A Framework and Compact Constructions for Non-monotonic Attribute-Based Encryption

Shota Yamada[1,⋆], Nuttapong Attrapadung[2],
Goichiro Hanaoka[2], and Noboru Kunihiro[1]

[1] The University of Tokyo
{yamada@it.,kunihiro}@k.u-tokyo.ac.jp
[2] National Institute of Advanced Industrial Science and Technology (AIST)
{n.attrapadung,hanaoka-goichiro}@aist.go.jp

Abstract. In this paper, we propose new non-monotonic attribute-based encryption schemes with compact parameters. The first three schemes are key-policy attribute-based encryption (KP-ABE) and the fourth scheme is ciphertext-policy attribute-based encryption (CP-ABE) scheme.

- Our first scheme achieves the shortest ciphertext overhead in the literature. Compared to the scheme by Attrapadung et al. (PKC2011), which is the best scheme in terms of the ciphertext overhead, our scheme shortens ciphertext overhead by 33%. The scheme also reduces the size of the master public key to about half.
- Our second scheme is proven secure under the decisional bilinear Diffie-Hellman (DBDH) assumption, which is one of the most standard assumptions in bilinear groups. Compared to the non-monotonic KP-ABE scheme from the same assumption by Ostrovsky et al. (ACM-CCS'07), our scheme reduces the size of the master public key and the ciphertext to about half.
- Our third scheme is the first non-monotonic KP-ABE scheme that can deal with unbounded size of set and access policies. That is, there is no restriction on the size of attribute sets and the number of allowed repetition of the same attributes which appear in an access policy. The master public key of our scheme consists of only constant number of group elements.
- Our fourth scheme is the first non-monotonic CP-ABE scheme that can deal with unbounded size of set and access policies. The master public key of the scheme consists of only constant number of group elements.

We construct our KP-ABE schemes in a modular manner. We first introduce special type of predicate encryption that we call two-mode identity based broadcast encryption (TIBBE). Then, we show that any TIBBE scheme that satisfies certain condition can be generically converted into non-monotonic KP-ABE scheme. Finally, we construct efficient TIBBE schemes and apply this conversion to obtain the above new non-monotonic KP-ABE schemes.

Keywords: Attribute-based encryption, non-monotonic access structure, compact parameters.

⋆ The first author is supported by a JSPS Research Fellowship for Young Scientists.

H. Krawczyk (Ed.): PKC 2014, LNCS 8383, pp. 275–292, 2014.

1 Introduction

In many systems, a server monitors access to sensitive data so that only certain users can access it. If the server is not fully trusted, the data must be encrypted. However, a standard public key encryption scheme is not appropriate, because it severely limits the users who can access the contents.

To solve this problem, Sahai and Waters [31] were the first to study attribute-based encryption (ABE). In ABE, one can encrypt data for a set of receivers that satisfy certain condition. In Sahai and Waters' scheme, a ciphertext and a private key are associated with a set of attributes, and the key can decrypt the ciphertext if and only if these sets overlap more than certain threshold. Goyal, Pandey, Sahai, and Waters [16] further extended their result and proposed schemes that support finer-grained access control. In their scheme, a ciphertext is associated with a set of attributes, and a private key is associated with an access structure that is specified by a Boolean formula. Decryption is possible when the set satisfies this Boolean formula. Their schemes are called key-policy ABE (KP-ABE), because the key specifies the access structure. Ciphertext-policy ABE (CP-ABE) is complementary form to KP-ABE in the sense that a ciphertext specifies an access structure while a key is associated with a set of attributes. The first studies of CP-ABE appear in [5,12].

The above schemes can express a wide class of access structures, but they are still limited because they only support a monotonic access structure. In particular, they cannot deal with an access structure that is associated with a Boolean formula that includes the negation of attributes. This is not convenient for real world applications. One possible solution to this problem is to explicitly include attributes that express absence of attributes in the attribute space, as suggested in [16]. For example, in the CP-ABE case, to generate a key for an attribute x_1, one should generate the key for a set that includes x_1 and attributes "Not x_j" for all attribute x_j such that $x_j \neq x_1$, using the underlying monotonic CP-ABE system. Then, a ciphertext for "Not x_2" can be decrypted by the key as desired, because "Not x_2" $\in \{x_1$, "Not x_2", "Not x_3", $\ldots,\}$. This solution works well in the settings where attribute space is small, but does not work if the attribute space is exponentially large.

Ostrovsky, Sahai, and Waters [28] addressed this problem and constructed the first KP-ABE scheme that supports a non-monotonic access structure by using an idea from the Naor-Pinkas revocation scheme [25]. Following their work, several non-monotonic KP/CP-ABE schemes have been proposed [21,26,3,27].

Our Contributions. In this paper, we propose new non-monotonic ABE schemes. Our new schemes either improve efficiency or achieve a new functionality that was previously not possible. We propose the following four schemes. The first three schemes are KP-ABE schemes and the last one is CP-ABE scheme.

- The first scheme has very compact ciphertexts. The ciphertext overhead of our scheme consists of only two group elements, which is even shorter than the currently shortest scheme of [3]. Furthermore, the scheme also reduces the size of master public key to about half while the private key size is slightly larger.

- The second scheme is proven secure under the decisional bilinear Diffie-Hellman (DBDH) assumption, which is one of the weakest number theoretic assumptions in bilinear groups. The public key and the ciphertext size of our scheme are about half the size of the scheme in [28], which is secure under the same assumption. The encryption algorithm of our scheme is at least two times faster than the existing scheme, but our decryption algorithm is somewhat slower.
- The third scheme is the first non-monotonic KP-ABE scheme in the standard model that supports fully unbounded attribute sets and access policies. That is, there is no restriction on the size of the attribute set, or on the number of times the same attributes can appear in an access policy. The master public key of the scheme is very compact: it consists of only constant number of group elements. Such a construction has previously only been possible in the random oracle model [21].
- The fourth scheme is the first non-monotonic CP-ABE scheme that supports fully unbounded size of attribute sets and access policies. The master public key of our scheme consists of only constant number of group elements.

We construct the above KP-ABE schemes in a modular way. First, we define a new predicate encryption that we call two mode identity based broadcast encryption (TIBBE). In TIBBE, a ciphertext is associated with a set of identities. A private key is associated with an identity and certain "type". There are two types of keys in the system. First type keys can decrypt the ciphertext iff the identity is included in the set, while the second type keys can iff the identity is *not* included. The notion of TIBBE is an extension of identity based broadcast encryption (IBBE) and identity based revocation (IBR). We show that any TIBBE scheme with a certain property can be generically converted into a non-monotonic KP-ABE scheme. This can be seen as an extension of the previous result in [3] that converts any IBBE scheme with certain properties into a (monotonic) KP-ABE scheme. Finally, we construct efficient TIBBE schemes. By applying our conversion to these schemes, we obtain our new non-monotonic KP-ABE schemes.

While we construct KP-ABE schemes in a modular way, our construction of the above non-monotonic CP-ABE scheme is more direct. Our construction is based on the (monotonic) CP-ABE scheme recently proposed by [30]. We extend their scheme to support a non-monotonic access structure by applying an idea from the IBR scheme in [21] to the CP-ABE setting.

Finally, we remark that all our schemes are selectively secure. Constructing adaptively secure schemes with similar property is left open for future research.

Other Related Works. After the work of Sahai and Waters [31], many CP/KP-ABE schemes have been proposed [16,15,32,17]. The first adaptively secure ABE schemes were proposed in [20] using composite order groups. Later, schemes on prime order groups were proposed [26,27,19,24]. The settings with multiple-authorities are investigated in several works [10,1,11,22]. To construct a scheme with even more general access structure is an important direction of research. Recently, there are significant progress toward this direction [33,13,14].

2 Preliminaries

2.1 Notation

We will treat a vector as a row vector, unless stated otherwise. For any vector $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{Z}_p^n$, $g^{\mathbf{a}} = (g^{a_1}, \ldots, g^{a_n})$. For $\mathbf{a}, \mathbf{z} \in \mathbb{Z}_p^n$, we denote their inner product as $\langle \mathbf{a}, \mathbf{z} \rangle = \mathbf{a} \cdot \mathbf{z}^\top = \sum_{i=1}^n a_i z_i$. We denote by $\mathbf{e}_i$ the i-th unit vector: its i-th component is one, all others are zero. We also denote by $[n]$ a set $\{1, \ldots, n\}$ for an integer $n > 0$ and $[n_1, \ldots, n_m] = [n_1] \times \cdots \times [n_m]$ for integers $n_1, \ldots, n_m > 0$. For a set U, we define $2^U = \{S | S \subseteq U\}$ and $\binom{U}{<k} = \{S | S \subseteq U, |S| < k\}$ for $k \leq |U|$.

2.2 Definition of Predicate Encryption

Here, we define the syntax of predicate encryption. We emphasize that we do not consider attribute hiding in this paper.[1]

Syntax. Let $R = \{R_N : A_N \times B_N \to \{0,1\} \mid N \in \mathbb{N}^c\}$ be a relation family where A_N and B_N denote "key attribute" and "ciphertext attribute" spaces and c is some fixed constant. The index $N = (n_1, n_2, \ldots, n_c)$ of R_N denotes the numbers of bounds for corresponding parameters. If an index N is not required, we say that R is an unbounded relation. A predicate encryption (PE) scheme for R consists of the following algorithms:

$\mathsf{Setup}(\lambda, N) \to (\mathsf{mpk}, \mathsf{msk})$: The setup algorithm takes as input a security parameter λ and a index N of the relation R_N and outputs a master public key mpk and a master secret key msk.

$\mathsf{KeyGen}(\mathsf{msk}, \mathsf{mpk}, X) \to \mathsf{sk}_X$: The key generation algorithm takes as input the master secret key msk, the master public key mpk, and a key attribute $X \in A_N$. It outputs a private key sk_X. We assume X is included in sk_X implicitly.

$\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{M}, Y) \to C$: The encryption algorithm takes as input a master public key mpk, the message M, and a ciphertext attribute $Y \in B_N$. It will output a ciphertext C.

$\mathsf{Decrypt}(\mathsf{mpk}, C, Y, \mathsf{sk}_X) \to \mathsf{M}$ or $\perp$: We assume that the decryption algorithm is deterministic. The decryption algorithm takes as input the public parameters mpk, a ciphertext C, ciphertext attribute $Y \in B_N$ and a private key sk_X. It outputs the message M or $\perp$ which represents that the ciphertext is not in a valid form.

We require correctness of decryption: that is, for all λ, N, all $(\mathsf{mpk}, \mathsf{msk})$ produced by $\mathsf{Setup}(\lambda, N)$, all $X \in A_N, Y \in B_N$ such that $R(X, Y) = 1$, and all sk_X returned by $\mathsf{KeyGen}(\mathsf{msk}, \mathsf{mpk}, X)$, $\mathsf{Decrypt}(\mathsf{mpk}, \mathsf{Encrypt}(\mathsf{mpk}, \mathsf{M}, Y), Y, \mathsf{sk}_X) = \mathsf{M}$ holds.

Security. We now define the security for an PE scheme Π. This security notion is defined by the following game between a challenger and an attacker $\mathcal{A}$.

At first, the challenger runs the setup algorithm and gives mpk to $\mathcal{A}$. Then $\mathcal{A}$ may adaptively make key-extraction queries. We denote this phase **Phase1**. In this phase, if $\mathcal{A}$ submits X to the challenger, the challenger returns $\mathsf{sk}_X \leftarrow \mathsf{KeyGen}(\mathsf{msk}, \mathsf{mpk}, X)$. At some point, $\mathcal{A}$ outputs two equal length messages

[1] This is called "public-index" predicate encryption, categorized in [9].

M_0 and M_1 and challenge ciphertext attribute $Y^\star \in B_N$. $Y^\star$ cannot satisfy $R(X, Y^\star) = 1$ for any attribute X such that $\mathcal{A}$ already queried private key for X. Then the challenger flips a random coin $\beta \in \{0,1\}$, runs $\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{M}_\beta, Y^\star) \to C^\star$ and gives challenge ciphertext $C^\star$ to $\mathcal{A}$. In **Phase2**, $\mathcal{A}$ may adaptively make queries as in **Phase1** with following added restriction: $\mathcal{A}$ cannot make a key-extraction query for X such that $R(X, Y^\star) = 1$. At last, $\mathcal{A}$ outputs a guess β' for β. We say that $\mathcal{A}$ succeeds if $\beta' = \beta$ and denote the probability of this event by $\Pr^{PE}_{\mathcal{A},\Pi}$. The advantage of an attacker $\mathcal{A}$ is defined as $\mathsf{Adv}^{PE}_{\mathcal{A},\Pi} = |\Pr^{PE}_{\mathcal{A},\Pi} - \frac{1}{2}|$. We say that Π is fully secure if $\mathsf{Adv}^{PE}_{\mathcal{A},\Pi}$ is negligible for all probabilistic polynomial time (PPT) adversary $\mathcal{A}$.

A weaker notion called selective security can be defined as in the above game with the exception that the adversary $\mathcal{A}$ has to choose the challenge ciphertext index $Y^\star$ before the setup phase but private key queries $X_1, \ldots, X_q$ can still be adaptive. All schemes proposed in this paper are selectively secure.

2.3 Linear Secret Sharing Scheme and Attribute-Based Encryption

Here, we first define linear secret sharing scheme (LSSS) following [4] and then define key/ciphertext-policy atrribute based encryption scheme as an instance of PE.

Definition 1 (Access Structure). *Let $\mathcal{P} = \{\mathcal{P}_1, \ldots, \mathcal{P}_n\}$ be a set of parties. A collection $\mathbb{A} \subset 2^{\mathcal{P}}$ is said to be monotone if, for all B, C, if $B \in \mathbb{A}$ and $B \subset C$, then $C \in \mathbb{A}$ holds. An access structure (resp., monotonic access structure) is a collection (resp., monotone collection) $\mathbb{A} \subset 2^{\mathcal{P}} \backslash \{\emptyset\}$. 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 Scheme). *Let $\mathcal{P}$ be a set of parties. Let L be an $\ell \times m$ matrix. Let $\pi : \{1, \ldots, \ell\} \to \mathcal{P}$ 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 (LSSS) in $\mathbb{Z}_p$ and is represented by (L, π) if it consists of two efficient algorithms:*

$\mathsf{Share}_{L,\pi}$. *There exists an efficient algorithm which takes as input $s \in \mathbb{Z}_p$ which is to be shared. It chooses $s_2, \ldots, s_m \xleftarrow{\$} \mathbb{Z}_p$ and let $\mathbf{s} = (s, s_2, \ldots, s_m)$. It outputs $L \cdot \mathbf{s}$ as the vector of ℓ shares. The share $\lambda_i = \langle \mathbf{L}_i, \mathbf{s} \rangle$ belongs to party $\pi(i)$, where $\mathbf{L}_i$ denotes the i-th row of L.*

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

Terminology for Non-monotonic Access Structure. We recall a technique by Ostrovsky Sahai, and Waters [28] to move from monotonic access structures to non-monotonic access structure. They assume a family $\{\Pi_{\mathbb{A}}\}_{\mathbb{A} \in \mathcal{AS}}$ of linear secret sharing schemes for a set of monotonic access structures $\mathbb{A}$. For each such access structure $\mathbb{A} \in \mathcal{AS}$, the set $\mathcal{P}$ of underlying parties has the following properties: The names of the parties in $\mathcal{P}$ may be of two types: either

the name is normal (like x) or it is primed (like x'), and if $x \in \mathcal{P}$ then $x' \in \mathcal{P}$ and vice versa. Conceptually, prime attributes are associated with negation of unprimed attributes.

A family $\mathcal{AS}$ of non-monotone access structures can be defined as follows. For each access structure $\mathbb{A} \in \mathcal{AS}$ over a set of parties $\mathcal{P}$, one defines a possibly non-monotonic access structure $NM(\mathbb{A})$ over the set $\tilde{\mathcal{P}}$ of all unprimed parties in $\mathcal{P}$. For every set $\tilde{S} \subset \tilde{\mathcal{P}}$, $N(\tilde{S})$ is defined as $N(\tilde{S}) = \tilde{S} \cup \{x' | x \in \tilde{\mathcal{P}} \backslash \tilde{S}\}$. Then, $NM(\mathbb{A})$ is defined by saying that $\tilde{S}$ is authorized in $NM(\mathbb{A})$ if and only if $N(\tilde{S})$ is authorized in $\mathbb{A}$. For each access set $X \in NM(\mathbb{A})$, there is a set in $\mathbb{A}$ containing the elements in X and primed elements for each party not in X.

Key-(Ciphertext) Policy Attribute-Based Encrypyion. Let $\mathcal{U} = \{0,1\}^*$ be an attribute space and $N = (n, \varphi)$ specify the corresponding bounds (the maximum numbers) on the size of attribute sets, the number of allowed repetition of same attributes which appear in a policy, respectively. Let $\mathcal{AS}_\varphi$ be a collection of access structures over $\mathcal{U}$ such that every access structure in $\mathcal{AS}_\varphi$ is specified by an access formula in which same attributes do not appear more than φ times. A bounded key (resp. ciphertext)-policy attribute-based encryption for $\mathcal{AS}_\varphi$ is a predicate encryption for $R^{\mathsf{KP}}_{(n,\varphi)} : \mathcal{AS}_\varphi \times \binom{\mathcal{U}}{<n} \to \{0,1\}$ (resp. $R^{\mathsf{CP}}_{(n,\varphi)} : \binom{\mathcal{U}}{<n} \times \mathcal{AS}_\varphi \to \{0,1\}$) defined by $R^{\mathsf{KP}}_{(n,\varphi)}(\mathbb{A}, \omega) = 1$ (resp. $R^{\mathsf{CP}}_{(n,\varphi)}(\omega, \mathbb{A}) = 1$) iff $\omega \in \mathbb{A}$ (for $\omega \subseteq U$ such that $|\omega| < n$ and $\mathbb{A} \in \mathcal{AS}_\varphi$). Let $\mathcal{AS}$ be a collection of access structure over $\mathcal{U}$. An unbounded key (resp., ciphertext)-policy attribute-based encryption scheme is a predicate encryption for $R^{\mathsf{KP}} : \mathcal{AS} \times 2^{\mathcal{U}} \to \{0,1\}$ (resp., $R^{\mathsf{CP}} : 2^{\mathcal{U}} \times \mathcal{AS} \to \{0,1\}$) defined by $R^{\mathsf{KP}}(\mathbb{A}, \omega) = 1$ (resp. $R^{\mathsf{CP}}(\omega, \mathbb{A}) = 1$) iff $\omega \in \mathbb{A}$ (for $\omega \subseteq U$ and $\mathbb{A} \in \mathcal{AS}$).

We note that the scheme of [27] (which was called unbounded ABE) can achieve the unbounded attribute set size, but it is still limited to the number of allowed repetition. Currently, only few KP-ABE schemes that are unbounded in full sence are known [21,23,30]. Note that the scheme in [21] uses random oracle model. In the CP-ABE setting, only scheme that is unbounded in full sense is recently proposed [30].

2.4 Number Theoretic Assumptions

We use groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order p with an efficiently computable mapping $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ s.t. $e(g^a, h^b) = e(g,h)^{ab}$ for any $(g,h) \in \mathbb{G} \times \mathbb{G}$, $a, b \in \mathbb{Z}$ and $e(g,h) \neq 1_{\mathbb{G}_T}$ whenever $g, h \neq 1_{\mathbb{G}}$.

Decisional Bilinear Diffie-Hellman (DBDH) Assumption. We say that an adversary $\mathcal{A}$ breaks the DBDH assumption on $(\mathbb{G}, \mathbb{G}_T)$ if $\mathcal{A}$ runs in polynomial time and $\frac{1}{2}|\Pr[\mathcal{A}(g, g^a, g^b, g^s, e(g,g)^{abs}) \to 0] - \Pr[\mathcal{A}(g, g^a, g^b, g^s, T) \to 0]|$ is negligible where $g \xleftarrow{\$} \mathbb{G}$, $T \xleftarrow{\$} \mathbb{G}_T$, $a, b, s \xleftarrow{\$} \mathbb{Z}_p$.

n-Decisional Bilinear Diffie-Hellman Exponent (n-DBDHE) Assumption [7]. We say that an adversary $\mathcal{A}$ breaks the n-DBDHE assumption on $(\mathbb{G}, \mathbb{G}_T)$ if $\mathcal{A}$ runs in polynomial time and $\frac{1}{2}|\Pr[\mathcal{A}(g, \{g^{a^i}\}_{i \in [2n] \backslash \{n+1\}}, g^s, e(g,g)^{s \cdot a^{n+1}}) \to 0] - \frac{1}{2}|\Pr[\mathcal{A}(g, \{g^{a^i}\}_{i \in [2n] \backslash \{n+1\}}, g^s, T) \to 0]|$ is negligible where $g \xleftarrow{\$} \mathbb{G}$, $T \xleftarrow{\$} \mathbb{G}_T$, $a, s \xleftarrow{\$} \mathbb{Z}_p$.

3 Linear Two-Mode Identity Based Broadcast Encryption and Conversion to Non-monotonic KP-ABE

In this section, we first introduce the two mode inner product encryption scheme (TIPE) and two mode identity based broadcast encryption schemes (TIBBE) and explain how the latter can be derived from the former. Then, we propose a general transformation that transforms any TIBBE scheme that satisfies a certain condition into a non-monotonic KP-ABE scheme. Our transformation is an extension of the generic transformation proposed in [3], which converts any IBBE scheme with certain conditions into (monotonic) KP-ABE scheme.

3.1 Definition of TIPE and TIBBE

In a TIPE scheme, a ciphertext is associated with a vector $\mathbf{y}$. A private key is associated with $\mathsf{type} \in \{\mathsf{ZIPE}, \mathsf{NIPE}\}$ and a vector $\mathbf{x}$. Decryption is possible iff $\mathsf{type} = \mathsf{ZIPE}$ and $\langle \mathbf{x}, \mathbf{y} \rangle = 0$, or $\mathsf{type} = \mathsf{NIPE}$ and $\langle \mathbf{x}, \mathbf{y} \rangle \neq 0$. In a TIBBE scheme, a ciphertext is associated with a set of identities S. A private key is associated with $\mathsf{type} \in \{\mathsf{IBBE}, \mathsf{IBR}\}$ and an identity ID. Decryption is possible iff $\mathsf{type} = \mathsf{IBBE}$ and $\mathsf{ID} \in S$, or $\mathsf{type} = \mathsf{IBR}$ and $\mathsf{ID} \notin S$.

Here, we formally define TIPE and TIBBE as instances of PE as follows.

Two-Mode Inner Product Encryption scheme. TIPE is a predicate encryption for $R^{\mathsf{TIPE}}_{(n,p)} : (\mathbb{Z}_p^n \times \{\mathsf{ZIPE}, \mathsf{NIPE}\}) \times \mathbb{Z}_p^n \to \{0,1\}$ defined by $R^{\mathsf{TIPE}}_{(n,p)}((\mathbf{x}, \mathsf{type}), \mathbf{y}) = 1$ iff $(\langle \mathbf{x}, \mathbf{y} \rangle = 0 \wedge \mathsf{type} = \mathsf{ZIPE}) \vee (\langle \mathbf{x}, \mathbf{y} \rangle \neq 0 \wedge \mathsf{type} = \mathsf{NIPE})$.

Two-Mode Identity Based Broadcast Encryption scheme. TIBBE is a predicate encryption for $R^{\mathsf{TIBBE}}_n : (\mathcal{I} \times \{\mathsf{IBBE}, \mathsf{IBR}\}) \times \binom{\mathcal{I}}{<n} \to \{0,1\}$ defined by $R^{\mathsf{TIBBE}}_n((\mathsf{ID}, \mathsf{type}), S) = 1$ iff $(\mathsf{ID} \in S \wedge \mathsf{type} = \mathsf{IBBE}) \vee (\mathsf{ID} \notin S \wedge \mathsf{type} = \mathsf{IBR})$.

In later sections, we construct TIPE schemes instead of TIBBE schemes when it is simpler to describe. TIBBE scheme can be derived from TIPE scheme by the following technique due to [18]. The setup algorithm of the TIBBE scheme is the same as TIPE scheme. To generate a private key for $(\mathsf{ID}, \mathsf{IBBE})$ (resp. $(\mathsf{ID}, \mathsf{IBR})$), one runs key generation algorithm of TIPE scheme to obtain a private key for $(\mathbf{x}, \mathsf{ZIPE})$ (resp. $(\mathbf{x}, \mathsf{NIPE})$) where $\mathbf{x} = (1, \mathsf{ID}, \ldots, \mathsf{ID}^{n-1})$. To encrypt a message M for a set $S = (\mathsf{ID}_1, \ldots, \mathsf{ID}_k)$, one defines $\mathbf{y} = (y_1, \ldots, y_n)$ as a coefficient vector from $P_S[Z] = \sum_{i=1}^{k+1} y_i Z^{i-1} = \prod_{\mathsf{ID}_j \in S}(Z - \mathsf{ID}_j)$ where, if $k+1 < n$, the coordinates $y_{k+1}, \ldots, y_n$ are all set to 0. Then, one runs encryption algorithm of TIPE scheme to encrypt M for a vector $\mathbf{y}$. To decrypt a ciphertext, one first defines $\mathbf{x}$ and $\mathbf{y}$ as above and runs the decryption algorithm of the TIPE scheme. Since $\mathsf{ID} \in S \Leftrightarrow P_S(\mathsf{ID}) = 0 \Leftrightarrow \langle \mathbf{x}, \mathbf{y} \rangle = 0$, the correctness of the resulting TIBBE scheme follows from the correctness of the underlying TIPE scheme. Furthermore, by the embedding lemma [8], the resulting TIBBE scheme is selectively secure if the underlying TIPE scheme is selectively secure.

3.2 Linear Two-Mode Identity Based Broadcast Encryption Template

We define a template for two-mode IBBE schemes that ensures that they give rise to selective secure non-monotonic KP-ABE schemes. We call this a linear

TIBBE template. Let $\mathbb{G}, \mathbb{G}_T$ be underlying bilinear groups of order p. The identity space of the scheme is $\mathcal{I} = \mathbb{Z}_p$. A linear TIBBE scheme is determined by parameters $n, n_1, n_2, \bar{n}_1, \in \mathbb{N}$, a distribution $\mathcal{G}$ on vectors of functions, and functions $\mathcal{D}^{\mathsf{IBBE}}$, $\mathcal{D}^{\mathsf{IBR}}$. $\mathcal{G}$'s output is tuple of functions $(f_1^{\mathsf{IBBE}}, f_2^{\mathsf{IBBE}}, f_1^{\mathsf{IBR}}, f_2^{\mathsf{IBR}}, F)$ where $f_1^{\mathsf{IBBE}} : \mathcal{I} \to \mathbb{G}, f_2^{\mathsf{IBBE}} : \mathcal{I} \to \mathbb{G}^{n_1}, f_1^{\mathsf{IBR}} : \mathcal{I} \to \mathbb{G}, f_2^{\mathsf{IBR}} : \mathcal{I} \to \mathbb{G}^{\bar{n}_1}, F : (\mathcal{I})^{\leq n-1} \times \mathbb{Z}_p \to \mathbb{G}^{\leq n_2}$. Here, we allow F to be probabilistic whereas all other functions are assumed to be deterministic. $\mathcal{D}^{\mathsf{IBBE}}$ and $\mathcal{D}^{\mathsf{IBR}}$ are functions such that $\mathcal{D}^{\mathsf{IBBE}} : \mathbb{G}^{n_1+1} \times \mathcal{I} \times \mathbb{G}^{n_2} \times \binom{\mathcal{I}}{<n} \to \mathbb{G}_T$, $\mathcal{D}^{\mathsf{IBR}} : \mathbb{G}^{\bar{n}_1+1} \times \mathcal{I} \times \mathbb{G}^{n_2} \times \binom{\mathcal{I}}{<n} \to \mathbb{G}_T$.

$\mathsf{Setup}(\lambda, n)$: Given a security parameter $\lambda \in \mathbb{N}$ and a bound $n \in \mathbb{Z}$ on the number of identities per ciphertext, the algorithm selects bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$ and a generator $g \xleftarrow{\$} \mathbb{G}$. It computes $e(g,g)^\alpha$ for a random $\alpha \xleftarrow{\$} \mathbb{Z}_p$ and chooses functions $(f_1^{\mathsf{IBBE}}, f_2^{\mathsf{IBBE}}, f_1^{\mathsf{IBR}}, f_2^{\mathsf{IBR}}, F) \xleftarrow{\$} \mathcal{G}$. The master secret key consists of $\mathsf{msk} = \alpha$ while the master public key is $\mathsf{mpk} = (g, e(g,g)^\alpha, \{f_1^{\mathsf{type}}, f_2^{\mathsf{type}}\}_{\mathsf{type} \in \{\mathsf{IBBE}, \mathsf{IBR}\}}, F, n, n_1, n_2, \bar{n}_1)$.

$\mathsf{KeyGen}(\mathsf{msk}, \mathsf{mpk}, (\mathsf{ID}, \mathsf{type}))$: To generate a private key for ID of type $\mathsf{type} \in \{\mathsf{IBBE}, \mathsf{IBR}\}$, it chooses $r \xleftarrow{\$} \mathbb{Z}_p$. Then, it computes the private key as

$$\mathsf{sk}_{(\mathsf{ID},\mathsf{type})} = (d_1, d_2) = \left(g^\alpha \cdot f_1^{\mathsf{type}}(\mathsf{ID})^r, f_2^{\mathsf{type}}(\mathsf{ID})^r\right).$$

$\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{M}, S)$: To encrypt $\mathsf{M} \in \mathbb{G}_T$ for a set of identities $S = (\mathsf{ID}_1, \ldots, \mathsf{ID}_k)$ where $k < n$, it chooses $s \xleftarrow{\$} \mathbb{Z}_p$ and computes the ciphertext as

$$C = (C_0, C_1) = (\mathsf{M} \cdot e(g,g)^{\alpha s}, F(\mathsf{ID}_1, \ldots, \mathsf{ID}_k, s)).$$

$\mathsf{Decrypt}(\mathsf{mpk}, C, S, \mathsf{sk}_{(\mathsf{ID},\mathsf{type})})$: It parses $\mathsf{sk}_{(\mathsf{ID},\mathsf{type})} = (d_1, d_2)$ and $C = (C_0, C_1)$ then runs

$$\mathcal{D}^{\mathsf{type}}\big((d_1, d_2), \mathsf{ID}, C_1, S\big) \to e(g,g)^{\alpha \cdot s},$$

and obtains $\mathsf{M} = C_0 / e(g,g)^\alpha$.

We also require that for all $(f_1^{\mathsf{IBBE}}, f_2^{\mathsf{IBBE}}, f_1^{\mathsf{IBR}}, f_2^{\mathsf{IBR}}, F) \xleftarrow{\$} \mathcal{G}$, the following property must hold. [2]

Correctness. For all $\alpha, r, s \in \mathbb{Z}_p$, randomness for F, $(\mathsf{ID}, \mathsf{type}) \in \mathcal{I} \times \{\mathsf{IBBE}, \mathsf{IBR}\}$, $S = \{\mathsf{ID}_1, \ldots, \mathsf{ID}_k\} \in \binom{\mathcal{I}}{<n}$ such that $(\mathsf{type} = \mathsf{IBBE} \wedge \mathsf{ID} \in S) \vee (\mathsf{type} = \mathsf{IBR} \wedge \mathsf{ID} \notin S)$ and randomness for F, we have

$$\mathcal{D}^{\mathsf{type}}\Big(\big(g^\alpha \cdot f_1^{\mathsf{type}}(\mathsf{ID})^r, f_2^{\mathsf{type}}(\mathsf{ID})^r\big), \mathsf{ID}, F(\mathsf{ID}_1, \ldots, \mathsf{ID}_k, s), S\Big) = e(g,g)^{\alpha \cdot s}.$$

3.3 Generic Conversion from Linear TIBBE to Non-monotonic KP-ABE

Let $\Pi_{\mathsf{TIBBE}} = (\mathsf{Setup}', \mathsf{Keygen}', \mathsf{Encrypt}', \mathsf{Decrypt}')$ be a linear TIBBE system. We construct a non-monotonic KP-ABE scheme from Π_{TIBBE} as follows.

$\mathsf{Setup}(\lambda, n)$: It simply outputs $\mathsf{Setup}'(\lambda, n) \to (\mathsf{mpk}, \mathsf{msk})$.

[2] In [3], the authors also assume a property called linearity. However, we do not need this property.

$\mathsf{KeyGen}(\mathsf{msk}, \mathsf{mpk}, \tilde{\mathbb{A}})$: The input to the algorithm is the master secret key msk, the master public key mpk, and a non-monotonic access structure $\tilde{\mathbb{A}}$ such that we have $\tilde{\mathbb{A}} = NM(\mathbb{A})$ for some monotonic access structure $\mathbb{A}$ over a set $\mathcal{P}$ of attributes and associated with a linear secret sharing scheme (L, π). Let L be an $\ell \times m$ matrix. First, it generates shares of α with (L, π). Namely, it chooses a vector $\mathbf{s} = (s_1, \ldots, s_m)$ such that $s_1 = \alpha$ and $s_2, \ldots, s_m \xleftarrow{\$} \mathbb{Z}_p$ and calculates $\lambda_i = \langle \mathbf{L}_i, \mathbf{s} \rangle$ for each $i = 1, \ldots, \ell$. The party corresponds to share λ_i is $\pi(i) = \breve{x}_i$, where x_i is underlying attribute, and can be primed (i.e., negated) or unprimed (non-negated). Then for each $i = 1, \ldots, \ell$, it picks $r_i \xleftarrow{\$} \mathbb{Z}_p$ and sets D_i for each $i = 1, \ldots, \ell$ as follows.

$$D_i = \begin{cases} \left(d'_{i,1} = g^{\lambda_i} \cdot f_1^{\mathsf{IBBE}}(x_i)^{r_i},\ d'_{i,2} = f_2^{\mathsf{IBBE}}(x_i)^{r_i}\right) & \text{if } \pi(i) = x_i \\ \left(d'_{i,1} = g^{\lambda_i} \cdot f_1^{\mathsf{IBR}}(x_i)^{r_i},\ d'_{i,2} = f_2^{\mathsf{IBR}}(x_i)^{r_i}\right) & \text{if } \pi(i) = x'_i. \end{cases}$$

It then outputs the private key as $\mathsf{sk}_{\tilde{\mathbb{A}}} = \{D_i\}_{i=1}^{\ell}$

$\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{M}, \omega)$: It simply outputs $\mathsf{Encrypt}'(\mathsf{mpk}, \mathsf{M}, \omega)$.

$\mathsf{Decrypt}(\mathsf{mpk}, C, \omega, \mathsf{sk}_{\tilde{\mathbb{A}}})$: Assume first that the policy $\tilde{\mathbb{A}}$ is satisfied by the attribute set ω, so that decryption is possible. Since $\tilde{\mathbb{A}} = NM(\mathbb{A})$ for some access structure $\mathbb{A}$ associated with a linear secret sharing scheme (L, π), we have $\omega' = N(\omega) \in \mathbb{A}$ and we let $I = \{i | \pi(i) \in \omega'\}$. Since ω' is authorized in $\mathbb{A}$, the receiver can efficiently compute reconstruction coefficients $\{(i, \mu_i)\}_{i \in I} = \mathsf{Recon}_{L,\pi}(\omega')$ such that $\sum_{i \in I} \mu_i \lambda_i = \alpha$. It parses $C = (C_0, C_1)$, $\mathsf{sk}_{\tilde{\mathbb{A}}} = \{D_i\}_{i=1}^{\ell}$ where $D_i = (d'_{i,1}, d'_{i,2})$ and computes $e(g,g)^{s \cdot \lambda_i}$ for each $i \in I$ as follows. (The correctness is shown later.)

$$\begin{cases} \mathcal{D}^{\mathsf{IBBE}}\big((d'_{i,1}, d'_{i,2}), x_i, C_1, \omega\big) \to e(g,g)^{s \cdot \lambda_i} & \text{if } \pi(i) = x_i \quad (1a) \\ \mathcal{D}^{\mathsf{IBR}}\big((d'_{i,1}, d'_{i,2}), x_i, C_1, \omega\big) \to e(g,g)^{s \cdot \lambda_i} & \text{if } \pi(i) = x'_i. \quad (1b) \end{cases}$$

Finally, it recovers message by $C_0 \cdot \prod_{i \in I} \big(e(g,g)^{s \cdot \lambda_i}\big)^{-\mu_i} = \mathsf{M}$.

Correctness. We now verify that equations (1a) and (1b) are correct. (1a) and (1b) follow from the correctness of the underlying TIBBE scheme by seeing D_i as a private key for $\big(\mathsf{ID} = x_i, \mathsf{type} \in \{\mathsf{IBBE}, \mathsf{IBR}\}\big)$ that is derived from $\mathsf{msk} = \lambda_i$ using randomness r_i. The security of the resulting scheme is established by the following Theorem. The proof is similar to that of Theorem 1 in [3] and can be found in full version of this paper.

Theorem 1. *If the underlying TIBBE scheme is selectively secure, then the resulting KP-ABE system above is also selectively secure.*

Remark. We have described the conversion for TIBBE scheme with a restriction that the number of identities per ciphertext is bounded by n. However, the same conversion also applies to a TIBBE scheme without such a restriction. In particular, we can apply the above conversion to our TIBBE scheme in Sec. 6.

4 TIPE Scheme with Compact Ciphertexts

In this section, we propose a TIPE scheme with compact ciphertext size. As we explained in Sec. 3.1, we can obtain a TIBBE scheme from the TIPE scheme. By applying the conversion in Sec. 3 to this TIBBE scheme, we obtain a new non-monotonic KP-ABE scheme with very short ciphertexts. The ciphertext overhead is 33% shorter than the non-monotonic KP-ABE ciphertext in [3] (the shortest in the literature). It also reduces the number of pairing operations in the decryption algorithm from 3 to 2. The public key size of our scheme is about half that of the existing scheme, but the private key of our scheme is slightly longer.

$\mathsf{Setup}(\lambda, n)$: It chooses bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$ with $g \xleftarrow{\$} \mathbb{G}$. It also picks $v, \alpha \xleftarrow{\$} \mathbb{Z}_p$ and $\mathbf{u} = (u_1, \ldots, u_n) \xleftarrow{\$} \mathbb{Z}_p^n$. Then it sets $V = g^v$ and $U = (U_1, \ldots, U_n) = g^{\mathbf{u}}$. It finally outputs the master public key $\mathsf{mpk} = (g, U_1, \ldots, U_n, V, e(g,g)^\alpha)$ and the master secret key $\mathsf{msk} = \alpha$.

$\mathsf{KeyGen}(\mathsf{msk}, \mathsf{mpk}, (\mathbf{x}, \mathsf{type}))$: To generate a private key for $\big(\mathbf{x} = (x_1 \neq 0, \ldots, x_n) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^{n-1}, \mathsf{type} \in \{\mathsf{ZIPE}, \mathsf{NIPE}\}\big)$, it chooses $r \xleftarrow{\$} \mathbb{Z}_p$ and computes

$$\begin{cases} \mathsf{sk}_{(\mathbf{x},\mathsf{ZIPE})} = \left(\begin{array}{c} D_1 = g^\alpha V^r, \quad D_2 = g^r, \\ \{K_i = (U_1^{-\frac{x_i}{x_1}} U_i)^r\}_{i=2}^n \end{array} \right) & \text{if } \mathsf{type} = \mathsf{ZIPE} \\ \mathsf{sk}_{(\mathbf{x},\mathsf{NIPE})} = \left(\begin{array}{c} D_1 = g^\alpha U_1^r, \quad D_2 = g^r, \quad D_3 = V^r, \\ \{K_i = (U_1^{-\frac{x_i}{x_1}} U_i)^r\}_{i=2}^n \end{array} \right) & \text{if } \mathsf{type} = \mathsf{NIPE}. \end{cases}$$

$\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{M}, \mathbf{y})$: To encrypt $\mathsf{M} \in \mathbb{G}_T$ for the vector $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_p^n$, it picks $s \xleftarrow{\$} \mathbb{Z}_p$ and computes the ciphertext as

$$C = \Big(C_0 = \mathsf{M} \cdot e(g,g)^{\alpha s}, C_1 = g^s, C_2 = (V U_1^{y_1} \cdots U_n^{y_n})^{-s}\Big).$$

$\mathsf{Decrypt}(\mathsf{mpk}, C, \mathbf{y}, \mathsf{sk}_{(\mathbf{x},\mathsf{type})})$: It computes

$$\begin{cases} e(C_1, D_1 \cdot \prod_{i=2}^n K_i^{y_i}) \cdot e(C_2, D_2) = e(g,g)^{s\alpha} & \text{if } \mathsf{type} = \mathsf{ZIPE} \\ e(C_1, D_1) \cdot \Big(e(C_1, D_3 \prod_{i=2}^n K_i^{y_i}) \cdot e(C_2, D_2)\Big)^{\frac{x_1}{\langle \mathbf{x}, \mathbf{y} \rangle}} = e(g,g)^{s\alpha} & \text{if } \mathsf{type} = \mathsf{NIPE} \end{cases}$$

and recovers the message by $C_0 / e(g,g)^{s\alpha} = \mathsf{M}$.

We construct the above scheme by combining the IPE scheme derived from the spatial encryption scheme in [8,2] and a variant of the NIPE scheme proposed in [3] so that they share the master public key and the ciphertext. The non-monotonic KP-ABE scheme derived from the above TIPE scheme has compact parameters, because of this share of parameters. The main technical challenge in the proof of the security of the scheme is to simulate the key generation oracle for two different types (i.e., ZIPE and NIPE) of keys *simultaneously*. To achieve this, we use a significantly different strategy to simulate NIPE keys than the security proof in [3]. The following theorem addresses the security of the scheme.

Theorem 2. *The above TIPE scheme is selectively secure under the n-DBDHE assumption.*

Before proving the theorem, we recall following lemma that is implicit in [8].

Lemma 1. *([8]) Let $\mathbb{G}$ be a multiplicative group with prime order p and g be its generator. Let n, m be some integer bounded by polynomial of λ, $\mathbf{a}$ be $\mathbf{a} = (a, a^2, \ldots, a^n) \in \mathbb{Z}_p^n$, $\tilde{\alpha}, \{w_i\}_{i=0}^m$ be elements in $\mathbb{Z}_p$, $\{\mathbf{z}_i\}_{i=0}^m$ be vectors in $\mathbb{Z}_p^n$. We also assume that $\mathbf{h} = (h_1, \ldots, h_n) \in \mathbb{Z}_p^n$ satisfies $\langle \mathbf{h}, \mathbf{z}_0 \rangle \neq 0$ and $\langle \mathbf{h}, \mathbf{z}_i \rangle = 0$ for $i \in [m]$. Then, there exists an PPT BHSim which takes $(\tilde{\alpha}, \{\mathbf{z}_i\}_{i=0}^m, \{w_i\}_{i=0}^m, \mathbf{h}, \{g^{a^i}\}_{i \in [2n] \setminus \{n+1\}})$ as input and outputs $(g^{a^{n+1}+\tilde{\alpha}} \cdot (g^{\langle \mathbf{z}_0, \mathbf{a} \rangle + w_0})^r, \{(g^{\langle \mathbf{z}_i, \mathbf{a} \rangle + w_i})^r\}_{i=1}^m)$ where $r \xleftarrow{\$} \mathbb{Z}_p$.*

Proof. (of Theorem 2.) We construct $\mathcal{B}$ that decides if $T = e(g,g)^{a^{n+1}s}$ given $(g, \{g^{a^i}\}_{i \in [2n] \setminus \{n+1\}}, g^s, T) \in \mathbb{G}^{2n+1} \times \mathbb{G}_T$ by using the selective adversary $\mathcal{A}$ against our scheme. We denote by $\mathbf{a}$ a vector $(a, a^2, \ldots, a^n)$.

Setup of Master Public Key. At the outset of the game, the adversary $\mathcal{A}$ declares the challenge vector $\mathbf{y}^\star = (y_1^\star, \ldots, y_n^\star) \in \mathbb{Z}_p^n$. $\mathcal{B}$ picks $\tilde{\alpha}, \tilde{v} \xleftarrow{\$} \mathbb{Z}_p$, $\tilde{\mathbf{u}} = (\tilde{u}_1, \ldots, \tilde{u}_n) \xleftarrow{\$} \mathbb{Z}_p^n$ and sets mpk as

$$\mathsf{mpk} = \big(g = g, e(g,g)^\alpha = e(g^a, g^{a^n}) \cdot e(g,g)^{\tilde{\alpha}}, \mathbf{U} = g^{\mathbf{a}} \cdot g^{\tilde{\mathbf{u}}}, V = g^{-\langle \mathbf{a}, \mathbf{y}^\star \rangle} \cdot g^{\tilde{v}}\big),$$

and gives it to $\mathcal{A}$. Here, we implicitly set $\alpha = \tilde{\alpha} + a^{n+1}$, $\mathbf{u} = \mathbf{a} + \tilde{\mathbf{u}}$, and $v = -\langle \mathbf{a}, \mathbf{y}^\star \rangle + \tilde{v}$.

Phase1 and 2. When $\mathcal{A}$ queries private key for $(\mathbf{x} = (x_1, \ldots, x_n), \mathsf{type}) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^{n-1} \times \{\mathsf{ZIPE}, \mathsf{NIPE}\}$, $\mathcal{B}$ answers as follows.

- If $\mathsf{type} = \mathsf{ZIPE}$, we have $\langle \mathbf{x}, \mathbf{y}^\star \rangle \neq 0$. In this case, $\mathcal{B}$ first sets $\mathbf{z}_0 = -\mathbf{y}^\star, \mathbf{z}_1 = \mathbf{0}, \mathbf{z}_i = -\frac{x_i}{x_1}\mathbf{e}_1 + \mathbf{e}_i$ for $i = 2, \ldots, n$, $w_0 = \tilde{v}, w_1 = 1$, and $w_i = -\frac{x_i}{x_1}\tilde{u}_1 + \tilde{u}_i$ for $i = 2, \ldots, n$. Then $\mathcal{B}$ runs $\mathsf{BHSim}(\tilde{\alpha}, \{\mathbf{z}_i\}_{i=0}^n, \{w_i\}_{i=0}^n, \mathbf{x}, \{g^{a^i}\}_{i \in [2n] \setminus \{n+1\}}) \to (Z_0, \{Z_i\}_{i=1}^n)$ and returns $(D_1, D_2, \{K_i\}_{i=2}^n) = (Z_0, Z_1, \{Z_i\}_{i=2}^n)$. We claim that $(D_1, D_2, \{K_i\}_{i=2}^n)$ is distributed the same as real private key. At first, we check that the input to BHSim is in a valid form. To see this, it suffices to check that $\langle \mathbf{x}, \mathbf{z}_0 \rangle = \langle \mathbf{x}, -\mathbf{y}^\star \rangle \neq 0$, $\langle \mathbf{x}, \mathbf{z}_1 \rangle = \langle \mathbf{x}, \mathbf{0} \rangle = 0$, and $\langle \mathbf{x}, \mathbf{z}_i \rangle = \langle \mathbf{x}, -\frac{x_i}{x_1}\mathbf{e}_1 + \mathbf{e}_i \rangle = -x_1 \cdot \frac{x_i}{x_1} + x_i = 0$ for $i = 2, \ldots, n$. Since the input to BHSim is in a valid form, $D_1 = Z_0 = g^{\tilde{\alpha} + a^{n+1}}(g^{-\langle \mathbf{a}, \mathbf{y}^\star \rangle} \cdot g^{\tilde{v}})^r = g^\alpha V^r$, $D_2 = Z_1 = (g^{\langle \mathbf{0}, \mathbf{a} \rangle + 1})^r = g^r$, and

$$K_i = Z_i = (g^{\langle -\frac{x_i}{x_1}\mathbf{e}_1 + \mathbf{e}_i, \mathbf{a} \rangle - \frac{x_i}{x_1}\tilde{u}_1 + \tilde{u}_i})^r = (g^{-\frac{x_i}{x_1}(a + \tilde{u}_1)} \cdot g^{a^i + \tilde{u}_i})^r = (U_1^{-\frac{x_i}{x_1}} \cdot U_i)^r$$

  for $i \in \{2, \ldots, n\}$ where $r \xleftarrow{\$} \mathbb{Z}_p$ as desired.
- If $\mathsf{type} = \mathsf{NIPE}$, we have $\langle \mathbf{x}, \mathbf{y}^\star \rangle = 0$. In this case, $\mathcal{B}$ first sets $\mathbf{z}_0 = \mathbf{e}_1, \mathbf{z}_1 = \mathbf{0}, \mathbf{z}_i = -\frac{x_i}{x_1}\mathbf{e}_1 + \mathbf{e}_i$ for $i = 2, \ldots, n$, $\mathbf{z}_{n+1} = -\mathbf{y}^\star$, $w_0 = \tilde{u}_1, w_1 = 1$, $w_i = -\frac{x_i}{x_1}\tilde{u}_1 + \tilde{u}_i$ for $i = 2, \ldots, n$, and $w_{n+1} = \tilde{v}$. Then $\mathcal{B}$ runs $\mathsf{BHSim}(\tilde{\alpha}, \{\mathbf{z}_i\}_{i=0}^{n+1}, \{w_i\}_{i=0}^{n+1}, \mathbf{x}, \{g^{a^i}\}_{i \in [2n] \setminus \{n+1\}}) \to (Z_0, \{Z_i\}_{i=1}^{n+1})$ and returns $(D_1, D_2, D_3, \{K_i\}_{i=2}^n) = (Z_0, Z_1, Z_{n+1}, \{Z_i\}_{i=2}^n)$. We claim that $(D_1, D_2, D_3, \{K_i\}_{i=2}^n)$ is

distributed the same as real private key. At first, we check that the input to BHSim is in a valid form. To see this, it suffices to check that $\langle \mathbf{x}, \mathbf{z}_0 \rangle = \langle \mathbf{x}, \mathbf{e}_1 \rangle = x_1 \neq 0$, $\langle \mathbf{x}, \mathbf{z}_1 \rangle = \langle \mathbf{x}, \mathbf{0} \rangle = 0$, $\langle \mathbf{x}, \mathbf{z}_i \rangle = \langle \mathbf{x}, -\frac{x_i}{x_1}\mathbf{e}_1 + \mathbf{e}_i \rangle = 0$ for $i = 2, \ldots, n$, and $\langle \mathbf{x}, \mathbf{z}_{n+1} \rangle = \langle \mathbf{x}, -\mathbf{y}^\star \rangle = 0$. Since the input to BHSim is in a valid form, we have

$$D_1 = Z_0 = g^{\tilde{\alpha}+a^{n+1}} \cdot (g^{\langle \mathbf{a}, \mathbf{e}_1 \rangle} \cdot g^{\tilde{u}_1})^r = g^{\alpha} \cdot (g^{a+\tilde{u}_1})^r = g^{\alpha} U_1^r$$

where $r \xleftarrow{\$} \mathbb{Z}_p$. We can also check that $D_2 = g^r$ and $\{K_i\}_{i=2}^n = \{(U_1^{-\frac{x_i}{x_1}} \cdot U_i)^r\}_{i=2}^n$ by exactly the same computation as in the case of $\mathsf{type} = \mathsf{ZIPE}$. Finally, we have that $D_3 = Z_{n+1} = (g^{-\langle \mathbf{a}, \mathbf{y}^\star \rangle + \tilde{v}})^r = V^r$ as desired.

Challenge. At some point in the game, $\mathcal{A}$ submits a pair of ciphertexts $(\mathsf{M}_0, \mathsf{M}_1)$ to $\mathcal{B}$. $\mathcal{B}$ flips a random coin $\beta \xleftarrow{\$} \{0,1\}$ and returns $(C_0, C_1, C_2) = (\mathsf{M}_\beta \cdot e(g^s, g^{\tilde{\alpha}}) \cdot T, g^s, (g^s)^{-(\langle \mathbf{y}^\star, \tilde{\mathbf{u}} \rangle + \tilde{v})})$ to $\mathcal{A}$. Since

$$(g^s)^{-(\langle \mathbf{y}^\star, \tilde{\mathbf{u}} \rangle + \tilde{v})} = (g^{\langle -\mathbf{a}, \mathbf{y}^\star \rangle + \tilde{v}} \cdot g^{\langle \mathbf{a}+\tilde{\mathbf{u}}, \mathbf{y}^\star \rangle})^{-s} = (V U_1^{y_1^\star} \cdots U_n^{y^\star})^{-s}$$

and $e(g^s, g^{\tilde{\alpha}}) \cdot e(g,g)^{a^{n+1}s} = e(g,g)^{s\alpha}$, the ciphertext is in a valid form if $T = e(g,g)^{a^{n+1}s}$.

Guess. Finally, $\mathcal{A}$ outputs its guess β' for β. If $\beta' = \beta$, $\mathcal{A}$ outputs 1 for its guess. Otherwise, it outputs 0. If $T = e(g,g)^{sa^{n+1}}$, the above simulation is perfect and thus $\mathcal{A}$ has non-negligible advantage. On the other hand, If T is a random element in $\mathbb{G}_T$, $\mathcal{A}$'s advantage is 0. Therefore, if $\mathcal{A}$ breaks our scheme with non-negligible advantage, $\mathcal{B}$ has a non-negligible advantage against the n-DBDHE assumption.

5 TIPE Scheme from the DBDH Assumption

In this section, we propose a TIPE scheme from the DBDH assumption, which is one of the weakest assumptions in bilinear groups. By sequentially applying the conversions from TIPE to TIBBE in Sec. 3.1 and from TIBBE to non-monotonic KP-ABE in Sec. 3 to the scheme, we obtain a new non-monotonic KP-ABE scheme from the DBDH assumption. Compared to the Non-monotonic KP-ABE scheme from the same assumption in [28], the public key and ciphertext size of our scheme are approximately half the size of theirs, and the private key size is comparable.

$\mathsf{Setup}(\lambda, n)$: It chooses bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$ with $g \xleftarrow{\$} \mathbb{G}$. It also picks $u, \alpha \xleftarrow{\$} \mathbb{Z}_p$ and $\mathbf{v} = (v_1, \ldots, v_n) \xleftarrow{\$} \mathbb{Z}_p^n$. Then it sets $U = g^u$ and $\mathbf{V} = (V_1, \ldots, V_n) = g^{\mathbf{v}}$. It finally outputs the master public key $\mathsf{mpk} = (g, U, V_1, \ldots, V_n, e(g,g)^\alpha)$ and the master secret key $\mathsf{msk} = \alpha$.

$\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{M}, \mathbf{y})$: To encrypt $\mathsf{M} \in \mathbb{G}_T$ for the vector $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_p^n$, it picks $s \xleftarrow{\$} \mathbb{Z}_p$ and computes the ciphertext as

$$C = \Big(C_0 = \mathsf{M} \cdot e(g,g)^{\alpha s}, C_1 = g^s, \{E_i = (U^{y_i} V_i)^{-s}\}_{i=1,\ldots n}\Big).$$

$\mathsf{KeyGen}(\mathsf{msk}, \mathsf{mpk}, (\mathbf{x}, \mathsf{type}))$: To generate a private key for $\big(\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n, \mathsf{type} \in \{\mathsf{ZIPE}, \mathsf{NIPE}\}\big)$, it chooses $r \xleftarrow{\$} \mathbb{Z}_p$ and computes

$$\begin{cases} \mathsf{sk}_{(\mathbf{x},\mathsf{ZIPE})} = \left(D_1 = g^{\alpha} \cdot (V_1^{x_1} \cdots V_n^{x_n})^r, D_2 = g^r\right) & \text{if } \mathsf{type} = \mathsf{ZIPE} \\ \mathsf{sk}_{(\mathbf{x},\mathsf{NIPE})} = \left(D_1 = g^{\alpha} U^r, D_2 = (V_1^{x_1} \cdots V_n^{x_n})^r, D_3 = g^r\right) & \text{if } \mathsf{type} = \mathsf{NIPE}. \end{cases}$$

$\mathsf{Decrypt}(\mathsf{mpk}, C, \mathbf{y}, \mathsf{sk}_{(\mathbf{x},\mathsf{type})})$: It computes

$$\begin{cases} e(C_1, D_1) \cdot e(\prod_{i=1}^{n} E_i^{x_i}, D_2) = e(g,g)^{s\alpha} & \text{if } \mathsf{type} = \mathsf{ZIPE} \\ e(C_1, D_1) \cdot \left(e(\prod_{i=1}^{n} E_i^{x_i}, D_3) \cdot e(C_1, D_2)\right)^{\frac{1}{\langle \mathbf{x},\mathbf{y} \rangle}} = e(g,g)^{s\alpha} & \text{if } \mathsf{type} = \mathsf{NIPE} \end{cases}$$

and recovers the message by $C_0 / e(g,g)^{s\alpha} = \mathsf{M}$.

The following theorem addresses the security of the scheme. The proof will be found in the full version of this paper.

Theorem 3. *The above TIPE scheme is selectively secure under the DBDH assumption.*

6 Unbounded TIBBE Scheme

In the TIBBE schemes derived from the TIPE schemes in Sec. 4 and 5, the number of identities per ciphertext is bounded by a parameter n. In this section, we propose a TIBBE scheme without such a restriction. The structure of the construction can be seen as a combination of the IBBE scheme implicit in KP-ABE scheme in [30] and the IBR scheme in [21]. By applying the conversion in Sec. 3 to the scheme, we obtain the first non-monotonic KP-ABE scheme in the standard model that does not restrict the number of attributes per ciphertext or the number of times the same attribute can be used in an access formula associated with a private key.

$\mathsf{Setup}(\lambda)$: It chooses bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^{\lambda}$ with $g \xleftarrow{\$} \mathbb{G}$. It also picks $H, U, V, W \xleftarrow{\$} \mathbb{G}$ and $b, \alpha \xleftarrow{\$} \mathbb{Z}_p^n$. Then it sets $B = g^b, B' = g^{b^2}, V' = V^b$. It finally outputs the master public key $\mathsf{mpk} = (g, H, U, W, B, B', V, V', e(g,g)^{\alpha})$ and the master secret key $\mathsf{msk} = \alpha$.

$\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{M}, S)$: To encrypt $\mathsf{M} \in \mathbb{G}_T$ for the set of identities $S = (\mathsf{ID}_1, \ldots, \mathsf{ID}_k) \subset \mathbb{Z}_p$, it chooses $s, t_1, \ldots, t_k \xleftarrow{\$} \mathbb{Z}_p$ and random $s_1, \ldots, s_k \in \mathbb{Z}_p$ such that $s_1 + \ldots + s_k = s$ and computes the ciphertext as $C =$

$$\left(C_0 = \mathsf{M} \cdot e(g,g)^{\alpha s}, C_1 = g^s, \left\{ \begin{array}{l} C_{i,1} = W^{-s} (U^{\mathsf{ID}_i} H)^{-t_i}, C_{i,2} = g^{t_i} \\ C'_{i,1} = (B'^{\mathsf{ID}_i} V')^{-s_i}, C'_{i,2} = B^{s_i} \end{array} \right\}_{i \in [k]} \right).$$

$\mathsf{KeyGen}(\mathsf{msk}, \mathsf{mpk}, (\mathsf{ID}, \mathsf{type}))$: To generate a private key for $\mathsf{ID} \in \mathbb{Z}_p$, it chooses $r \xleftarrow{\$} \mathbb{Z}_p$ and computes the private key as

$$\begin{cases} \mathsf{sk}_{(\mathsf{ID},\mathsf{IBBE})} = \left(D_1 = g^{\alpha} \cdot W^r, D_2 = (U^{\mathsf{ID}} H)^r, D_3 = g^r\right) & \text{if } \mathsf{type} = \mathsf{IBBE} \\ \mathsf{sk}_{(\mathsf{ID},\mathsf{IBR})} = \left(D_1 = g^{\alpha} \cdot (B')^r, D_2 = (B^{\mathsf{ID}} V)^r, D_3 = g^r\right) & \text{if } \mathsf{type} = \mathsf{IBR}. \end{cases}$$

$\mathsf{Decrypt}(\mathsf{mpk}, C, S, \mathsf{sk}_{(\mathsf{ID},\mathsf{type})})$: We assume that in the case of $\mathsf{type} = \mathsf{IBBE}$, ID is contained in $\mathsf{ID} \in S = \{\mathsf{ID}_1, \ldots, \mathsf{ID}_k\}$, so that decryption is possible. Therefore, there is an $\tau \in [k]$ such that $\mathsf{ID} = \mathsf{ID}_\tau$. It computes

$$\begin{cases} e(C_1, D_1) \cdot e(C_{\tau,1}, D_3) \cdot e(C_{\tau,2}, D_2) = e(g,g)^{s\alpha} & \text{if } \mathsf{type} = \mathsf{IBBE} \\ e(C_1, D_1) \cdot \prod_{i=1}^{k} \left(e(C'_{i,1}, D_3) \cdot e(C'_{i,2}, D_2)\right)^{\frac{1}{(\mathsf{ID}_i - \mathsf{ID})}} = e(g,g)^{s\alpha} & \text{if } \mathsf{type} = \mathsf{IBR} \end{cases}$$

and recovers the message by $C_0/e(g,g)^{s\alpha} = \mathsf{M}$.

We can prove selective security of the scheme under the new assumption that we call n-(A) assumption which is secure in the generic group model. The definition of the assumption and the proof will appear in the full version of this paper.

7 Unbounded Non-monotonic CP-ABE Scheme

In this section, we propose the first non-monotonic CP-ABE scheme that does not restrict the size of the attributes set or the number of times the same attribute can be used in an access formula. Our starting point for the construction of the scheme is the unbounded (monotonic) CP-ABE scheme in [30]. To support the non-monotonic access structure, we first construct a suitable revocation mechanism, which can be seen as a ciphertext-policy version of the IBR scheme in [21]. Then, we combine this with the CP-ABE scheme in [30] to obtain our new scheme. Because some parameters are shared between the two schemes, the public key of our scheme is only one group element longer than that of the scheme in [30], while our scheme supports a more general access structure.

$\mathsf{Setup}(\lambda)$: It chooses bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$ with $g \xleftarrow{\$} \mathbb{G}$. It also picks $b, \alpha \xleftarrow{\$} \mathbb{Z}_p$ and $H, U, V, W \xleftarrow{\$} \mathbb{G}$. Then it sets $V' = U^b$ and outputs the master public key $\mathsf{mpk} = (g, H, U, V, V', W, e(g,g)^\alpha)$ and the master secret key $\mathsf{msk} = (\alpha, b)$.

$\mathsf{KeyGen}(\mathsf{msk}, \mathsf{mpk}, \omega)$: To generate a private key for a set of attributes $\omega = \{\omega_1, \ldots \omega_k\} \subset \mathbb{Z}_p$, it chooses $r, r_1, \ldots, r_k \xleftarrow{\$} \mathbb{Z}_p$ and random $r'_1, \ldots, r'_k \in \mathbb{Z}_p$ such that $r'_1 + \ldots + r'_k = r$. It then outputs the private key as

$$\mathsf{sk}_\omega = \left(D_1 = g^\alpha W^r, D_2 = g^r, \left\{ \begin{array}{ll} K_{i,1} = V^{-r}(U^{\omega_i} H)^{r_i}, & K_{i,2} = g^{r_i} \\ K'_{i,1} = (U^{b\omega_i} H^b)^{r'_i}, & K'_{i,2} = g^{br'_i} \end{array} \right\}_{i \in [k]} \right).$$

$\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{M}, \tilde{\mathbb{A}})$: The input to the algorithm is the master public key mpk, the message $\mathsf{M} \in \mathbb{G}_T$ and a non-monotonic access structure $\tilde{\mathbb{A}}$ such that we have $\tilde{\mathbb{A}} = NM(\mathbb{A})$ for some monotonic access structure $\mathbb{A}$ over a set $\mathcal{P}$ of attributes and associated with a linear secret sharing scheme (L, π). Let L be an $\ell \times m$ matrix. First, it picks random $\mathbf{s} = (s, s_2, \ldots, s_m) \xleftarrow{\$} \mathbb{Z}_p^m$ and computes share of s for $\pi(i)$ by $\lambda_i = \langle \mathbf{L}_i \cdot \mathbf{s} \rangle$ for $i = 1, \ldots, \ell$. It then

computes $C_0 = \mathsf{M} \cdot e(g,g)^{\alpha \cdot s}$, $C_1 = g^s$. It also computes $(C_{i,1}, C_{i,2}, C_{i,3})$ for every $i = 1, \ldots, \ell$ as follows.

$$\begin{cases} C_{i,1} = W^{\lambda_i} V^{t_i},\ C_{i,2} = (U^{x_i} H)^{-t_i},\ C_{i,3} = g^{t_i} & \text{if } \pi(i) = x_i \\ C_{i,1} = W^{\lambda_i} (V')^{t_i},\ C_{i,2} = (U^{x_i} H)^{-t_i},\ C_{i,3} = g^{t_i} & \text{if } \pi(i) = x'_i \end{cases}$$

where $t_i \xleftarrow{\$} \mathbb{Z}_p$. The final output is $C = (C_0, C_1, \{C_{i,1}, C_{i,2}, C_{i,3}\}_{i \in [\ell]})$.

$\mathsf{Decrypt}(\mathsf{mpk}, C, \omega, \mathsf{sk}_{\tilde{\mathbb{A}}})$: Assume first that the policy $\tilde{\mathbb{A}}$ is satisfied by the attribute set ω, so that decryption is possible. Since $\tilde{\mathbb{A}} = NM(\mathbb{A})$ for some access structure $\mathbb{A}$ associated with a linear secret sharing scheme (L, π), we have $\omega' = N(\omega) \in \mathbb{A}$ and we let $I = \{i | \pi(i) \in \omega'\}$. Since ω' is authorized in $\mathbb{A}$, the receiver can efficiently compute reconstruction coefficients $\{(i, \mu_i)\}_{i \in I} = \mathsf{Recon}_{L,\pi}(\omega')$ such that $\sum_{i \in I} \mu_i \lambda_i = s$. It parses $C = (C_0, C_1, \{C_{i,1}, C_{i,2}, C_{i,3}\}_{i \in [\ell]})$, $\mathsf{sk}_\omega = \big(D_1, D_2, \{K_{i,1}, K_{i,2}, K'_{i,1}, K'_{i,2}\}_{i \in [k]}\big)$ and computes $e(g,g)^{r \cdot \lambda_i}$ for each $i \in I$ as

$$\begin{cases} e(C_{i,1}, D_2) \cdot e(C_{i,2}, K_{\tau,2}) \cdot e(C_{i,3}, K_{\tau,1}) \to e(g,W)^{r\lambda_i} & \text{if } \pi(i) = x_i \\ e(C_{i,1}, D_2) \cdot \prod_{j \in [k]} \big(e(C_{i,3}, K'_{j,1}) \cdot e(C_{i,2}, K'_{j,2})\big)^{\frac{1}{x_i - \omega_j}} = e(g,W)^{r\lambda_i} & \text{if } \pi(i) = x'_i \end{cases}$$

where τ is the index such that $\omega_\tau = x_i$. Such τ exists if $i \in I$ and $\pi(i)$ is non-negated attribute. Next, it computes $e(C_1, D_1) \cdot \prod_{i \in I} \big(e(g,W)^{r\lambda_i}\big)^{-\mu_i} = e(g^s, g^\alpha) e(g,W)^{sr} e(g,W)^{-r \sum_{i \in I} \mu_i \lambda_i} = e(g,g)^{\alpha \cdot s}$. Finally, it recovers the message by $C_0 / e(g,g)^{s\alpha} = \mathsf{M}$.

We can prove selective security of the scheme under the new assumption that we call n-(B) assumption which is secure in the generic group model. The definition of the assumption and the proof will appear in the full version of this paper.

8 Comparisons

Here, we compare our schemes with existing schemes. In Table 1, we compare non-monotonic KP-ABE schemes with compact ciphertexts. In Table 2, we compare non-monotonic KP-ABE schemes from the DBDH assumption. In Table 3 (resp., 4), we compare the KP (resp., CP)-ABE schemes which allow unbounded size for set of attributes associated with ciphertext (resp., private key). In these tables, $\bar{n} = |\text{attribute set}| = |\omega|$, n is the maximum bound of $\bar{n}$ (i.e., $|\omega| < n$), φ is the number of allowed repetition of the same attributes which appear in a policy, and t_1 and t_2 are the number of non-negated and negated attributes that apper in an access policy. We also let $t = t_1 + t_2$. The terms "reg-exp." and "mult-exp." refer to regular and multi-exponentiation in $\mathbb{G}$ and $\mathbb{G}_T$. The Pippenger algorithm [29] can efficiently compute the latter. The term "pair" refers to pairing computation. The columun "unbounded set" in Table 3 (resp., 4) states whether unbounded attribute set size is allowed for ciphertext (resp., for key) or

not. The columun "unbounded multi-use" states whether unboudned reuse of the same policy for a key (resp., ciphertext) is allowed or not.

In Table 2, we only highlight the encryption cost. As for the efficiency of the decryption algorithm, our scheme in Sec. 5 is somewhat slower than [28], because of the additional exponentiations. Note that the schemes in [27] achieve adaptive security, whereas all the other schemes achieve only selective security.

Table 1. Comparison of non-monotonic KP-ABE with compact ciphertexts

Schemes	Master public key size ($\lvert\mathbb{G}\rvert, \lvert\mathbb{G}_T\rvert$)	Ciphertext overhead $\lvert\mathbb{G}\rvert$	Private key size $\lvert\mathbb{G}\rvert$	Computational cost for encryption (reg,mult)-exp	decryption (pair,mult-exp)	Assumption
ALP [3]	$(2n+2, 1)$	3	$(n+1)t$	$(2, 2)$	$(3, 3^*)$	n-DBDHE
Ours in Sec. 4.	$(n+2, 1)$	2	$(n+1)t + t_2$	$(2, 1)$	$(2, 2^*)$	n-DBDHE

* These multi-exponentiation is heavier than that needed in the encryption algorithm.

Table 2. Comparison of non-monotonic KP-ABE schemes from the DBDH

Schemes	Master public key size ($\lvert\mathbb{G}\rvert, \lvert\mathbb{G}_T\rvert$)	Ciphertext overhead $\lvert\mathbb{G}\rvert$	Private key size $\lvert\mathbb{G}\rvert$	Encryption cost reg-exp.	mult-exp.
OSW [28]	$(2n+2, 0)$	$2n-1$	$2t_1 + 3t_2$	2	$2n^{\ddagger}$
Ours in Sec. 5	$(n+2, 1)$	$n+1$	$2t_1 + 3t_2$	2	n

† For simplicity, we compare these schemes in a most basic form. However, we can modify the schemes so that the ciphertext size only depends on $\bar{n}$ instead of n, which might be preferable in many case, by the technique in [28]. As a result, master public key and the private key becomes larger, whereas it makes ciphertext size smaller and encryption/decryption cost lower.

‡ These multi-exponentiations are heavier than that of our scheme in Sec. 5.

Table 3. Comparison of KP-ABE schemes with unbounded attribute set size

Schemes	Access structure	Ciphertext overhead ($\lvert\mathbb{G}\rvert$)	unbounded set	Private key size($\mathbb{G}$)	unbounded multi-use	Assumption
LSW[21]	non-monotone	$3\bar{n}+1$	Yes	$2t + t_2$	Yes	RO+n-MEBDH
OT[27]	non-monotone	$14\bar{n}\varphi + 5$	Yes	$14t + 5$	No	DLIN
RW[30]	monotone	$2\bar{n} + 1$	Yes	$3t_1$	Yes	n-1assumption
LW[23]	monotone	$3\bar{n} + 1$	Yes	$4t_1$	Yes	assumption 1-4
Ours in Sec. 6	non-monotone	$4\bar{n} + 1$	Yes	$3t$	Yes	n-(A) assumption

§ LW scheme [23] is constructed in composite order group.

Table 4. Comparison of CP-ABE schemes with unbounded attribute set size

Schemes	Access structure	Ciphertext overhead ($\lvert\mathbb{G}\rvert$)	unbounded multi-use	Private key size($\mathbb{G}$)	unbounded set	Assumption
OT[27]	non-monotone	$14t + 5$	No	$14\bar{n}\varphi + 5$	Yes	DLIN
RW[30]	monotone	$3t_1 + 1$	Yes	$2\bar{n} + 2$	Yes	n-2 assumption
Ours in Sec. 7	non-monotone	$3t + 1$	Yes	$4\bar{n} + 2$	Yes	n-(B) assumption

Acknowledgement. We thank Yannis Rouselakis, Brent Waters, anonymous reviewers of PKC 2014, and members of Shin-Akarui-Angou-Benkyoukai for their helpful discussions and comments.

References

1. Attrapadung, N., Imai, H.: Conjunctive broadcast and attribute-based encryption. In: Shacham, H., Waters, B. (eds.) Pairing 2009. LNCS, vol. 5671, pp. 248–265. Springer, Heidelberg (2009)
2. Attrapadung, N., Libert, B.: Functional encryption for inner product: Achieving constant-size ciphertexts with adaptive security or support for negation. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 384–402. Springer, Heidelberg (2010)
3. Attrapadung, N., Libert, B., de Panafieu, E.: Expressive key-policy attribute-based encryption with constant-size ciphertexts. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 90–108. Springer, Heidelberg (2011)
4. Beimel, A.: Secure Schemes for Secret Sharing and Key Distribution. PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel (1986)
5. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, pp. 321–334 (2007)
6. Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 443–459. Springer, Heidelberg (2004)
7. 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)
8. 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)
9. Boneh, D., Sahai, A., Waters, B.: Functional Encryption: Definitions and Challenges. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 253–273. Springer, Heidelberg (2011)
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. Chase, M., Chow, S.S.M.: Improving privacy and security in multi-authority attribute-based encryption. In: ACM Conference on Computer and Communications Security, pp. 121–130 (2009)
12. Cheung, L., Newport, C.C.: Provably secure ciphertext policy abe. In: ACM Conference on Computer and Communications Security, pp. 456–465 (2007)
13. Garg, S., Gentry, C., Halevi, S., Sahai, A., Waters, B.: Attribute-based encryption for circuits from multilinear maps. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 479–499. Springer, Heidelberg (2013)
14. Gorbunov, S., Vaikuntanathan, V., Wee, H.: Attribute-based encryption for circuits. In: STOC, pp. 545–554 (2013)
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, p. 89 (2006)
17. Hohenberger, S., Waters, B.: Attribute-based encryption with fast decryption. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 162–179. Springer, Heidelberg (2013)

18. Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer, Heidelberg (2008)
19. Lewko, A.: Tools for simulating features of composite order bilinear groups in the prime order setting. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 318–335. Springer, Heidelberg (2012)
20. Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: Attribute-based encryption and (Hierarchical) inner product encryption. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 62–91. Springer, Heidelberg (2010)
21. Lewko, A.B., Sahai, A., Waters, B.: Revocation systems with very small private keys. In: IEEE Symposium on Security and Privacy, pp. 273–285 (2010)
22. Lewko, A., Waters, B.: Decentralizing attribute-based encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 568–588. Springer, Heidelberg (2011)
23. Lewko, A., Waters, B.: Unbounded HIBE and attribute-based encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 547–567. Springer, Heidelberg (2011)
24. Lewko, A., Waters, B.: New proof methods for attribute-based encryption: Achieving full security through selective techniques. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 180–198. Springer, Heidelberg (2012)
25. Naor, M., Pinkas, B.: Efficient trace and revoke schemes. In: Frankel, Y. (ed.) FC 2000. LNCS, vol. 1962, pp. 1–20. Springer, Heidelberg (2001)
26. Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 191–208. Springer, Heidelberg (2010)
27. Okamoto, T., Takashima, K.: Fully secure unbounded inner-product and attribute-based encryption. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 349–366. Springer, Heidelberg (2012)
28. Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. In: ACM Conference on Computer and Communications Security, pp. 195–203 (2007)
29. Pippenger, N.: On the evaluation of powers and related problems (preliminary version). In: FOCS, pp. 258–263 (1976)
30. Rouselakis, Y., Waters, B.: Practical constructions and new proof methods for large universe attribute-based encryption. In: ACM Conference on Computer and Communications Security, pp. 463–474 (2013)
31. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)
32. Waters, B.: Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 53–70. Springer, Heidelberg (2011)
33. Waters, B.: Functional encryption for regular languages. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 218–235. Springer, Heidelberg (2012)