Conjunctive Broadcast and Attribute-Based Encryption

Nuttapong Attrapadung and Hideki Imai

Research Center for Information Security (RCIS),
National Institute of Advanced Industrial Science and Technology (AIST)
Akihabara-Daibiru Room 1003, 1-18-13, Sotokanda,
Chiyoda-ku, Tokyo 101-0021, Japan
{n.attrapadung,h-imai}@aist.go.jp

Abstract. Attribute-based encryption (ABE) system enables an access control mechanism over encrypted data by specifying access policies among private keys and ciphertexts. There are two flavors of ABE, namely key-policy and ciphertext-policy, depending on which of private keys or ciphertexts that access policies are associated with. In this paper we propose a new cryptosystem called *Broadcast ABE* for both flavors. Broadcast ABE can be used to construct ABE systems with *direct* revocation mechanism. Direct revocation has a useful property that revocation can be done without affecting any non-revoked users; in particular, it does not require users to update keys periodically. For key-policy variant, our systems appear to be the first fully-functional directly revocable schemes. For ciphertext-policy variant, our systems improve the efficiency from the previously best revocable schemes; in particular, one of our schemes admits ciphertext and private key sizes roughly the same as the currently best (non-revocable) ciphertext-policy ABE. Broadcast ABE can also be utilized to construct multi-authority ABE in the disjunctive setting.

Keywords: Attribute-based encryption, Ciphertext policy, Key policy, Broadcast encryption, Revocable ABE, Disjunctive multi-authority ABE.

1 Introduction

Background. Attribute-based encryption (ABE) enables an access control mechanism over encrypted data using access policies and ascribed attributes among private keys and ciphertexts. ABE comes in two flavors called Ciphertext-Policy ABE and Key-Policy ABE.

In Ciphertext-Policy ABE, an encryptor can express any access policy, stating what kind of receivers will be able to decrypt the message, directly in the encryption algorithm (which can be run by anyone knowing the universal public key issued priorly by an authority). Such a policy is specified in terms of access structure over attributes. A user is ascribed by an attribute set, in the sense that each attribute corresponds to one of her credential, and

H. Shacham and B. Waters (Eds.): Pairing 2009, LNCS 5671, pp. 248–265, 2009.

is priorly given the private key from the authority. Such a user can decrypt a ciphertext if her attribute satisfies the access policy associated to the ciphertext. An example application of CP-ABE is secure mailing list system with access policy. There, a private key will be assigned for an attribute set, such as {"MANAGER", "AGE:30", "INSTITUTE:ABC"}, while policies over attributes such as "MANAGER" $\vee$ ("TRAINEE" $\wedge$ "AGE:25") will be associated to ciphertexts.

In Key-Policy ABE, the roles of an attribute set and an access policy are swapped from what we described for CP-ABE. Attribute sets are used to annotate the ciphertexts and access policies over these attributes are associated to users' secret keys. An example application of KP-ABE is pay-TV system with package policy (called target broadcast system in [16]). There, a ciphertext will associate with an attribute set, such as ω = {"TITLE:24", "GENRE:SUSPENSE", "SEASON:2", "EPISODE:13" }, while a policy such as $\mathbb{A}$ = "SOCCER" $\vee$("TITLE:24" $\wedge$ "SEASON:5") will be associated to TV program package keys that user receives when subscribes.

Previous Works. ABE was introduced by Sahai and Waters [21] in the context of a generalization of ID-based encryption (IBE) called Fuzzy IBE, which is an ABE that allows only single threshold access structures. The first (and still being state-of-the-art) KP-ABE that allow any monotone access structures was proposed by Goyal et al. [16], while the first such CP-ABE, albeit with the security proof in the generic bilinear group model, was proposed by Bethencourt, Sahai, and Waters [5]. Ostrovsky, Sahai, and Waters [20] then subsequently extended both schemes to handle also any non-monotone structures; therefore, negated clauses can be specified in policies. Goyal et al. [15] presented bounded CP-ABE in the standard model. Waters [23] recently proposed the first fully expressive CP-ABE in the standard model. Chase [10] presented KP-ABE in multi-authority setting.

1.1 Two Motivating Problems

Motivation 1: Revocation Scheme for ABE. Revocation mechanism is necessary for any encryption schemes that involve many users, since some private keys might get compromised at some point. In simpler primitives such as public key infrastructure and IBE, there are many revocation methods proposed in the literature [17,1,18,7,13,6]. In attribute-based setting, Boldyreva et al. [6] only recently proposed a revocable KP-ABE scheme. Their scheme uses a key update approach roughly as follows. Consider the package pay-TV system example as above. The sender will encrypt to the attribute set $\omega \cup$ {"TIME:2009.WEEK3"}, where it also includes the present time slot attribute. The key authority periodically announces a key update material at each time slot so that only non-revoked users can update their key, *e.g.,* a user with a key for policy $\mathbb{A}$ can compute a key for $\mathbb{A} \wedge$ "TIME:2009.WEEK3", which can be used to decrypt ciphertexts encrypted at this time slot. We call this approach an *indirect* revocation, since the authority indirectly enables revocation by forcing revoked users to be unable to update their keys.

While the indirect revocation has an elegant property that senders do not need to know the revocation list, it also has a disadvantage that the key update phase can be a bottleneck for both the key authority and *all* non-revoked users. It is thus left as an open problem to find an efficient revocation mechanism which can be done *without affecting any non-revoked users and public key.* With this restriction, it must be that the sender obtains the revocation list (and somehow will embed it into the ciphertext), since otherwise revocation cannot take effect after all. This setting (where sender knows the revocation list) is reasonable especially in the package pay-TV system example, where the sender is the program distributor company, who should possess the pirate key list to be revoked. We will call such solution where a sender directly specifies the revocation list when encrypting a *direct* revocation.

For KP-ABE, a direct revocation approach is, however, not possible yet for the normal present form of KP-ABE algorithm since a normal KP-ABE scheme allows only specifying *attribute set* associated to the ciphertext, not *access policy.* This motivates us to model and construct such a scheme in this paper. We note that Gollé et al. [14] proposed a directly revocable KP-ABE but their scheme is heuristic and works only when the number of attributes associated to each ciphertext is exactly half of the universe size.

On the other hand, for CP-ABE, such direct revocation can be done by using ABE that supports *negative* clauses, proposed by Ostrovsky, Sahai, Waters [20]. To do so, one just adds conjunctively the AND of negation of revoked user identities (where each is considered as an attribute here). However, this solution still somewhat lacks efficiency performance. In particular, their CP-ABE scheme[1] will pose overhead $O(|R|)$ group elements additively to the size of ciphertext and $O(\log n)$ multiplicatively to the size of private key over the original CP-ABE scheme of Bethencourt et al. [5], where n is the maximum size of revoked attributes set R. This motivates us to look for more efficient revocation schemes for CP-ABE. We note that Sahai and Waters [22] recently proposed ABE that support negative clauses which has efficiency improvement over the Ostrovsky et al. scheme [20]. However, their paper included only a KP-ABE variant.

Motivation 2: Disjunctive Multi-Authority ABE. One limitation in ABE systems is the need to trust single central authority. A natural extension of ABE to avoid this is to have many authorities where each can derive a private key. Consider the policy-based secure mailing list example described in the usage of CP-ABE above. Suppose that the sender wishes to send an email encrypted under some policy and she only trusts authorities say $A_1, \ldots, A_t$. She wishes to encrypt the email so that only user who possesses a key such that its attribute set satisfies the policy and it is generated from one of those t trusted authority can decrypt. Using a trivial approach would require ciphertext of size $O(t \cdot c)$ where c is the ciphertext size in the basic ABE. Our goal is to obtain more efficient scheme that requires ciphertext of size only $O(c)$, which is independent of t.

A similar problem to this was indeed recently addressed by Boneh and Hamburg [9]. In their paper, they proposed a framework called Generalized IBE

[1] The mentioned scheme was implicitly introduced in §3.5 of [20].

(GIBE) and gives a concrete construction of its special case called Spatial Encryption. One property of their framework is that any primitive that is casted as GIBE can be efficiently augmented to its disjunctive multi-authority version. In their paper, they showed that KP-ABE also falls into the GIBE framework. However, the key size of the KP-ABE instantiated from Spatial Encryption is linear to the access structure size, which may be exponentially large.

We note that Chase [10] also proposed Multi-Authority ABE, albeit in the *conjunctive* setting. In conjunctive setting, the attribute space for each authority is disjoint, while in our disjunctive setting, the attribute space is the same for all authorities. Also, in conjunctive setting, a private key will be created by gathering elements from all authorities, while in our disjunctive setting, a private key can be derived solely by each authority.

1.2 Our Contributions

We propose a new primitive called *Conjunctive Broadcast and Attributed Based Encryption*, or simply *Broadcast ABE* for shorthand. Roughly speaking, it adds conjunctively a broadcast dimension *á la* Broadcast Encryption (BE) to ABE. Broadcast ABE efficiently solves both motivated problems: it can be used as an ABE system that has a direct revocation mechanism and a disjunctive multi-authority ABE. We refer to [12,19,18,11,2,8,22] for historic details on BE.

In Broadcast ABE, a private key will be associated also with a user index ID and the ciphertext will be associated also with a user index set S, besides a set of attributes and an access structure (respectively if CP-ABE is considered, or vice versa if KP-ABE is considered). The decryption can be done if the condition on attributes on the ABE part holds as usual *and*, in addition, $\mathsf{ID} \in S$. Broadcast ABE also realizes private key delegation in proper ways.

To realize a directly revocable ABE scheme, we set ID to be used as a unique serial number for each private key. To encrypt with a revoked serial number set R the sender just sets $S = \mathcal{U} \setminus R$, where $\mathcal{U}$ is the universe of user indexes, while the attribute related part is done as usual.

To realize a disjunctive multi-authority ABE scheme, we set ID to be used as each authority's identity. To derive a private key for a user, an authority delegates its key by specifying the attribute part properly.

Our Approach. We propose two concrete Broadcast Key-Policy ABE schemes and two concrete Broadcast Ciphertext-Policy ABE schemes. Each Broadcast Key-Policy ABE scheme is based on state-of-the-art Broadcast Encryption scheme either by Boneh-Gentry-Waters [8] or Sahai-Waters [22] combined algebraically with Goyal et al. KP-ABE [16]. Similarly, each Broadcast Ciphertext-Policy ABE scheme is based on Broadcast Encryption scheme either by Boneh-Gentry-Waters or Sahai-Waters combined algebraically with Waters' CP-ABE [23].

Each of four combinations is non-trivial at the first place, since, for example, one may think of obtaining Broadcast ABE by using AND-double encryption (even in a secure way) of BE and ABE. However, one can easily find out that this mislead method is insecure due to collusion attacks of two attackers. Our schemes algebraically combine those schemes in a more sophisticated way.

Efficiency. Our first broadcast KP-ABE scheme has almost the same efficiency in ciphertext and private key sizes to that of original KP-ABE of Goyal et al.[16], albeit it has a large pubic key size linear to n, where n is the size of user index universe. Our second broadcast KP-ABE scheme reduces the public key size to almost the same of the original KP-ABE while the ciphertext requires only $2|R|$ group elements additively. Note that these are the first fully functional directly revocable KP-ABE schemes in the literature. The performance also holds similarly for broadcast CP-ABE variant. In particular, our revocable CP-ABE schemes outperform the previous method applied from [20].

Organization of the Paper. We first provide preliminary materials in §2. We present the definition of Broadcast ABE in §3. In §4 and §5, we present our four concrete broadcast ABE schemes for Key-policy and Ciphertext-policy variant respectively. We give a brief security proof overview in §6 and postpone the full proofs to the full version. The key delegation algorithms for each scheme are described in §7. Finally, in §8, we present efficiency performance comparison.

2 Preliminaries

2.1 Access Structures and Linear Secret Sharing

We first provide the notion of access structure and linear secret sharing scheme as follows. Such formalization is recapped from [23].

Definition 1 (Access Structures). *Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^{\mathcal{P}}$ is monotone if for all B, C we have that if $B \in \mathbb{A}$ and $B \subseteq C$ then $C \in \mathbb{A}$. An access structure (respectively, monotonic access structure) is a collection (respectively, monotone collection) $\mathbb{A} \subseteq 2^{\mathcal{P}} \setminus \{\emptyset\}$. The sets in $\mathbb{A}$ are called the authorized sets, and the sets not in $\mathbb{A}$ are called the unauthorized sets.*

Definition 2 (Linear Secret Sharing Schemes (LSSS)). *Let $\mathcal{P}$ be a set of parties. Let M be a matrix of size $\ell \times k$. Let $\rho : \{1, \ldots, \ell\} \to \mathcal{P}$ be 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 $\mathcal{P}$ is a linear secret-sharing scheme in $\mathbb{Z}_p$ and is represented by (M, ρ) if it consists of two polynomial-time algorithms:*

$\mathsf{Share}_{(M,\rho)}$: *The algorithm takes as input $s \in \mathbb{Z}_p$ which is to be shared. It randomly chooses $y_2, \ldots, y_k \in \mathbb{Z}_p$ and let $\boldsymbol{v} = (s, y_2, \ldots, y_k)$. It outputs $M\boldsymbol{v}$ as the vector of ℓ shares. The share $\lambda_{\rho(i)} := \boldsymbol{M_i} \cdot \boldsymbol{v}$ belongs to party $\rho(i)$, where we denote $\boldsymbol{M_i}$ as the ith row in M.*

$\mathsf{Recon}_{(M,\rho)}$: *The algorithm takes as input $S \in \mathbb{A}$. Let $I = \{i|\ \rho(i) \in S\}$. It outputs reconstruction constants $\{(i, \mu_i)\}_{i \in I}$ which has a linear reconstruction property: $\sum_{i \in I} \mu_i \cdot \lambda_{\rho(i)} = s$.*

2.2 Bilinear Maps and Some Assumptions

Bilinear Maps. We briefly review facts about bilinear maps. Let $\mathbb{G}, \mathbb{G}_T$ be multiplicative groups of prime order p. Let g be a generator of $\mathbb{G}$. A bilinear map is a map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ for which the following hold: (1) e is bilinear; that is, for all $u, v \in \mathbb{G}$, $a, b \in \mathbb{Z}$, we have $e(u^a, v^b) = e(u, v)^{ab}$. (2) The map is non-degenerate: $e(g, g) \neq 1$. We say that $\mathbb{G}$ is a bilinear group if the group action in $\mathbb{G}$ can be computed efficiently and there exists $\mathbb{G}_T$ for which the bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is efficiently computable.

Decision BDHE Assumption. Let $\mathbb{G}$ be a bilinear group of prime order p. The Decision q-BDHE (Bilinear Diffie-Hellman Exponent) problem [8] in $\mathbb{G}$ is stated as follows: first the challenger picks a generator $g \in \mathbb{G}$ and random exponent s, α. The attacker is given a vector

$$\boldsymbol{Y} = \Big(g, g^s, g^\alpha, g^{(\alpha^2)}, \ldots, g^{(\alpha^q)}, g^{(\alpha^{q+2})}, \ldots, g^{(\alpha^{2q})}\Big)$$

and an element $Z \in \mathbb{G}_T$ as input, determine if $Z = e(g, g)^{\alpha^{q+1}s}$. We denote $g_i = g^{(\alpha^i)} \in \mathbb{G}$ for shorthand. An algorithm $\mathcal{A}$ that outputs $b \in \{0, 1\}$ has advantage ϵ in solving Decision q-BDHE in $\mathbb{G}$ if $|\Pr\big[\mathcal{A}\big(\boldsymbol{Y}, e(g, g)^{\alpha^{q+1}s}\big) = 0\big] - \Pr\big[\mathcal{A}\big(\boldsymbol{Y}, Z\big) = 0\big]| \geq \epsilon$. We refer to the distribution on the left as $\mathcal{P}_{BDHE}$ and the distribution on the right as $\mathcal{R}_{BDHE}$. We say that the Decision q-BDHE assumption holds in $\mathbb{G}$ if no polynomial-time algorithm has a non-negligible advantage in solving the problem.

Decision MEBDH Assumption. Let $\mathbb{G}$ be a bilinear group of prime order p. The Decision q-MEBDH (Multi-Exponent Bilinear Diffie-Hellman) problem [22] in $\mathbb{G}$ is stated as follows: first the challenger picks a generator $g \in \mathbb{G}$ and random exponent $s, \alpha, a_1, \ldots, a_r$. The attacker is given a vector $\boldsymbol{X} =$

$$\begin{array}{rr} & g,\ g^s,\ e(g,g)^\alpha \\ \forall_{1 \leq i,j \leq q} & g^{a_i},\ g^{a_i s},\ a^{a_i a_j},\ g^{\alpha/a_i^2} \\ \forall_{1 \leq i,j,k \leq q, i \neq j} & g^{a_i a_j s},\ g^{\alpha a_j/a_i^2},\ g^{\alpha a_i a_j/a_k^2},\ g^{\alpha a_i^2/a_j^2} \end{array}$$

and an element $Z \in \mathbb{G}_T$ as input, determine if $Z = e(g, g)^{\alpha s}$. An algorithm $\mathcal{A}$ that outputs $b \in \{0, 1\}$ has advantage ϵ in solving Decision q-MEBDH in $\mathbb{G}$ if $|\Pr\big[\mathcal{A}(\boldsymbol{X}, e(g, g)^{\alpha s}) = 0\big] - \Pr\big[\mathcal{A}(\boldsymbol{X}, Z) = 0\big]| \geq \epsilon$. We refer to the distribution on the left as $\mathcal{P}_{MEBDH}$ and the distribution on the right as $\mathcal{R}_{MEBDH}$. We say that the Decision q-MEBDH assumption holds in $\mathbb{G}$ if no polynomial-time algorithm has a non-negligible advantage in solving the problem.

3 Definitions and Applications

3.1 Broadcast Key-Policy ABE

Let $\mathcal{U}$ denote the set of all user indexes. Let $\mathcal{N}$ be the set of all attributes. Note that both $\mathcal{U}$ and $\mathcal{N}$ are possibly of exponential sizes. Let $\mathcal{A}$ denote the set of access structures over $\mathcal{N}$ which are allowed to be used. A $(\mathcal{U}, \mathcal{A})$ Broadcast Key-Policy Attribute-Based Encryption (BKP-ABE) scheme consists of four default algorithms $\mathsf{Setup}, \mathsf{Encrypt}, \mathsf{KeyGen}, \mathsf{Decrypt}$ and may also include one optional additional algorithm $\mathsf{Delegate}$.

$\mathsf{Setup} \rightarrow (\mathsf{pk}, \mathsf{msk})$**.** This is a randomized algorithm that takes no input other than the implicit security parameter. It outputs the public key pk and a master key msk.

$\mathsf{Encrypt}(S, \omega, \mathcal{M}, \mathsf{pk}) \rightarrow \mathsf{ct}$**.** This is a randomized algorithm that takes as input a user index set $S \subseteq \mathcal{U}$, a set of attributes $\omega \subseteq \mathcal{N}$, a message $\mathcal{M}$, and the public key pk. It outputs a ciphertext ct.

$\mathsf{KeyGen}(\mathsf{ID}, \mathbb{A}, \mathsf{msk}, \mathsf{pk}) \rightarrow \mathsf{sk}_{(\mathsf{ID},\mathbb{A})}$**.** This is a randomized algorithm that takes as input a user index $\mathsf{ID} \in \mathcal{U}$, an access structure $\mathbb{A} \in \mathcal{A}$, the master key msk, and the public key pk. It outputs a private decryption key $\mathsf{sk}_{(\mathsf{ID},\mathbb{A})}$, which we sometimes simply denote as sk when its subscript is unambiguous.

$\mathsf{Decrypt}(\mathsf{ct}, (S, \omega), \mathsf{sk}_{(\mathsf{ID},\mathbb{A})}, (\mathsf{ID}, \mathbb{A}), \mathsf{pk}) \rightarrow \mathcal{M}$**.** This algorithm takes as input the ciphertext ct that was encrypted under a user set S with a set ω of attributes, the decryption key $\mathsf{sk}_{(\mathsf{ID},\mathbb{A})}$ for user index ID with access control structure $\mathbb{A}$, and the public key pk. It outputs the message $\mathcal{M}$ if $\omega \in \mathbb{A}$ *and* $\mathsf{ID} \in S$.

$\mathsf{Delegate}\big((\mathsf{x}, \mathsf{y}), \mathsf{sk}_{(\mathsf{x},\mathsf{y})}, (\mathsf{x}', \mathsf{y}'), \mathsf{pk}\big) \rightarrow \mathsf{sk}_{(\mathsf{x}',\mathsf{y}')}$**.** This is a randomized algorithm that takes as input a secret key $\mathsf{sk}_{(\mathsf{x},\mathsf{y})}$ (with its subscript) and a new subscript $(\mathsf{x}', \mathsf{y}')$. It outputs a key $\mathsf{sk}_{(\mathsf{x}',\mathsf{y}')}$. Let $\top$ be a special symbol. If we write this operation as $\mathsf{sk}_{(\mathsf{x},\mathsf{y})} \rightarrow \mathsf{sk}_{(\mathsf{x}',\mathsf{y}')}$ and denote $\mathsf{msk} = \mathsf{sk}_{(\top,\top)}$, then this algorithm is defined over the sequences

$$\mathsf{sk}_{(\top,\top)} \rightarrow \mathsf{sk}_{(\mathsf{ID},\top)} \rightarrow \mathsf{sk}_{(\mathsf{ID},\mathbb{A})}, \quad \mathsf{sk}_{(\top,\top)} \rightarrow \mathsf{sk}_{(\top,\mathbb{A})} \rightarrow \mathsf{sk}_{(\mathsf{ID},\mathbb{A})}, \quad \mathsf{sk}_{(\mathsf{x},\mathbb{A})} \rightarrow \mathsf{sk}_{(\mathsf{x},\mathbb{A}')},$$

for any $\mathsf{ID} \in \mathcal{U}$; $\mathbb{A}, \mathbb{A}' \in \mathcal{A}$ where $\mathbb{A} \subseteq \mathbb{A}'$ and x can be either $\top$ or any $\mathsf{ID} \in \mathcal{U}$.

We require the standard correctness of decryption, that is, if $\mathsf{Setup} \rightarrow (\mathsf{pk}, \mathsf{msk})$ then $\mathsf{Decrypt}\Big(\mathsf{Encrypt}(S, \omega, \mathcal{M}, \mathsf{pk}), (S, \omega), \mathsf{KeyGen}(\mathsf{ID}, \mathbb{A}, \mathsf{msk}, \mathsf{pk}), (\mathsf{ID}, \mathbb{A}), \mathsf{pk}\Big) \rightarrow \mathcal{M}$ for all $\mathcal{M}$ in message space; $\mathsf{ID} \in \mathcal{U}$; $\mathbb{A} \in \mathcal{A}$; $\omega \in \mathcal{N}$; $S \subseteq \mathcal{U}$. For the scheme with $\mathsf{Delegate}$ defined, we also require that $\mathsf{sk}_{(\mathsf{ID},\mathbb{A})}$ output from this algorithm has the same distribution as the one from KeyGen algorithm.

The selective security notion for BKP-ABE is defined in the following game.

Init. The adversary declares the target set of user indexes $S^\star$ and the target attribute set $\omega^\star$.

Setup. The challenger runs the Setup algorithm of ABE and gives the public key pk to the adversary.

Phase 1. The adversary is allowed to issue queries for private keys for pairs of user index and access structure $(\mathsf{ID}, \mathbb{A})$ such that $\omega^\star \notin \mathbb{A}$ *or* $\mathsf{ID} \notin S^\star$, *i.e.,* the negated condition of that of a legitimate key which can be used to decrypt a challenge ciphertext.

For the scheme with $\mathsf{Delegate}$ defined, the adversary can also query the key for $\mathsf{sk}_{(\mathsf{ID},\top)}$ such that $\mathsf{ID} \notin S^\star$, and the key for $\mathsf{sk}_{(\top,\mathbb{A})}$ such that $\omega^\star \notin \mathbb{A}$.

Challenge. The adversary submits two equal length messages $\mathcal{M}_0$ and $\mathcal{M}_1$. The challenger flips a random bit b and computes the challenge ciphertext $\mathsf{ct}^\star$ of $\mathcal{M}_b$ on the target pair $(\mathbb{S}^\star, \omega^\star)$ of user set and target attribute set and then gives $\mathsf{ct}^\star$ to the adversary.

Phase 2. Phase 1 is repeated.

Guess. The adversary outputs a guess b' of b.
The advantage of an adversary in this game is defined as $\Pr[b = b'] - \frac{1}{2}$. Note that this can be extended to handle chosen-ciphertext attacks by allowing decryption queries in Phase 1,2.

Definition 3. *A BKP-ABE scheme is secure in the selective security notion if all polynomial time adversaries have at most a negligible advantage in the above game.*

3.2 Broadcast Ciphertext-Policy ABE

Let $\mathcal{U}, \mathcal{N}, \mathcal{A}$ denote the same values as before. A $(\mathcal{U}, \mathcal{A})$ Broadcast Ciphertext-Policy Attribute-Based Encryption (BCP-ABE) scheme is defined in exactly the same way as BKP-ABE except only that the role of the access structure and the set of attribute is swapped. That is, the private key is assigned to a pair of user index $\mathsf{ID} \in \mathcal{U}$ and attribute set $\psi \subseteq \mathcal{N}$, and the ciphertext corresponds to a pair of user set $S \subseteq \mathcal{U}$ and access structure $\mathbb{A} \in \mathcal{A}$. The decryption can be done iff $\psi \in \mathbb{A}$ *and* $\mathsf{ID} \in S$. The definition of security notion can be adapted from the key-policy case straightforwardly.

3.3 Solutions to Motivating Problems

Directly Revocable ABE. We apply broadcast ABE for realizing a direct revocation on ABE as follows. We use ID as a unique serial number for each private key (*e.g.,* ID can be the number of keys distributed so far). That is, when a user request a key for y for appropriate y depending on KP-ABE or CP-ABE, the authority picks an unused ID, and returns $\mathsf{sk}_{(\mathsf{ID},\mathsf{y})}$. When encrypting, a sender associates the set $S = \mathcal{U} \setminus R$, where R is the revoked serial number set, together with the usual attribute-based part. In particular, whether users in S can decrypt or not is a *don't care* condition, which is left to be evaluated solely from the attribute-based part. The only *care* condition is that users in R cannot decrypt.

Disjunctive Multi-authority ABE. We apply Broadcast ABE for realizing disjunctive multi-authority ABE as follows. We use broadcast ABE in which the key $\mathsf{sk}_{(\mathsf{ID},\top)}$ is defined (and its corresponding $\mathsf{Delegate}$). $\mathsf{sk}_{(\mathsf{ID},\top)}$ will be the key for the authority of identity ID. To generate key for a user, an authority delegates key $\mathsf{sk}_{(\mathsf{ID},\mathsf{y})}$ for appropriate y depending on KP-ABE or CP-ABE. To encrypt under a set of trusted authority S, the sender encrypt under user index set S and appropriate attribute set or access structure depending on KP-ABE or CP-ABE.

4 Broadcast Key-Policy ABE

We now present our two broadcast key-policy ABE schemes. The first scheme $\mathsf{BKP\text{-}ABE1}$ is a combination of broadcast encryption of Boneh-Gentry-Waters [8] and KP-ABE of Goyal et al. [16]. The second scheme $\mathsf{BKP\text{-}ABE2}$ is a combination of broadcast encryption of Sahai-Waters [22] and KP-ABE of Goyal et al. [16].

The first scheme $\mathsf{BKP\text{-}ABE1}$ has user index universe $\mathcal{U} = [n] = \{1, \dots, n\}$. $\mathsf{BKP\text{-}ABE2}$ has user index universe $\mathcal{U} = \mathbb{Z}_p$. We note that the universe being $\mathcal{U} = \mathbb{Z}_p$ implies that one can think of the primitive as an identity-based version in the broadcast dimension, where we can hash any string in $\{0,1\}^*$ into $\mathbb{Z}_p$ in the real usage. ID-based version implicitly implies the dynamic aspect of our scheme since a key for every user ($\in \{0,1\}^*$) will be well-defined from initialization.

Both schemes have attribute universe $\mathcal{N} = \mathbb{Z}_p$ and can deal with any linear secret-sharing access structure which we denote its universe as $\mathcal{A}_{\mathsf{LSSS}}$. Consequently, we let an access structure in its LSSS matrix form (*cf.* Definition 2) be input directly to the algorithms in the scheme.

In each scheme, let m be the maximum size of objective attribute set allowed to be associated with a ciphertext, *i.e.,* we restrict $|\omega| \leq m$. Let $m' = m - 1$.

The intuition behind each combination that recurs throughout this paper is that we combine the "core key" of both underlying schemes algebraically into single element so as to prevent collusion attacks. (Recall that such attack could be mounted in the case of simple combination by AND-double encryption in the mislead method described in §1). We will describe the intuition for only the first scheme. For the readers who are familiar with Boneh-Gentry-Waters BE [8], we recall that $g^{\alpha^{\mathsf{ID}}\gamma}$ is the private key element of user ID. To combine this key seamlessly to the core part of the KP-ABE scheme, we use the secret exponent $\alpha^{\mathsf{ID}}\gamma$ as the secret to be shared in the LSSS of the Goyal et al. [16] KP-ABE. We note that this technique is somewhat reminiscent of the scheme in [4].

4.1 Construction BKP-ABE1

▶ Setup: The algorithm first picks a random generator $g \in \mathbb{G}$ and a random $\alpha \in \mathbb{Z}_p$. It computes $g_i = g^{(\alpha^i)} \in \mathbb{G}$ for $i = 1, 2, \dots, n, n{+}2, \dots, 2n$. Next, it randomly picks $\gamma \in \mathbb{Z}_p$ and sets $v = g^\gamma \in \mathbb{G}$. It then randomly picks $h_0, \dots, h_{m'} \in \mathbb{G}$. The public key is $\mathsf{pk} = \big(g, g_1, \dots, g_n, g_{n+2}, \dots, g_{2n}, v, h_0, \dots, h_{m'}\big)$. The master key is $\mathsf{msk} = (\alpha, \gamma)$. It outputs $(\mathsf{pk}, \mathsf{msk})$. Define a function $F : \mathbb{Z}_p \to \mathbb{G}$ by $F(x) = \prod_{j=0}^{m'} h_j^{(x^j)}$.

▶ $\mathsf{Encrypt}(S, \omega, \mathcal{M}, \mathsf{pk})$: Inputs to the encryption algorithm are a user index set $S \subseteq \mathcal{U}$ and an attribute set $\omega \subseteq \mathcal{N}$. Pick a random $s \in \mathbb{Z}_p$. It then computes the ciphertext as $\mathsf{ct} = \big(C, C^{(1)}, \{C_k^{(2)}\}_{k\in\omega}, C^{(3)}\big)$ where

$$C = \mathcal{M} \cdot e(g_n, g_1)^s, \quad C^{(1)} = g^s, \quad C_k^{(2)} = F(k)^s, \quad C^{(3)} = (v \prod_{j\in S} g_{n+1-j})^s.$$

▶ $\mathsf{KeyGen}(\mathsf{ID}, (N, \pi), \mathsf{msk}, \mathsf{pk})$: Inputs to the encryption algorithm are a user index $\mathsf{ID} \in \mathcal{U}$ and a LSSS access structure $(N, \pi) \in \mathcal{A}_{\mathsf{LSSS}}$. Let N be $\ell_{\mathsf{o}} \times k_{\mathsf{o}}$

matrix. The algorithm first randomly chooses $z_2 \dots, z_{k_o} \in \mathbb{Z}_p$ and lets $\boldsymbol{v} = (\alpha^{\mathsf{ID}}\gamma, z_2, \dots, z_{k_o})$. For $i = 1$ to ℓ_o, it calculates $\sigma_i = \boldsymbol{N_i} \cdot \boldsymbol{v}$, where $\boldsymbol{N_i}$ is the vector corresponding to ith row of N. It also randomly chooses $r_1, \dots, r_{\ell_o} \in \mathbb{Z}_p$. It outputs the private key as $\mathsf{sk}_{(\mathsf{ID},(N,\pi))} = \big(\{D_i^{(1)}\}_{i\in[1,\ell_o]}, \{D_i^{(2)}\}_{i\in[1,\ell_o]}\big)$ where

$$D_i^{(1)} = g^{\sigma_i} F(\pi(i))^{r_i}, \qquad D_i^{(2)} = g^{r_i}. \tag{1}$$

▶ $\mathsf{Decrypt}(\mathsf{ct}, (S, \omega), \mathsf{sk}_{(\mathsf{ID},(N,\pi))}, (\mathsf{ID}, (N, \pi)), \mathsf{pk})$: Suppose that the attribute set ω satisfies the access structure (N, π) and the user index $\mathsf{ID} \in S$ (so that the decryption is possible). Let $I_o = \{i |\ \pi(i) \in \omega\}$. It then calculates corresponding sets of reconstruction constants $\{(i, \nu_i)\}_{i\in I_o} = \mathsf{Recon}_{(N,\pi)}(\omega)$. Then it computes the following

$$K = \frac{e(g_{\mathsf{ID}}, C^{(3)})}{e(\prod\limits_{\substack{j\in S\\ j\neq \mathsf{ID}}} g_{n+1-j+\mathsf{ID}}, C^{(1)})} \prod_{i=1}^{\ell_o} \left(\frac{e(C^{(2)}_{\pi(i)}, D_i^{(2)})}{e(D_i^{(1)}, C^{(1)})} \right)^{\nu_i},$$

and obtains message $\mathcal{M} = C/K$.

Correctness. We can verify its correctness as

$$\begin{aligned} K &= \frac{e(g_{\mathsf{ID}}, (v \prod_{j\in S} g_{n+1-j})^s)}{e(\prod\limits_{\substack{j\in S\\ j\neq \mathsf{ID}}} g_{n+1-j+\mathsf{ID}}, g^s)} \cdot \prod_{i=1}^{\ell_o} \left(\frac{e(F(\pi(i))^s, g^{r_i})}{e(g^{\sigma_i} F(\pi(i))^{r_i}, g^s)} \right)^{\nu_i} \\ &= \frac{e(g^{(\alpha^{\mathsf{ID}})}, (g^{\gamma} \prod_{j\in S} g_{n+1-j})^s)}{e(\prod\limits_{\substack{j\in S\\ j\neq \mathsf{ID}}} g_{n+1-j+\mathsf{ID}}, g^s)} \cdot \frac{1}{\prod_{i=1}^{\ell_o} e(g, g)^{s\cdot\sigma_i\cdot\nu_i}} \\ &= \frac{e(g, g)^{(\alpha^{\mathsf{ID}}\gamma s)} e(g, \prod_{j\in S} g_{n+1-j+\mathsf{ID}})^s}{e(\prod\limits_{\substack{j\in S\\ j\neq \mathsf{ID}}} g_{n+1-j+\mathsf{ID}}, g)^s} \cdot \frac{1}{e(g, g)^{s\cdot(\alpha^{\mathsf{ID}}\gamma)}} = e(g, g_{n+1})^s. \end{aligned}$$

Theorem 1. *If an adversary can break the* BKP-ABE1 *scheme with advantage* ϵ *in the selective security model for* $(\mathcal{U} = [n], \mathcal{A}_{\mathsf{LSSS}})$*-BKP-ABE, then a simulator with advantage* ϵ *in solving the Decision n-BDHE problem can be constructed.*

4.2 Construction BKP-ABE2

▶ Setup: The algorithm first picks a random generator $g, v, h_0, \dots, h_{m'} \in \mathbb{G}$ and random $\alpha, b \in \mathbb{Z}_p$. The public key is $\mathsf{pk} = \big(g, g^b, g^{b^2}, v, v^b, h_0, \dots, h_{m'}, e(g, g)^{\alpha}\big)$. The master key is $\mathsf{msk} = (\alpha, b)$. It outputs $(\mathsf{pk}, \mathsf{msk})$. Define a function $F : \mathbb{Z}_p \to \mathbb{G}$ by $F(x) = \prod_{j=0}^{m'} h_j^{(x^j)}$.

▶ $\mathsf{Encrypt}(S, \omega, \mathcal{M}, \mathsf{pk})$: Inputs to the encryption algorithm are a user index set $S \subseteq \mathcal{U}$ and an attribute set $\omega \subseteq \mathcal{N}$. Let $R = \mathcal{U} \setminus S$. Denote $R = \{\mathsf{ID}_1, \dots, \mathsf{ID}_r\}$.

Pick a random $s \in \mathbb{Z}_p$. Choose random $s_1, \ldots, s_r \in \mathbb{Z}_p$ such that $s = s_1 + \cdots + s_r$. It computes ciphertext $\mathsf{ct} = \big(C, C^{(1)}, \{C^{(2)}_k\}_{k\in\omega}, \{C^{(3)}_j\}_{j\in[1,r]}, \{C^{(4)}_j\}_{j\in[1,r]}\big)$ as

$$C = \mathcal{M} \cdot (e(g,g)^{\alpha})^s, \qquad C^{(1)} = g^s, \qquad C^{(2)}_k = F(k)^s,$$
$$C^{(3)}_j = g^{b\cdot s_j}, \qquad C^{(4)}_j = (g^{b^2\cdot \mathsf{ID}_j} \upsilon^b)^{s_j}.$$

▶ $\mathsf{KeyGen}(\mathsf{ID}, (N,\pi), \mathsf{msk}, \mathsf{pk})$: Inputs to the encryption algorithm are a user index $\mathsf{ID} \in \mathcal{U}$ and a LSSS access structure $(N,\pi) \in \mathcal{A}_{\mathsf{LSSS}}$. Let N be $\ell_{\mathsf{o}} \times k_{\mathsf{o}}$ matrix. The algorithm first randomly chooses $t, z_2 \ldots, z_{k_{\mathsf{o}}} \in \mathbb{Z}_p$ and lets $\boldsymbol{v} = (\alpha + b^2 t, z_2, \ldots, z_{k_{\mathsf{o}}})$. For $i = 1$ to ℓ_{o}, it calculates $\sigma_i = \boldsymbol{N_i} \cdot \boldsymbol{v}$, where $\boldsymbol{N_i}$ is the vector corresponding to ith row of N. It also randomly chooses $r_1, \ldots, r_{\ell_{\mathsf{o}}} \in \mathbb{Z}_p$. It outputs the private key as $\mathsf{sk} = \big(\{D^{(1)}_i\}_{i\in[1,\ell_{\mathsf{o}}]}, \{D^{(2)}_i\}_{i\in[1,\ell_{\mathsf{o}}]}, D^{(3)}, D^{(4)}\big)$ where

$$D^{(1)}_i = g^{\sigma_i} F(\pi(i))^{r_i}, \qquad D^{(2)}_i = g^{r_i}$$
$$D^{(3)} = (g^{b\cdot\mathsf{ID}}\upsilon)^t, \qquad D^{(4)} = g^t. \tag{2}$$

▶ $\mathsf{Decrypt}(\mathsf{ct}, (S,\omega), \mathsf{sk}, (\mathsf{ID}, (N,\pi)), \mathsf{pk})$: Suppose that the attribute set ω satisfies the access structure (N,π) and the user index $\mathsf{ID} \in S$ (so that the decryption is possible). Let $I_{\mathsf{o}} = \{i |\ \pi(i) \in \omega\}$. It then calculates corresponding sets of reconstruction constants $\{(i,\nu_i)\}_{i\in I_{\mathsf{o}}} = \mathsf{Recon}_{(N,\pi)}(\omega)$. Then it computes

$$K = \prod_{i=1}^{\ell_{\mathsf{o}}} \left(\frac{e(D^{(1)}_i, C^{(1)})}{e(C^{(2)}_{\pi(i)}, D^{(2)}_i)} \right)^{\nu_i} \cdot \prod_{j=1}^{r} \left(\frac{e(D^{(4)}, C^{(4)}_j)}{e(D^{(3)}, C^{(3)}_j)} \right)^{1/(\mathsf{ID}-\mathsf{ID}_j)},$$

where it can compute since $\mathsf{ID} \neq \mathsf{ID}_j$ for all $j = 1, \ldots, r$. It then obtains message $\mathcal{M} = C/K$.

Correctness. We can verify its correctness as

$$\begin{aligned} K &= \prod_{i=1}^{\ell_{\mathsf{o}}} \left(\frac{e(g^{\sigma_i} F(\pi(i))^{r_i}, g^s)}{e(F(\pi(i))^s, g^{r_i})} \right)^{\nu_i} \cdot \prod_{j=1}^{r} \left(\frac{e\left(g^t, (g^{b^2\cdot\mathsf{ID}_j}\upsilon^b)^{s_j}\right)}{e\left((g^{b\cdot\mathsf{ID}}\upsilon)^t, g^{b\cdot s_j}\right)} \right)^{1/(\mathsf{ID}-\mathsf{ID}_j)} \\ &= \prod_{i=1}^{\ell_{\mathsf{o}}} e(g,g)^{s\cdot\sigma_i\cdot\nu_i} \cdot \prod_{j=1}^{r} \frac{1}{e\left(g,g\right)^{s_j\cdot b^2\cdot t}} \\ &= e(g,g)^{s\cdot(\alpha+b^2 t)} \cdot \frac{1}{e\left(g,g\right)^{s\cdot b^2\cdot t}} = e(g,g)^{\alpha s}. \end{aligned}$$

Theorem 2. *If an adversary can break the BKP-ABE2 scheme with advantage ϵ in the selective security model for $(\mathcal{U} = \mathbb{Z}_p, \mathcal{A}_{\mathsf{LSSS}})$-BKP-ABE, then a simulator with advantage ϵ in solving the Decision q-MEBDH problem can be constructed, where the size of target revoked set $|R^\star| \leq q$.*

5 Broadcast Ciphertext-Policy ABE

We now present our two broadcast ciphertext-policy ABE schemes. The first scheme $\mathsf{BCP\text{-}ABE1}$ is a combination of broadcast encryption of Boneh-Gentry-Waters [8] and CP-ABE of Waters [23] (the random-oracle-free large-universe scheme). The second scheme $\mathsf{BCP\text{-}ABE2}$ is a combination of broadcast encryption of Sahai-Waters [22] and CP-ABE of Waters. Both schemes have universes as $\mathcal{U} = \mathcal{N} = \mathbb{Z}_p$ and can deal with any linear secret-sharing access structure $\mathcal{A}_{\mathsf{LSSS}}$.

For each scheme, let m be the maximum size of subjective attribute set allowed to be assigned to a key, *i.e.,* we restrict $|\psi| \le m$. Let $\ell_{\mathsf{s,max}}$ be the maximum number of rows allowed in a subjective access structure matrix. Let $m' = m + \ell_{\mathsf{s,max}} - 1$. Also, We will restrict ρ to be an injective function as in [23], but we can extend to an unrestricted scheme similarly also as in [23].

5.1 Construction BCP-ABE1

▶ Setup: The algorithm first picks a random generator $g \in \mathbb{G}$ and a random $\alpha \in \mathbb{Z}_p$. It computes $g_i = g^{(\alpha^i)} \in \mathbb{G}$ for $i = 1, 2, \dots, n, n{+}2, \dots, 2n$. Next, it randomly picks $\gamma \in \mathbb{Z}_p$ and sets $v = g^{\gamma} \in \mathbb{G}$. It then randomly picks $h_0, \dots, h_{m'} \in \mathbb{G}$. The public key is $\mathsf{pk} = \big(g, g_1, \dots, g_n, g_{n+2}, \dots, g_{2n}, v, h_0, \dots, h_{m'}\big)$. The master key is $\mathsf{msk} = (\alpha, \gamma)$. It outputs $(\mathsf{pk}, \mathsf{msk})$. Define a function $F : \mathbb{Z}_p \to \mathbb{G}$ by $F(x) = \prod_{j=0}^{m'} h_j^{(x^j)}$.

▶ $\mathsf{Encrypt}(S, (M, \rho), \mathcal{M}, \mathsf{pk})$: Inputs to the encryption algorithm are a user index set $S \subseteq \mathcal{U}$ and a LSSS access structure (M, ρ) for subjective policy. Let M be $\ell_{\mathsf{s}} \times k_{\mathsf{s}}$ matrix. The algorithm first randomly chooses $s, y_2, \dots, y_{k_{\mathsf{s}}} \in \mathbb{Z}_p$ and lets $\boldsymbol{u} = (s, y_2, \dots, y_{k_{\mathsf{s}}})$. For $i = 1$ to ℓ_{s}, it calculates $\lambda_i = \boldsymbol{M_i} \cdot \boldsymbol{u}$, where $\boldsymbol{M_i}$ is the vector corresponding to ith row of M. The ciphertext ct is set to $\mathsf{ct} = (C, C^{(1)}, \{C_i^{(2)}\}_{i \in [1, \ell_{\mathsf{s}}]}, C^{(3)})$, where

$$C = \mathcal{M} \cdot e(g_n, g_1)^s, \quad C^{(1)} = g^s, \quad C_i^{(2)} = (g_1)^{\lambda_i} F(\rho(i))^{-s}, \quad C^{(3)} = (v \prod_{j \in S} g_{n+1-j})^s.$$

▶ $\mathsf{KeyGen}(\mathsf{ID}, \psi, \mathsf{msk}, \mathsf{pk})$: Inputs to the encryption algorithm are a user index $\mathsf{ID} \in \mathcal{U}$ and an attribute set $\psi \subseteq \mathcal{N}$. The algorithm randomly chooses $r \in \mathbb{Z}_p$. It outputs the private key as $\mathsf{sk} = \big(D^{(1)}, D^{(2)}, \{D_x^{(3)}\}_{x \in \psi}\big)$ where

$$D^{(1)} = g^{\alpha^{\mathsf{ID}}\gamma + \alpha r}, \qquad D^{(2)} = g^r, \qquad D_x^{(3)} = F(x)^r. \tag{3}$$

▶ $\mathsf{Decrypt}(\mathsf{ct}, (S, (M, \rho)), \mathsf{sk}, (\mathsf{ID}, \psi), \mathsf{pk})$: Suppose that the attribute set ψ satisfies the access structure (M, ρ) and the user index $\mathsf{ID} \in S$ (so that the decryption is possible). Let $I_{\mathsf{s}} = \{i | \ \rho(i) \in \psi\}$. It then calculates corresponding sets of reconstruction constants $\{(i, \mu_i)\}_{i \in I_{\mathsf{s}}} = \mathsf{Recon}_{(M,\rho)}(\psi)$. Then it computes the following and obtains message $\mathcal{M} = C/K$.

$$K = \frac{e(g_{\mathsf{ID}}, C^{(3)})}{e(\prod_{\substack{j \in S \\ j \neq \mathsf{ID}}} g_{n+1-j+\mathsf{ID}}, C^{(1)})} \cdot \frac{\prod_{i=1}^{\ell_{\mathsf{s}}} \left(e(C_i^{(2)}, D^{(2)}) \cdot e(C^{(1)}, D^{(3)}_{\rho(i)}) \right)^{\mu_i}}{e(C^{(1)}, D^{(1)})}.$$

We leave the correctness verification to readers due to limited space here.

Theorem 3. *If an adversary can break the* BCP-ABE1 *scheme with advantage ϵ in the selective security model for $(\mathcal{U} = [n], \mathcal{A}_{\mathsf{LSSS}})$-BCP-ABE with a challenge subjective access structure matrix of size $\ell_{\mathsf{s}}^\star \times k_{\mathsf{s}}^\star$ such that $n \geq m + k_{\mathsf{s}}^\star$, then a simulator with advantage ϵ in solving the Decision n-BDHE problem can be constructed.*

5.2 Construction BCP-ABE2

▶ Setup: The algorithm first picks a random generator $g, v, h_0, \ldots, h_{m'} \in \mathbb{G}$ and random $\alpha, a, b \in \mathbb{Z}_p$. The public key is $\mathsf{pk} = \big(g, g^b, g^{b^2}, v, v^b, g^a, h_0, \ldots, h_{m'}, e(g,g)^\alpha\big)$. The master key is $\mathsf{msk} = (\alpha, b)$. It outputs $(\mathsf{pk}, \mathsf{msk})$. Define a function $F : \mathbb{Z}_p \to \mathbb{G}$ by $F(x) = \prod_{j=0}^{m'} h_j^{(x^j)}$.

▶ Encrypt$(S, (M, \rho), \mathcal{M}, \mathsf{pk})$: Inputs to the encryption algorithm are a user index set $S \subseteq \mathcal{U}$ and a LSSS access structure (M, ρ) for subjective policy. Let M be $\ell_{\mathsf{s}} \times k_{\mathsf{s}}$ matrix. Let $R = \mathcal{U} \setminus S$. Denote $R = \{\mathsf{ID}_1, \ldots, \mathsf{ID}_r\}$. The algorithm first randomly chooses $s, y_2, \ldots, y_{k_{\mathsf{s}}} \in \mathbb{Z}_p$ and lets $\boldsymbol{u} = (s, y_2, \ldots, y_{k_{\mathsf{s}}})$. For $i = 1$ to ℓ_{s}, it calculates $\lambda_i = \boldsymbol{M_i} \cdot \boldsymbol{u}$, where $\boldsymbol{M_i}$ is the vector corresponding to ith row of M. It also chooses random $s_1, \ldots, s_r \in \mathbb{Z}_p$ such that $s = s_1 + \cdots + s_r$. The ciphertext ct is set to $\mathsf{ct} = (C, C^{(1)}, \{C_i^{(2)}\}_{i \in [1, \ell_{\mathsf{s}}]}, \{C_j^{(3)}\}_{j \in [1,r]}, \{C_j^{(4)}\}_{j \in [1,r]})$, where

$$C = \mathcal{M} \cdot (e(g,g)^\alpha)^s, \qquad C^{(1)} = g^s, \qquad C_i^{(2)} = g^{a\lambda_i} F(\rho(i))^{-s},$$
$$C_j^{(3)} = g^{b \cdot s_j}, \qquad C_j^{(4)} = (g^{b^2 \cdot \mathsf{ID}_j} v^b)^{s_j}.$$

▶ KeyGen$(\mathsf{ID}, \psi, \mathsf{msk}, \mathsf{pk})$: Inputs to the encryption algorithm are a user index $\mathsf{ID} \in \mathcal{U}$ and an attribute set $\psi \subseteq \mathcal{N}$. The algorithm randomly chooses $t, r \in \mathbb{Z}_p$. It outputs the private key as $\mathsf{sk} = \big(D^{(1)}, D^{(2)}, \{D_x^{(3)}\}_{x \in \psi}, D^{(4)}, D^{(5)}\big)$ where

$$D^{(1)} = g^{\alpha + b^2 t} \cdot g^{ar}, \qquad D^{(2)} = g^r, \qquad D_x^{(3)} = F(x)^r,$$
$$D^{(4)} = (g^{b \cdot \mathsf{ID}} v)^t, \qquad D^{(5)} = g^t. \tag{4}$$

▶ Decrypt$(\mathsf{ct}, (S, (M, \rho)), \mathsf{sk}, (\mathsf{ID}, \psi), \mathsf{pk})$: Suppose that the attribute set ψ satisfies the access structure (M, ρ) and the user index $\mathsf{ID} \in S$ (so that the decryption is possible). Let $I_{\mathsf{s}} = \{i |\ \rho(i) \in \psi\}$. It then calculates corresponding sets of reconstruction constants $\{(i, \mu_i)\}_{i \in I_{\mathsf{s}}} = \mathsf{Recon}_{(M,\rho)}(\psi)$. Then it computes

$$K = \frac{e(C^{(1)}, D^{(1)})}{\prod_{i=1}^{\ell_{\mathsf{s}}} \left(e(C_i^{(2)}, D^{(2)}) \cdot e(C^{(1)}, D^{(3)}_{\rho(i)}) \right)^{\mu_i}} \cdot \prod_{j=1}^{r} \left(\frac{e(D^{(5)}, C_j^{(4)})}{e(D^{(4)}, C_j^{(3)})} \right)^{1/(\mathsf{ID} - \mathsf{ID}_j)},$$

where it can compute since $\mathsf{ID} \neq \mathsf{ID}_j$ for $j = 1, \ldots, r$. It then obtains $\mathcal{M} = C/K$.

Theorem 4. *If an adversary can break the* $\mathsf{BCP\text{-}ABE2}$ *scheme with advantage* ϵ *in the selective security model for* $(\mathcal{U} = \mathbb{Z}_p, \mathcal{A}_{\mathsf{LSSS}})$*-BCP-ABE with a challenge subjective access structure matrix of size* $\ell_{\mathsf{s}}^\star \times k_{\mathsf{s}}^\star$ *such that* $q \geq m + k_{\mathsf{s}}^\star$*, then a simulator with advantage* ϵ *in solving the Decision q-MEBDH problem can be constructed.*

6 Security Proof Overview

Due to limited space, we only give the security proof overview for the proposed schemes here and postpone the full proofs to the the full version of this paper.

Since each system is based on the combination of two underlying schemes, the security proof will be based on both proofs of underlying schemes. It is natural to prove the security by reducing to the stronger assumption out of two base assumptions. To do so, we must extract a problem instance for the other (weaker) base assumption out of the stronger one, so that we can also embed that weaker assumption for the corresponding part of primitive. We summarize the assumptions and the extracted part in Table 1. The assumption at the gray-color slot, which is the stronger one, is the actual underlying assumption for the security of each of our schemes to be reduced to. Note that the extracted assumption for the fourth scheme is indeed not a problem instance for Decision BDHE; however, we are able to prove the ABE part using this assumption.

Table 1. Assumptions in our broadcast ABE and their underlying BE and ABE

Scheme	BE		ABE		Extracted assumption
BKP-ABE1	BGW[8]	BDHE	GPSW[16]	BDH	$(g^s, g^\alpha, g^{\alpha^q}, Z \overset{?}{=} e(g,g)^{\alpha^{q+1}s})$
BKP-ABE2	SW[22]	MEBDH	GPSW[16]	BDH	$(g^s, g^{a_1^2}, g^{\alpha/a_1^2}, Z \overset{?}{=} e(g,g)^{\alpha s})$
BCP-ABE1	BGW[8]	BDHE	W[23]	BDHE	
BCP-ABE2	SW[22]	MEBDH	W[23]	BDHE	$(g^s, \forall_{1\leq i,j\leq q; i\neq j}\ g^{a_i^2}, g^{\alpha/a_i^2}, g^{\alpha a_i^2/a_j^2},$ $Z \overset{?}{=} e(g,g)^{\alpha s})$

7 Adding Key Delegation

In this section, we describe the key delegation algorithm for each of our four schemes. Due to limited space, we postpone those of the two broadcast CP-ABE schemes to the full-length version of this paper. They can be done quite similarly to the cases of broadcast KP-ABE below with some proper re-randomization.

We can say that our schemes subsume the original BE [8,22] and ABE [16,23], since one can delegate keys in these schemes to our broadcast ABE schemes.

7.1 Delegation in BKP-ABE1

This scheme supports delegation of type $\mathsf{sk}_{(\top,\top)} \to \mathsf{sk}_{(\mathsf{ID},\top)} \to \mathsf{sk}_{(\mathsf{ID},(N,\pi))}$. Note that we can base our KP-ABE portion of BKP-ABE on the access tree based approach instead of the LSSS based approach [16] and obtain a BKP-ABE which supports delegation also of type $\mathsf{sk}_{(\mathsf{x},\mathbb{A})} \to \mathsf{sk}_{(\mathsf{x},\mathbb{A}')}$. We omit that details here.

▶ $\mathsf{Delegate}\big[\mathsf{sk}_{(\top,\top)} \rightarrow \mathsf{sk}_{(\mathsf{ID},\top)} \rightarrow \mathsf{sk}_{(\mathsf{ID},(N,\pi))}\big]$: From the master key $\mathsf{msk} = \mathsf{sk}_{(\top,\top)}$ it computes the key $\mathsf{sk}_{(\mathsf{ID},\top)} = g^{(\alpha^{\mathsf{ID}}\gamma)}$. The key $\mathsf{sk}_{(\mathsf{ID},\top)}$ can be delegated to $\mathsf{sk}_{(\mathsf{ID},(N,\pi))} = \big(\{D_i^{(1)}\}_{i\in[1,\ell_{\mathsf{o}}]}, \{D_i^{(2)}\}_{i\in[1,\ell_{\mathsf{o}}]}\big)$ by randomly choosing $z_2,\ldots,z_{k_{\mathsf{o}}}$, $r_1,\ldots,r_{\ell_{\mathsf{o}}} \in \mathbb{Z}_p$ and setting

$$D_i^{(1)} = \big(\mathsf{sk}_{(\mathsf{ID},\top)}\big)^{N_{i,1}} g^{\sum_{j=2}^{k_{\mathsf{o}}} N_{i,j}z_j} F(\pi(i))^{r_i}, \qquad D_i^{(2)} = g^{r_i}.$$

We can show that this key has the same distribution as the one from KeyGen by implicitly defining $\boldsymbol{v} = (\alpha^{\mathsf{ID}}\gamma, z_2, \ldots, z_{k_{\mathsf{o}}})$ and observing that $D_i^{(1)} = g^{\boldsymbol{N_i}\cdot\boldsymbol{v}}F(\pi(i))^{r_i}$ as required.

7.2 Delegation in BKP-ABE2

This scheme supports delegation of both types: $\mathsf{sk}_{(\top,\top)} \rightarrow \mathsf{sk}_{(\mathsf{ID},\top)} \rightarrow \mathsf{sk}_{(\mathsf{ID},(N,\pi))}$ and $\mathsf{sk}_{(\top,\top)} \rightarrow \mathsf{sk}_{(\top,(N,\pi))} \rightarrow \mathsf{sk}_{(\mathsf{ID},(N,\pi))}$. Again, we can base our scheme on the access tree approach and obtain the delegation of type $\mathsf{sk}_{(\mathsf{x},\mathbb{A})} \rightarrow \mathsf{sk}_{(\mathsf{x},\mathbb{A}')}$.

▶ $\mathsf{Delegate}\big[\mathsf{sk}_{(\top,\top)} \rightarrow \mathsf{sk}_{(\mathsf{ID},\top)} \rightarrow \mathsf{sk}_{(\mathsf{ID},(N,\pi))}\big]$: From the master key $\mathsf{msk} = \mathsf{sk}_{(\top,\top)}$ it computes the key $\mathsf{sk}_{(\mathsf{ID},\top)} = \big(D^{(1)}, D^{(3)}, D^{(4)}\big)$ by randomly choosing $t \in \mathbb{Z}_p$ and setting

$$D^{(1)} = g^{\alpha + b^2 t}, \qquad D^{(3)} = (g^{b\cdot\mathsf{ID}}v)^t, \qquad D^{(4)} = g^t.$$

The key $\mathsf{sk}_{(\mathsf{ID},\top)}$ can then be delegated to the key $\mathsf{sk}_{(\mathsf{ID},(N,\pi))} = \big(\{D_i'^{(1)}\}_{i\in[1,\ell_{\mathsf{o}}]}, \{D_i'^{(2)}\}_{i\in[1,\ell_{\mathsf{o}}]}, D'^{(3)}, D'^{(4)}\big)$ by randomly choosing $z_2,\ldots,z_{k_{\mathsf{o}}}, r_1,\ldots,r_{\ell_{\mathsf{o}}}, t' \in \mathbb{Z}_p$ and setting

$$\begin{aligned} D_i'^{(1)} &= \big(D^{(1)} \cdot (g^{b^2})^{t'}\big)^{N_{i,1}} g^{\sum_{j=2}^{k_{\mathsf{o}}} N_{i,j}z_j} F(\pi(i))^{r_i}, \qquad & D_i'^{(2)} &= g^{r_i} \\ D'^{(3)} &= D^{(3)} \cdot (g^{b\cdot\mathsf{ID}}v)^{t'}, & D'^{(4)} &= D^{(4)} \cdot g^{t'}. \end{aligned}$$

We can show that this key has the same distribution as the one from KeyGen by implicitly defining $\boldsymbol{v} = (\alpha + b^2(t+t'), z_2, \ldots, z_{k_{\mathsf{o}}})$ and observing that $D_i'^{(1)} = g^{\boldsymbol{N_i}\cdot\boldsymbol{v}}F(\pi(i))^{r_i}$ as required. The other terms are immediate.

▶ $\mathsf{Delegate}\big[\mathsf{sk}_{(\top,\top)} \rightarrow \mathsf{sk}_{(\top,(N,\pi))} \rightarrow \mathsf{sk}_{(\mathsf{ID},(N,\pi))}\big]$: From the master key $\mathsf{msk} = \mathsf{sk}_{(\top,\top)}$ it computes the key $\mathsf{sk}_{(\top,\mathbb{A})} = \big(\{D_i^{(1)}\}_{i\in[1,\ell_{\mathsf{o}}]}, \{D_i^{(2)}\}_{i\in[1,\ell_{\mathsf{o}}]}\big)$ as follows. It randomly chooses $z_2 \ldots, z_{k_{\mathsf{o}}}, r_1, \ldots, r_{\ell_{\mathsf{o}}} \in \mathbb{Z}_p$ and lets $\boldsymbol{u} = (\alpha, z_2, \ldots, z_{k_{\mathsf{o}}})$. For $i = 1$ to ℓ_{o}, it calculates $\sigma_i = \boldsymbol{N_i} \cdot \boldsymbol{u}$. It then lets

$$D_i^{(1)} = g^{\sigma_i}F(\pi(i))^{r_i}, \qquad D_i^{(2)} = g^{r_i}.$$

The key $\mathsf{sk}_{(\top,\mathbb{A})}$ can then be delegated to the key $\mathsf{sk}_{(\mathsf{ID},(N,\pi))} = \big(\{D_i'^{(1)}\}_{i\in[1,\ell_{\mathsf{o}}]}, \{D_i'^{(2)}\}_{i\in[1,\ell_{\mathsf{o}}]}, D'^{(3)}, D'^{(4)}\big)$ by randomly choosing $z'_2,\ldots,z'_{k_{\mathsf{o}}}, r'_1,\ldots,r'_{\ell_{\mathsf{o}}}, t \in \mathbb{Z}_p$ and setting

$$\begin{aligned} D_i'^{(1)} &= D_i^{(1)} \cdot (g^{b^2})^{tN_{i,1}} g^{\sum_{j=2}^{k_{\mathsf{o}}} N_{i,j}z'_j} F(\pi(i))^{r'_i}, \qquad & D_i'^{(2)} &= D_i^{(2)} \cdot g^{r'_i} \\ D'^{(3)} &= (g^{b\cdot\mathsf{ID}}v)^t, & D'^{(4)} &= g^t. \end{aligned}$$

We can show that this key has the same distribution as the one from KeyGen by implicitly defining $\boldsymbol{v} = (\alpha + b^2 t, z_2 + z'_2, \ldots, z_{k_\circ} + z'_{k_\circ})$ and observing that $D'^{(1)}_i = g^{\boldsymbol{N_i} \cdot \boldsymbol{v}} F(\pi(i))^{r_i + r'_i}$ as required. The other terms are immediate.

8 Efficiency

Table Description. In this section, we give an efficiency comparison using Table 2. Each amount in the table shows the number of group elements in $\mathbb{G}$, which is a bilinear group with bilinear map $\mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. The exception is that for those values with †, one element of $\mathbb{G}_T$ is included in that amount. $|\text{cipher}|$, $|\text{priv}|$, $|\text{pub}|$ are the sizes of ciphertext for key encapsulation, private key and public key respectively. Here r is the number of revoked user, n is the number of all users. Let t be the size of rows in LSSS access structure matrix, which is equal to the number of attributes appeared in the access structure. Recall that an access structure is associated with ciphertext in the case of ciphertext-policy ABE and with private key in the case of key-policy ABE. Let ℓ be the maximum size allowed for t. Let k be the size of the attribute set (associated with private key in the case of ciphertext-policy ABE and with ciphertext in the case of key-policy ABE). Let m be the maximum size allowed for k.

The OSW scheme refers to the scheme mentioned implicitly in §3.5 of [20]. The amount in the column in gray color shows the overhead of the present revocable scheme to its underlying original (non-revocable) ABE schemes: the underlying CP-ABE of OSW scheme [20] is Bethencourt et al. scheme [5] (in which security proof is done only in the generic group and random oracle model); the underlying CP-ABE of both BCP-ABE1,2 is Waters' CP-ABE [23]; the underlying KP-ABE of both BKP-ABE1,2 is KP-ABE of Goyal et al. [16]. In particular, the amount excluding the gray column is the efficiency of those original schemes.

Efficiency of Revocable ABE. BKP-ABE1 scheme has almost the same efficiency in ciphertext and private key sizes to that of the original (non-revocable)

Table 2. Efficiency comparison among directly revocable ABE schemes

	Revocable CP-ABE		Revocable KP-ABE	
Previous	OSW [20]		None	
	$\lvert\text{cipher}\rvert = (2t+1)$	$+O(r)$		
	$\lvert\text{priv}\rvert = (2k+2)$	$\cdot(\log n)$		
	$\lvert\text{pub}\rvert = (3^\dagger$	$\cdot \log n) + O(n)$		
Ours	BCP-ABE1		BKP-ABE1	
	$\lvert\text{cipher}\rvert = (t+1)$	$+1$	$\lvert\text{cipher}\rvert = (k+1)$	$+1$
	$\lvert\text{priv}\rvert = (k+2)$		$\lvert\text{priv}\rvert = (2t)$	
	$\lvert\text{pub}\rvert = (m+\ell+3)^\dagger$	$+(2n-1)$	$\lvert\text{pub}\rvert = (m+4)$	$+(2n-2)$
	BCP-ABE2		BKP-ABE2	
	$\lvert\text{cipher}\rvert = (t+1)$	$+2r$	$\lvert\text{cipher}\rvert = (k+1)$	$+2r$
	$\lvert\text{priv}\rvert = (k+2)$	$+2$	$\lvert\text{priv}\rvert = (2t)$	$+2$
	$\lvert\text{pub}\rvert = (m+\ell+3)^\dagger$	$+4$	$\lvert\text{pub}\rvert = (m+4)$	$+3^\dagger$

KP-ABE of Goyal et al.[16], albeit it has a large pubic key size linear to n. BKP-ABE2 scheme reduces the public key size to almost the same of the original (non-revocable) KP-ABE while the ciphertext requires only $2r$ group elements additively. Note that these are the first fully functional directly revocable KP-ABE schemes in the literature. The efficiency performance also holds similarly for revocable CP-ABE variant. In particular, it performs better than the previous OSW scheme, whose ciphertext requires $O(r)$ elements additively and private key requires $\log n$ overhead multiplicatively to the original scheme. Note that we can improve all the four proposed schemes by using random oracle; the resulting schemes reduce the public key size by m elements.

We finally note two *implicit* possible schemes. Applying Sahai-Waters negated clause framework [22] to Waters' CP-ABE (analogously to the KP case described in §5 of [22]), one can obtain CP-ABE that supports negated clauses, which can be used as revocable CP-ABE as described in §1. This improves the OSW scheme but is still less efficient than our dedicated BCP-ABE. Furthermore, concurrently to this paper, Attrapadung and Imai [3] recently proposed a new variant of ABE called dual-policy ABE (DP-ABE), which is a conjunctively combined scheme from KP and CP ABE. By using negated clauses in CP part, DP-ABE gives a revocable KP-ABE, but our dedicated BKP-ABE schemes are more efficient.

Efficiency of Disjunctive Multi-authority ABE. The efficiency from Table 2 translates to the disjunctive multi-authority ABE application as it is, where n is the number of all authorities and $r = n - |S|$ is the number of revoked authorities. For ciphertext-policy case, the only previous scheme is the trivial concatenated scheme, whose ciphertext requires $|S|$ overhead multiplicatively to the original ABE scheme. For key-policy case, a simple multi-authority scheme which is better than the trivial one can be constructed from KP-ABE by setting the authority key using policy ID. The key for policy $\mathbb{A}$ derived from this authority is set using policy $\mathsf{ID} \wedge \mathbb{A}$. Encrypting to attribute set ω is done by associating $\omega \cup \{S\}$ to ciphertext. This scheme poses overhead $|S|$ additively to ciphertext size. Our first BCP and BKP ABE is more efficient: its ciphertext size is roughly the same as its original ABE.

References

1. Aiello, W., Lodha, S., Ostrovsky, R.: Fast digital identity revocation (extended abstract). In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 137–152. Springer, Heidelberg (1998)
2. Attrapadung, N., Imai, H.: Graph-decomposition-based frameworks for subset-cover broadcast encryption and efficient instantiations. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 100–120. Springer, Heidelberg (2005)
3. Attrapadung, N., Imai, H.: Dual-policy attribute based encryption. In: Abdalla, M., Pointcheval, D., Fouque, P.-A., Vergnaud, D. (eds.) ACNS 2009. LNCS, vol. 5536, pp. 168–185. Springer, Heidelberg (2009)
4. Attrapadung, N., Furukawa, J., Imai, H.: Forward-secure and searchable broadcast encryption with short ciphertexts and private keys. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 161–177. Springer, Heidelberg (2006)

5. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy 2007, pp. 321–334 (2007)
6. Boldyreva, A., Goyal, V., Kumar, V.: Identity-based encryption with efficient revocation. In: ACM Conference on Computer and Communications Security 2008, pp. 417–426 (2008)
7. Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
8. Boneh, D., Gentry, C., Waters, B.: Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 258–275. Springer, Heidelberg (2005)
9. Boneh, D., Hamburg, M.: Generalized identity based and broadcast encryption schemes. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 455–470. Springer, Heidelberg (2008)
10. Chase, M.: Multi-authority attribute based encryption. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 515–534. Springer, Heidelberg (2007)
11. Dodis, Y., Fazio, N.: Public-key broadcast encryption for stateless receivers. In: Feigenbaum, J. (ed.) DRM 2002. LNCS, vol. 2696, pp. 61–80. Springer, Heidelberg (2002)
12. Fiat, A., Naor, M.: Broadcast encryption. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 480–491. Springer, Heidelberg (1993)
13. Gentry, C.: Certificate-based encryption and the certificate revocation problem. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 272–293. Springer, Heidelberg (2003)
14. Gollé, P., Staddon, J., Gagne, M., Rasmussen, P.: A content-driven access control system. In: Symposium on Identity and Trust on the Internet — IDtrust 2008, pp. 26–35 (2008)
15. Goyal, V., Jain, A., Pandey, O., Sahai, A.: Bounded ciphertext policy attribute-based encryption. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I. (eds.) ICALP 2008, Part II. LNCS, vol. 5126, pp. 579–591. Springer, Heidelberg (2008)
16. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM Conference on Computer and Communications Security 2006, pp. 89–98 (2006)
17. Micali, S.: Efficient certificate revocation. Tech. Report MIT/LCS/TM-542b (1996)
18. Naor, D., Naor, M., Lotspiech, J.: Revocation and tracing schemes for stateless receivers. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 41–62. Springer, Heidelberg (2001)
19. Naor, M., Pinkas, B.: Efficient trace and revoke schemes. In: Frankel, Y. (ed.) FC 2000. LNCS, vol. 1962, pp. 1–20. Springer, Heidelberg (2001)
20. Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. In: ACM Conference on Computer and Communications Security 2007, pp. 195–203 (2007)
21. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)
22. Sahai, A., Waters, B.: Revocation systems with very small private keys. Cryptology ePrint archive: report 2008/309 (2008)
23. Waters, B.: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. Cryptology ePrint archive: report 2008/290 (2008)