Non-degeneracy: $e(g, g) \neq 1$.

2.2. Access Structures

Definition 2 (Access Structure [28]) A set of parties be denoted as $\{Q_1, Q_2, ..., Q_n\}$. We say the collection of $\mathbb{A} \subseteq 2^{\{Q_1, Q_2, ..., Q_n\}}$ is monotone $if\ \forall A, B : if\ A \in \mathbb{A}\ and\ A \subseteq B\ then\ B \in \mathbb{A}$.

In this paper, attributes are the equivalent of the parties. In our context, the access structure is monotone [10].

2.3. Linear Secret-Sharing Schemes

Definition 3 (Linear Secret-Sharing Schemes (LSSS)) A secret-sharing scheme Π over a set of parties P is called linear (over $\mathbb{Z}_p$) if

(1) A vector is formed by the shares for each party over $\mathbb{Z}_p$.

(2) We call the matrix M with l rows and n columns the share-generating matrix. For all $i = 1, ..., l$, we let the function ρ be defined the party labeling row i as $\rho(i)$. When aiming to share a secret $s \in \mathbb{Z}_p$, we choose a random vector $v = (s, r_2, ..., r_n)$, where $r_2, ..., r_n \in \mathbb{Z}_p$ are randomly chosen, then $(Mv)_i$ for $i = 1, ..., l$ is the l shares of the secret s and the party $\rho(i)$ owns the share $(Mv)_i$.

As mentioned in [28] that, every LSSS also possesses the *linear reconstruction* property. Linear reconstruction is defined as follows: let $S \in \mathbb{A}$ be any authorized set, and let $I \subset (1, 2, ..., l)$ be the following set that $I = (i : \rho(i) \in \mathbb{Z}_p)$. A constant set that satisfies $\omega_i \in \mathbb{Z}_p$ must exist. If λ_i are valid shares of any secret s, then we have: $\sum_{i \in I} \omega_i \lambda_i = s$.

3. Our Proposed CP-ABE Scheme

A straightforward method to directly construct an ABE system on the k-BDH assumption is lacking. We explain the difficulty in reducing ABE security to the k-BDH assumption.

In the k-BDH assumption, we are given $2k + 3$ elements in group $\mathbb{G}$, which are referred to as "the given terms": $(g, g^x, g^y, v_1, ..., v_k, v_1^{\hat{r}_1}, ..., v_k^{\hat{r}_k})$ and to distinguish the target term $T = e(g, g)^{xy(\hat{r}_1 + \cdots + \hat{r}_k)}$. As in most encryption schemes, we use the target term to randomize the encrypted message m (e.g., we can randomize the encrypted message m by generating the ciphertext component $C_0 = m \cdot e(g, g)^{xy(\hat{r}_1 + \cdots + \hat{r}_k)}$) and then use the given terms to generate ciphertext components and private key components. However, this process is difficult because the given terms include bases $(v_1, v_2, ..., v_k)$ that we cannot directly transform to the generator g, which is the *only generator* that exists in the target term. To combine the encrypted message (e.g., C_0) with the other ciphertext components and private key components, we must express the relations between the target term and the given terms, and we must *implicitly* associate generator g with generator $(v_1, v_2, ..., v_k)$.

Our CP-ABE scheme is a variant of Waters' CP-ABE scheme that was proposed on the DBDH assumption (Section 6 of [10]). To adapt Waters' scheme to the k-BDH assumption, we use the cancellation trick of [12]. We build a connection between generator g and generators $(v_1, ..., v_k)$ by setting $v_t = g^{s_t}$ for $t = 1, ..., k$. For any v_t, we choose a random a_t and implicitly set a corresponding element: $s_{t,1} = a_t y / s_t$ and set $r_t = \hat{r}_t / a_t$. Then, we can create the target term $e(g,g)^{xy(\hat{r}_1 + r_2 + \cdots + \hat{r}_k)}$ according to the given terms and the terms of $s_{t,1}, (t \in [k])$: $\prod_{t\in[k]} e(g^x, v_t^{r_t})^{s_{t,1}} = \prod_{t\in[k]} e(g^x, g^{s_t})^{\hat{r}_t / a_t \cdot a_t y / s_t} = \prod_{t\in[k]} e(g,g)^{xy\hat{r}_t}$ (let set $[k]$ denote a positive integer set in which all positive integers in the set are less than or equal to positive integer k).

The formal definition of CP-ABE is as follows.

3.1. Ciphertext-Policy ABE

A CP-ABE scheme based on the k'-BDH assumption includes four algorithms: *Setup, Encrypt, KeyGen*, and *Decrypt.* The k'-BDH assumption belongs to the k-BDH assumption family, where parameter k' is the corresponding value of the assumption.

Setup(λ,U,k'). A security parameter λ, an attribute universe description U, and parameter k' are all used as inputs to the setup algorithm. The outputs are public parameters PK and a master key MSK.

Encrypt(PK,m,$\mathbb{A}$). Public parameters PK, a message m, and an access structure $\mathbb{A}$ over the attribute universe are used as inputs to the encryption algorithm. Ciphertext CT is encrypted using message m and access structure $\mathbb{A}$. A user must own a set of attributes that satisfies the access structure $\mathbb{A}$ to decrypt the ciphertext.

Key Generation(MK,S). A master key MSK and a set of attributes S that describes the key are used as inputs to the key generation algorithm. The output is a private key SK.

Decrypt(PK,CT,SK). Public parameters PK, a ciphertext CT linked with an access policy $\mathbb{A}$, and a private key SK associated with a set S of attributes are used as inputs to the decryption algorithm. This algorithm can decrypt the ciphertext and recover a message m once the access structure $\mathbb{A}$ is satisfied by the set of attribute set S.

Security Model for CP-ABE. The security model of CP-ABE is a game between the challenger and the adversary. First, the adversary publishes the challenge access structure $\mathbb{A}^*$. The adversary can ask the challenger to encrypt message m in respect of the access structure $\mathbb{A}^*$ and also can query for any private key corresponding to attribute set S such that S does not satisfy $\mathbb{A}^*$. We give the formal security game as follows.

Init. The adversary publishes a challenging access structure $\mathbb{A}^*$, which it will attempt to attack.

Setup. The challenger runs the setup algorithm and generates public parameters PK, which are then given to the adversary.

Phase 1. The adversary can repeatedly query the private keys associated with sets of attributes $S_1, ..., S_{q_1}$. The limitation of each query is that none of the queried attribute sets satisfies the challenging access structure $\mathbb{A}^*$.

Challenge. The adversary must submit two equal-length messages m_0 and m_1. The challenger flips a coin b and encrypts message m_b under the challenging access structure $\mathbb{A}^*$. The challenger gives the ciphertext CT^* to the adversary.

Phase 2. Phase 1 is repeated with the same limitation that none of the sets of queried attributes $S_{q_1+1}, ..., S_q$ satisfies the challenging access structure $\mathbb{A}^*$.

Guess. The adversary outputs a guess b' of b. The advantage of an adversary in this game is defined as $Pr[b' = b] - \frac{1}{2}$.

Definition 4. A CP-ABE scheme is secure if all polynomial time (PPT) adversaries have at most a negligible advantage ε in the above game.

3.2. Our Proposed CP-ABE Scheme

3.3. Proposed CP-ABE Scheme

We restrict $\rho(.)$, a function that associates rows of a LSSS matrix M to attributes, to be injective. Let set $[x]$ denote a positive integer set where all integers in the set are less than or equal to positive integer x, i.e., $[x] = \{1, 2, ..., x\}$. We give our construction as follows.

Setup(U,n_{max},k') The setup algorithm takes the number of attributes U, the maximum number of columns n_{max} in the access structure matrix, and parameter k' as inputs. Parameter k' implies that the scheme must be constructed on the k'-BDH assumption, i.e., the assumption is given the terms $(g, g^x, g^y, v_1, ..., v_{k'}, v_1^{r_1}, ..., v_{k'}^{r_{k'}})$ and to distinguish the term of $e(g, g)^{xy(r_1+\cdots+r_{k'})}$.

The setup algorithm selects the following: a group $\mathbb{G}$ of prime order p and generators $g, v_1, ..., v_{k'},\ x, a_1, ..., a_{k'}, r_1, ..., r_{k'} \in Z_p$, and $k' \times n_{max} \times U$ random elements $(h_{1,1,1}, ..., h_{k',n_{max},U})$.

The public key is published as

$$g, g^x, v_t : (t \in [k']), v_t^{r_t} : (t \in [k']), h_{t,i,j} : (t \in [k'], i \in [n_{max}], j \in [U]).$$

The algorithm sets the master secret key $MSK = (r_1, ..., r_{k'}, x)$.

Encrypt(PK,(M,ρ),m) The encryption algorithm uses public parameters PK, a message m, and an LSSS access structure (M, ρ) as inputs. Function $\rho(.)$, which is an injective function, associates rows of M to attributes.

Assuming that M is an $\ell \times n_{max}$ matrix. The algorithm chooses k' random vectors $\overrightarrow{v_1} = (s_{1,1}, s_{1,2}, ..., s_{1,n_{max}}), ..., \overrightarrow{v_{k'}} = (s_{k',1}, s_{k',2}, ..., s_{k',n_{max}})$. The above k' vectors will be used to share the k' encryption exponents $s_{1,1}, ..., s_{k',1}$.

The algorithm first computes

$$C_0 = m \cdot e(g^x, v_1^{r_1})^{s_{1,1}} e(g^x, v_2^{r_2})^{s_{2,1}} \cdots e(g^x, v_{k'}^{r_{k'}})^{s_{k',1}} = m \prod_{t \in [k']} e(g^x, v_t^{r_t})^{s_{t,1}}.$$

Then, the algorithm computes

$$C_t = v_t^{s_{t,1}} : (t \in [k']).$$

Finally, the algorithm computes

$$C_{t,i,\tau} = g^{xM_{\tau,i} \cdot s_{t,i}} h_{t,i,\rho(\tau)}^{-s_{t,1}} : (t \in [k'], i \in [n_{max}], \tau \in [\ell]).$$

Ciphertext is published as

$$C_0, C_t : (t \in [k']), C_{t,i,\tau} : (t \in [k'], i \in [n_{max}], \tau \in [\ell]).$$

along with a description of (M, ρ).

KeyGen(MSK,S) The KeyGen algorithm takes the MSK and a set S of attributes as inputs. The algorithm chooses $k' \times n_{max}$ random elements

$$p_{t,i} \in Z_p : (t \in [k'], i \in [n_{max}]).$$

The algorithm first computes

$$K_t = g^{xr_t} g^{xp_{t,1}} : (t \in [k']).$$

Then, the algorithm computes

$$L_{t,i} = v_t^{p_{t,i}} : (t \in [k'], i \in [n_{max}]).$$

Finally, the algorithm computes

$$N_{t,\chi} = \prod_{i \in [n_{max}]} (h_{t,i,\chi})^{p_{t,i}} : (t \in [k'], \chi \in S).$$

The private key is issued to the user as follows

$$K_t : (t \in [k']), L_{t,i} : (t \in [k'], i \in [n_{max}]), N_{t,\chi} : (\chi \in S, t \in [k']).$$

Decrypt(CT,SK) The decryption algorithm takes ciphertext CT for access structure (M, ρ) and a private key for set S as inputs. Assuming that attribute set S satisfies the access structure, we define set $J = \{\tau : \rho(\tau) \in S\}$. Then, if for some $t \in [k']$, terms $\{\lambda_{t,\tau} = M_{t,\tau} \cdot \overrightarrow{v_t}\}$ are valid shares of secret $s_{t,1}$ over access matrix M, we can find a constant set $\{\omega_{t,\tau} \in \mathbb{Z}_p\}_{\tau \in J}$ efficiently that satisfies

$$\begin{gathered}\sum_{\tau \in J} \omega_{t,\tau} M_{\tau,1} = 1, \\ \sum_{\tau \in J} \omega_{t,\tau} M_{\tau,2} = 0, \\ \vdots \\ \sum_{\tau \in J} \omega_{t,\tau} M_{\tau,n_{max}} = 0.\end{gathered}$$

The above equations hold true because, according to the description of LSSS in Section 2.3, if terms $\{\lambda_{t,\tau} = M_{t,\tau} \cdot \overrightarrow{v_t}\}$ are valid shares of secret $s_{t,1}$ over access matrix M, then the decryptor can efficiently find constants $\{\omega_{t,\tau} \in \mathbb{Z}_p\}_{\tau \in J}$ that allows the equation $\sum_{\tau \in J} \omega_{t,\tau}\lambda_{t,\tau} = s_{t,1}$ to hold. The decryptor finds such constants by finding constants that let the following equation hold: $\sum_{\tau \in J} \omega_{t,\tau} M_{t,\tau} = (1, 0, \cdots, 0)$ (so, $\sum_{\tau \in J} \omega_{t,\tau}\lambda_{t,\tau} = \sum_{\tau \in J} \omega_{t,\tau} M_{t,\tau} \cdot \overrightarrow{v_t} = (1, 0, \cdots, 0) \cdot (s_{t,1}, s_{t,2}, \cdots, s_{t,n_{max}}) =$ $s_{t,1}$).

Using the above LSSS properties, the decryption algorithm works as follows. The decryption algorithm first computes

$$\begin{aligned} CT_1 &= e(C_1, K_1)e(C_2, K_2) \cdots e(C_{k'}, K_{k'}) \\ &= \prod_{t \in [k']} e(g, v_t)^{x s_{t,1} r_t} \prod_{t \in [k']} e(g, v_t)^{x s_{t,1} p_{t,1}}. \end{aligned}$$

Then, the algorithm computes (according to the above description, $\sum\limits_{\tau\in J}\omega_{t,\tau}M_{\tau,1}=1$ and $\sum\limits_{\tau\in J}\omega_{t,\tau}M_{\tau,i}=0$ for $\tau\in\{2,3,...,n_{max}\}$)

$$\begin{aligned} CT_2 &= \prod_{t\in[k']}\prod_{i\in[n_{max}]} e(L_{t,i},\prod_{\tau\in J}C_{t,i,\tau}^{\omega_{t,\tau}}) \\ &= \prod_{t\in[k']}\prod_{i\in[n_{max}]} e(v_t^{p_{t,i}}, g^{\sum\limits_{\tau\in J}x\omega_{t,\tau}M_{\tau,i}s_{t,i}}) \times \prod_{t\in[k']}\prod_{i\in[n_{max}]} e(v_t^{p_{t,i}},\prod_{\tau\in J}h_{t,i,\rho(\tau)}^{-s_{t,1}\omega_{t,\tau}}) \\ &= \prod_{t\in[k']} e(g,v_t)^{xs_{t,1}p_{t,1}} \prod_{t\in[k']}\prod_{i\in[n_{max}]} e(v_t^{p_{t,i}},\prod_{\tau\in J}h_{t,i,\rho(\tau)}^{-s_{t,1}\omega_{t,\tau}}). \end{aligned}$$

The algorithm also computes

$$\begin{aligned} CT_3 &= \prod_{t\in[k']}\prod_{\tau\in J} e(N_{t,\rho(\tau)}^{\omega_{t,\tau}}, C_t) \\ &= \prod_{t\in[k']}\prod_{\tau\in J} e(\prod_{i\in[n_{max}]} h_{t,i,\rho(\tau)}^{p_{t,i}\omega_{t,\tau}}, v_t^{s_{t,1}}) \\ &= \prod_{t\in[k']}\prod_{i\in[n_{max}]} e(v_t^{p_{t,i}},\prod_{\tau\in J}h_{t,i,\rho(\tau)}^{s_{t,1}\omega_{t,\tau}}). \end{aligned}$$

Finally, the algorithm recovers a message m through the following computation

$$m = C_0\cdot(CT_1/(CT_2\cdot CT_3))^{-1}.$$

3.4. Proof

Our proposed scheme is constructed on the k'-BDH assumption, where parameter k' is given in the setup phase; therefore, we must reduce our scheme to the k'-BDH assumption to proof its security. We use the following theorem to prove the selective security of our scheme.

Theorem 2 *Suppose that the k'-BDH assumption holds true, then no polytime adversary $\mathcal{A}$ can selectively break our CP-ABE system.*

Proof. If an adversary $\mathcal{A}$ can selectively break our scheme with a non-negligible advantage $\xi_1 = Adv_{\mathcal{A}}$, then we show that we can build a challenger $\mathcal{B}$ that can resolve the k'-BDH assumption with a non-negligible advantage $\xi_2 = Adv_{\mathcal{B}}$.

Init. The challenger $\mathcal{B}$ first accepts the k'-BDH challenge: $\vec{z} = (g, g^x, g^y, v_1, ..., v_{k'}, v_1^{\hat{r}_1}, ..., v_{k'}^{\hat{r}_{k'}})$ and T, the challenger wants to decide if the element $T = e(g,g)^{xy(\hat{r}_1+\cdots+\hat{r}_{k'})}$ or is a random element in the group $\mathbb{G}_T$. Then the adversary $\mathcal{A}$ chooses a challenge $\ell\times n_{max}$ matrix M^* and a challenge injective function ρ^* which associates rows of M^* to attributes. $\mathcal{A}$ publishes the challenge access structure (M^*, ρ^*).

Setup. Challenger $\mathcal{B}$ chooses a random element $z_{t,i,j} \in \mathbb{Z}_p$ and sets the public parameter $h_{t,i,j} : (t \in [k'], i \in [n_{max}], j \in [U])$ as follows:

$$h_{t,i,j} = \begin{cases} v_t^{z_{t,i,j}} g^{xM^*_{d,i}} & (d \in [\ell]) \wedge (\exists \rho^*(d) = j) \\ v_t^{z_{t,i,j}} & else. \end{cases} \tag{1}$$

$\mathcal{B}$ sets parameter $h_{t,i,j}$ using the following methods: if attribute j is associated with row x in the challenge matrix M^* (note that M^* has ℓ rows, so we have $d \in [\ell]$), then $\mathcal{B}$ chooses $z_{t,i,j} \in \mathbb{Z}_p$ and sets $h_{t,i,j} = v_t^{z_{t,i,j}} g^{xM^*_{d,i}}$, else $\mathcal{B}$ only sets $h_{t,i,j} = v_t^{z_{t,i,j}}$.

Challenger $\mathcal{B}$ chooses a_t for $t \in [k']$ and sets the public key as follows:

$$g, g^x, v_t : (t \in [k']), (v_t^{\hat{r}_t})^{1/a_t} : (t \in [k']), h_{t,i,j} : (t \in [k'], i \in [n_{max}], j \in [U]).$$

According to the setting above, challenger $\mathcal{B}$ implicitly sets $r_t = \hat{r}_t / a_t$ for $t \in [k']$.

Phase 1. $\mathcal{B}$ answers private key queries from adversary $\mathcal{A}$ in this phase.

If adversary $\mathcal{A}$ queries a private key for a set S that does not satisfy the challenge access structure (M^*, ρ^*), then according to the LSSS property [28], $\mathcal{B}$ can efficiently find a vector $\vec{\omega} = (\omega_1, ..., \omega_{n_{max}})$ that satisfies $\omega_1 = -1$ and $M_i^* \cdot \vec{w} = 0$ for all i where $\rho^*(i) \in S$.

$\mathcal{B}$ chooses $\theta_{t,i} \in Z_p$ and *implicitly* sets parameter $p_{t,i}$ as

$$p_{t,i} = \theta_{t,i} + \omega_i \hat{r}_t / a_t \quad (t \in [k'], i \in [n_{max}]). \tag{2}$$

With the use of $p_{t,i}$, $\mathcal{B}$ sets parameter $L_{t,i}$ for $t \in [k']$ and $i \in [n_{max}]$ as follows:

$$L_{t,i} = v_t^{\theta_{t,i} + \omega_i \hat{r}_t / a_t} = v_t^{\theta_{t,i}} ((v_t^{\hat{r}_t})^{1/a_t})^{\omega_i}.$$

$\mathcal{B}$ knows the values of v_t and $v_t^{r_t}$, parameter $L_{t,i}$ can be computed.

According to the vector setting $\vec{\omega}$, we have $\omega_1 = -1$, so $\mathcal{B}$ can easily construct parameter K_t as

$$K_t = g^{x\hat{r}_t/a_t + x\theta_{t,1} + x\omega_1 \hat{r}_t / a_t} = g^{x\theta_{t,1}}.$$

Finally, let $d \in [\ell]$ denote a row in the challenge matrix M^*; $\mathcal{B}$ sets parameter $N_{t,\chi}$ as follows:

$$N_{t,\chi} = \begin{cases} \prod\limits_{i\in[n_{max}]} (v_t^{\hat{r}_t})^{z_{t,i,\chi} w_i/a_t} g^{x\theta_{t,i} M^*_{d,i}} v_t^{z_{t,i,\chi}\theta_{t,i}} & (\exists \rho^*(d) = \chi), \\ \prod\limits_{i\in[n_{max}]} v_t^{z_{t,i,\chi}\theta_{t,i}} (v_t^{\hat{r}_t})^{\omega_i z_{t,i,\chi}/a_t} & (\neg\exists \rho^*(d) = \chi). \end{cases} \tag{3}$$

$\mathcal{B}$ sets parameter $N_{t,\chi}$ using the following methods: if attribute χ is associated with row d in challenge matrix M^*, then according to equations (1) and (2), we have

$$N_{t,\chi} = \prod_{i\in[n_{max}]} (v_t^{\hat{r}_t})^{z_{t,i,\chi} w_i/a_t} g^{x\theta_{t,i} M^*_{d,i}} v_t^{z_{t,i,\chi}\theta_{t,i}} (g^{x\hat{r}_t})^{M^*_{d,i} w_i/a_t}. \tag{4}$$

In Equation (4), only term $g^{x\hat{r}_t}$ is unknown by challenger $\mathcal{B}$. However, according to the vector description $\vec{\omega}$, when a row d satisfies $\rho^*(d) = \chi$, then we have $\sum\limits_{i\in[n_{max}]} M^*_{d,i}\omega_i = 0$. So, term $g^{x\hat{r}_t}$ will not appear in Equation (4). Then, $\mathcal{B}$ can compute parameter $N_{t,y}$ successfully as shown in Equation (3).

In addition, when no row x associated with attribute j, then according to Equations (1) and (2), we have

$$N_{t,\chi} = \prod_{i\in[n_{max}]} (v_t^{\hat{r}_t})^{z_{t,i,\chi} w_i/a_t} v_t^{z_{t,i,\chi}\theta_{t,i}}. \tag{5}$$

In Equation (5), all terms are known by challenger $\mathcal{B}$, so $\mathcal{B}$ can construct parameter $N_{t,y}$ successfully.

Challenge. In this phase, adversary $\mathcal{A}$ outputs two messages m_0, m_1, both with the same length, and gives them to challenger $\mathcal{B}$.

$\mathcal{B}$ sets parameter $C_t : (t \in [k'])$ as

$$C_t \;\; = \;\; v_t^{s_{t,1}} = (g^y)^{a_t} : (t \in [k']).$$

Let $v_t = g^{s_t}$ for every $t \in [k']$. Then, in the above equation, $\mathcal{B}$ implicitly sets the value $s_{t,1} = a_t y/s_t$, so that we have: $C_t = v_t^{s_{t,1}} = (g^{s_t})^{a_t y/s_t} = (g^y)^{a_t}$.

$\mathcal{B}$ then creates the value of $C_{t,i,j}$. For every vector $\vec{v_t}$, $\mathcal{B}$ chooses a random vector $\vec{y_t} = (0, y_{t,2}, ..., y_{t,n_{max}})$ and *implicitly* sets vector $\vec{v_t}$ for $t \in [k']$ as follows

$$\begin{aligned}\vec{v_t} &= \underbrace{(a_t y/s_t, a_t y/s_t, ..., a_t y/s_t)}_{n_{max}} + \vec{y_t} \\ &= (a_t y/s_t, a_t y/s_t + y_{t,2}, ..., a_t y/s_t + y_{t,n_{max}}).\end{aligned}$$

Vector $\vec{v_t}$ is properly distributed because vector $\vec{y_t}$ randomizes vector $(a_t y/s_t, a_t y/s_t, ..., a_t y/s_t)$. In addition, the following equations hold true: $s_{t,i} = a_t y/s_t + y_{t,i}$ and $y_{t,1} = 0$ for every $t \in [k']$.

Using vector $\vec{v_t}$, $\mathcal{B}$ creates parameter $C_{t,i,\tau}$ as follows

$$C_{t,i,\tau} = (g^x)^{M^*_{\tau,i} y_{t,i}} (g^y)^{-z_{t,i,\tau} a_t}.$$

Every attribute τ in the challenge phase must be associated with a row ϱ_τ in the challenge matrix M^*. Thus, we have: $\rho^*(\varrho_\tau) = \tau$. Then,

$$h_{t,i,\tau} = v_t^{z_{t,i,\tau}} g^{x M^*_{\varrho_\tau,i}} : (t \in [k'], i \in [n_{max}], \rho^*(\varrho_\tau) = \tau).$$

Thus, $\mathcal{B}$ computes ciphertext $C_{t,i,\tau}$ as

$$\begin{aligned}C_{t,i,\tau} &= g^{x M^*_{\varrho_\tau,i} a_t y/s_t} g^{x M^*_{\varrho_\tau,i} y_{t,i}} \times v_t^{-z_{t,i,\tau} a_t y/s_t} g^{-x M^*_{\varrho_\tau,i} a_t y/s_t} \\ &= (g^x)^{M^*_{\varrho_\tau,i} y_{t,i}} (g^y)^{-z_{t,i,\tau} a_t}.\end{aligned}$$

$\mathcal{B}$ then flips a coin $\beta \in \{0, 1\}$ and creates the following ciphertext

$$C_0 = m_\beta \cdot T.$$

We observe that

$$\begin{aligned}\prod_{t \in [k']} e(g^x, v_t^{r_t})^{s_{t,1}} &= \prod_{t \in [k']} e(g^x, (g^{s_t})^{\hat{r}_t/a_t})^{a_t y/s_t} \\ &= e(g, g)^{xy(\hat{r}_1 + \hat{r}_2 + \cdots + \hat{r}_{k'})}.\end{aligned}$$

.

Phase 2. This phase is exactly as Same as Phase 1.

Guess. Finally, a guess β' of β will be output by Adversary $\mathcal{A}$. On the basis of the output of $\mathcal{A}$, challenger $\mathcal{B}$ outputs 0 indicating that $T = e(g, g)^{xy(r_1 + ... + r_{k'})}$ if $\beta = \beta'$; else, it outputs 1 indicating that T is a random group element in $\mathbb{G}_T$.

When $T = e(g, g)^{xy(r_1 + ... + r_{k'})}$, challenger $\mathcal{B}$ actually perfectly simulation the game with the adversary; else, if T is a random group element, the advantage for adversary successfully guess the message m_β is negligible. Therefore, the decisional k'-BDH game can be played by challenger $\mathcal{B}$ with a non-negligible advantage. □

System	Ciphertext Size	Key Size	Enc. Time	Dec. Time
Sec. 3	$\mathcal{O}(k'n^2)$	$\mathcal{O}(k'k_{max}A + k'n_{max})$	$\mathcal{O}(k'n^2)$	$\mathcal{O}(k'nT)$
[10] sec.3	$\mathcal{O}(n)$	$\mathcal{O}(A)$	$\mathcal{O}(n)$	$\mathcal{O}(T)$
[10] sec.5	$\mathcal{O}(n)$	$\mathcal{O}(k_{max}A)$	$\mathcal{O}(n)$	$\mathcal{O}(T)$
[10] sec.6	$\mathcal{O}(n^2)$	$\mathcal{O}(k_{max}A + n_{max})$	$\mathcal{O}(n^2)$	$\mathcal{O}(nT)$

Table 1: The Performance Comparisons of ABE Schemes

System	Assumption	Resist Cheon's Attack	Support Assumption Shifted?
Sec. 3	k'-BDH Assumption	Y	Y
[10] sec.3	q-Parallel DBDHE Assumption	N	N
[10] sec.5	q-DBDHE Assumption	N	N
[10] sec.6	DBDH Assumption	Y	N

Table 2: The Security of ABE Schemes

4. Discussion

We now compare the performance of our two schemes with that of Waters' three CP-ABE schemes [10]. Let n be the size of the access formula, A be the number of attributes for the user's private key, k_{max} be the maximum number of times a single attribute may appear in an access formula, n_{max} be the bound on the size of any access formula (i.e., the number of columns), and T be the minimum number of nodes satisfied by the formula. Efficiency for the ABE schemes is shown in Table 1, while security for the ABE schemes is shown in Table 2.

Our scheme is built on the k'-BDH assumption in the k-BDH assumption family, whereas Waters' three CP-ABE schemes are built on the q-Parallel DBDHE assumption (q-type DBDH assumption), the q-DBDHE assumption (q-type DBDH assumption), and the DBDH assumption.

First, we must point out that ABEs based on the q-type DBDH assumption are more efficient. We observe from Table 1 that Schemes 2 and 3 outperform all other schemes. The stronger the assumption that the scheme relies on, the more efficient the scheme. However, considering the security drawback for the q-type DBDH assumption, we construct our system on a weaker assumption (scheme 1 in Table 1), to ensure the systems absolute security.

We analyze schemes 1 and 4 in Table 1 and Table 2. When $k' = 1$, the k'-BDH assumption is equivalent to the DBDH assumption. When $k' > 1$, the k'-BDH assumption is weaker than the DBDH assumption. We observe from Table 1 that when $k' = 1$, our scheme has the same storage and time performance as Waters' scheme (scheme 4, which is constructed based on DBDH assumption). When k' increases, our scheme's performance becomes approximately k' times that of Waters' scheme. However, we can obtain an ABE system reduced to the k'-BDH assumption, which is weaker than the DBDH assumption, to achieve much stronger system security.

Using our construction, we overcome the problem that when DBDH, or an assumption stronger than DBDH, becomes unsecure, we provide a method to construct a new scheme to replace the old scheme, with the cost that we must reduce efficiency. However, when security is threatened, system security must be prioritized.

5. Conclusion

We present a new method to construct CP-ABE system on the k-BDH assumption family; where an assumption in the k-BDH assumption family becomes weaker when the values of parameter k increases. Our scheme is a variant of Waters' ABE system built on the DBDH assumption, but we create a CP-ABE system on any k'-BDH assumption in the k-BDH assumption family. If the current k'-BDH assumption becomes unsecure, we can shift our system to the l'-BDH assumption, where $l' > k'$, ensuring absolute system security.

Acknowledgement

This work was supported by the Ministry of education of Humanities and Social Science project under Grant No.15YJCZH029 and the Social science planning project of Guangzhou City under Grant No. 2016gzyb25.

Reference

[1] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. *EUROCRYPT*, 3494:457–473, 2005.

[2] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. *ACM Conference on Computer and Communications Security*, pages 89–98, 2006.

[3] Melissa Chase. Multi-authority attribute based encryption. In Salil P. Vadhan, editor, *TCC*, volume 4392 of *Lecture Notes in Computer Science*, pages 515–534. Springer, 2007.

[4] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker. Mediated ciphertext-policy attribute-based encryption and its application. *Information Security Applications*, 5932:309–323, 2009.

[5] Hua Deng, Qianhong Wu, Bo Qin, Josep Domingo-Ferrer, Lei Zhang, Jianwei Liu, and Wenchang Shi. Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. *Information Sciences*, 275:370–384, 2014.

[6] V. Goyal, A. Jain, O. Pandey, and A. Sahai. Bounded ciphertext policy attribute based encryption. *Proceedings of the ICALP*, pages 579–591, 2008.

[7] Susan Hohenberger and Brent Waters. Attribute-based encryption with fast decryption. *IACR Cryptology ePrint Archive*, 2013:265, 2013.

[8] Jung Hee Cheon. Security analysis of the strong diffie-hellman problem. In Serge Vaudenay, editor, *EUROCRYPT*, volume 4004 of *Lecture Notes in Computer Science*, pages 1–11. Springer, 2006.

[9] Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-based encryption with non-monotonic access structures. *IACR Cryptology ePrint Archive*, 2007:323, 2007.

[10] Brent Waters. Ciphertext policy attribute based encryption : An expressive, efficient, and provably secure realization. *Cryptology ePrint report*, 2008/290.

[11] Yannis Rouselakis andBrent Waters. Practical constructions and new proof methods for large universe attribute-based encryption. In *Proceedings of the 2013 ACM SIGSAC conference on Computer and communications security*, pages 463–474, 2013.

[12] Karyn Benson, Hovav Shacham, and Brent Waters. The k-bdh assumption family: Bilinear map cryptography from progressively weaker assumptions. *Topics in Cryptology C CT-RSA 2013*, 7779:310–325, 2013.

[13] Dan Boneh and Xavier Boyen. Efficient selective-id secure identity-based encryption without random oracles. In *Proceedings of Eurocrypt 2004*, volume 3027, pages 223–238, 2004.

[14] Clifford Cocks. An identity based encryption scheme based on quadratic residues. *IMA Int.Conf.*, 7:360–363, 2001.

[15] Adi Shamir. Identity-based cryptosystems and signature schemes. *Advances in Cryptology: Proceedings of CRYPTO 84*, 7:47–53, 1984.

[16] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. *CRYPTO*, 2139:213–229, 2001.

[17] Nuttapong Attrapadung, Benoit Libert, and Elie de Panafieu. Expressive key-policy attribute based encryption with constant-size ciphertexts. *Public Key Cryptography*, 6571:90–108, 2011.

[18] Yannis Rouselakis and Brent Waters. New constructions and proof methods for large universe attribute-based encryption. *IACR Cryptology ePrint Archive*, 2012:583, 2012.

[19] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. *IEEE Symposium on Security and Privacy*, pages 321–334, 2007.

[20] Zhibin Zhou, Dijiang Huang, and Zhijie Wang. Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption. *IEEE Transactions on Computers*, 64(1):126–138, January 2015.

[21] Xavier Boyen. Attribute-based functional encryption on lattices. In *TCC*, pages 122–142, 2013.

[22] Guoyan Zhang, Jing Qin, and Shams Qazi. Multi-authority attribute-based encryption scheme from lattices. *J. UCS*, 21(3):483–5001, 2015.

[23] Katsuyuki Takashima. New proof techniques for DLIN-based adaptively secure attribute-based encryption and their application. *IACR Cryptology ePrint Archive*, 2015:1021, 2015.

[24] Yogachandran Rahulamathavan. User collusion avoidance scheme for privacy-preserving decentralized key-policy attribute-based encryption – full version, February 03 2016.

[25] Jason Crampton and Alexandre Pinto. Attribute-based encryption for access control using elementary operations. In *CSF*, pages 125–139. IEEE, 2014.

[26] Federico Giacon, Riccardo Aragona, and Massimiliano Sala. A proof of security for a key-policy RS-ABE scheme, March 21 2016.

[27] Xingbing Fu. Unidirectional proxy re-encryption for access structure transformation in attribute-based encryption schemes. *I. J. Network Security*, 17(2):142–149, 2015.

[28] Amos Beimel. *Secure Schemes for Secret Sharing and Key Distribution.* PhD thesis, Technion, Haifa, Israel, 1996.