Attribute Based Encryption with Direct Efficiency Tradeoff

Nuttapong Attrapadung[1(✉)], Goichiro Hanaoka[1], Tsutomu Matsumoto[2], Tadanori Teruya[1], and Shota Yamada[1]

[1] National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan
{n.attrapadung,hanaoka-goichiro,tadanori.teruya, yamada-shota}@aist.go.jp
[2] Yokohama National University, Yokohama, Japan
tsutomu@ynu.ac.jp

Abstract. We propose the first fully secure unbounded Attribute-Based Encryption (ABE) scheme such that the key size and ciphertext size can be directly traded off. Our proposed scheme is parameterized by a positive integer d, which can be arbitrarily chosen at setup. In our scheme, the ciphertext size is $O(t/d)$, the private key size is $O(md)$, and the public key size is $O(d)$, where t, m are the sizes of attribute sets and policies corresponding to ciphertext and private key, respectively.

Our scheme can be considered as a generalization that includes two of the state-of-the-art ABE instantiations, namely, the unbounded ABE scheme and the ABE scheme with constant-size ciphertexts proposed by Attrapadung (Eurocrypt 2014). Indeed, these two schemes correspond to the two extreme cases of our scheme, that is, when setting $d = 1$ and when setting d as the maximum size of allowed attribute sets, respectively. Furthermore, our scheme also yields a tradeoff between encryption and decryption time. Interestingly, when estimating efficiency using numerical parameters, the decryption time is minimized at d being somewhere in the middle of the spectrum.

We believe that this tradeoff can provide advantages in applications where size and/or time resources are concretely fixed in advance, as we can flexibly adjust d to match available resources and thus make the most of them. Such situations include, but are not limited to, implementations of ABE in tiny hardware tokens.

Keywords: Attribute-based encryption · Efficiency tradeoff · Unbounded · Short ciphertext · Full security

1 Introduction

Attribute-based encryption (ABE), introduced by Sahai and Waters [23], is a useful paradigm that generalizes traditional public key encryption. Instead of encrypting to a target recipient, a sender can specify in a more general way

M. Manulis et al. (Eds.): ACNS 2016, LNCS 9696, pp. 249–266, 2016.
DOI: 10.1007/978-3-319-39555-5_14

about who should be able to view the message. In ABE for predicate R, which is a boolean function $R : \mathbb{X} \times \mathbb{Y} \to \{0,1\}$, a private key, which is issued by an authority, is associated with an attribute $X \in \mathbb{X}$, while a ciphertext encrypting a message M is associated with an attribute $Y \in \mathbb{Y}$. A key for X can decrypt a ciphertext for Y if and only if $R(X,Y) = 1$. In this paper, we focus on ABE for boolean formulae predicate, which is one of the most useful ABE primitive, first considered by Goyal *et al.* [13]. For simplicity, we mainly consider the *key-policy* type of ABE [13][1]. In such a scheme, a key is associated with a boolean formula (a policy), while a ciphertext is associated with an assignment of boolean variables (an attribute set), and the decryption succeeds if and only if the assignment satisfies the formula. In what follows, we let t be the size of an attribute set corresponding to a ciphertext and m be the size of a policy corresponding to a private key.

Two of the state-of-the-art *fully-secure*[2] ABE schemes for boolean formulae were proposed by Attrapadung [2]:

1. The first scheme is the fully-secure *unbounded* ABE of [2]. Such a scheme has a (completely) unbounded property where every parameter does not require any maximum bound at the setup of the scheme. All the other ABE schemes for boolean formulae in the literature either have bounds in some parameters [10, 16,18–21,26] and/or only selectively secure[3] [15,17,22]. This scheme has an obvious advantage in that the scheme has scalability in their *functionality*, in particular, it works for any sizes of attribute sets and policies, and any number of attribute multi-use in one policy. In this scheme, the ciphertext size is $O(t)$ (or more precisely, ct group elements for a constant $c > 1$) and the key size is $O(m)$.
2. The second scheme is the fully-secure ABE with *constant-size ciphertexts* of [2]. All the other constant-size-ciphertext ABE schemes for boolean formulae in the literature are only selectively secure [6] or semi-adaptively secure[4] [11,24]. This scheme has an advantage of scalability in *efficiency*: it requires very short ciphertexts of size $O(1)$, regardless of any t, which is the size of an attribute set assigned to a ciphertext. On the downside, it requires the maximum bound for t, say T, to be fixed at the setup (but no bound is required for all the other parameters). Moreover, the key size is quite large as it becomes $O(mT)$.

Note that the above two schemes were originally proposed in composite-order groups in [2]. Their prime-order variants, which are considered more efficient (*cf.* [14]), were then subsequently obtained in [3].

[1] The other types are ciphertext-policy [8,25] and dual-policy [5] ABE.

[2] Full security (or also called adaptive security) is the standard security notion for ABE. In this notion, the adversary can adaptively query keys for any attribute X as long as $R(X, Y^\star) = 0$ where $Y^\star$ is an adversarially and adaptively chosen attribute for the challenge ciphertext.

[3] Selective security refers to a weak notion where the adversary is required to announce the challenge ciphertext attribute $Y^\star$ upfront before seeing the public key.

[4] Semi-adaptive security is an intermediate notion between selective and full security.

Due to the drawback of the first scheme in that the ciphertext size is not constant (hence we may say that it lacks scalability in efficiency) and the drawbacks of the second scheme in that the key size is large and the attribute set size is bounded (and hence it lacks scalability in functionality), it is natural to seek for a new scheme with better scalability in both efficiency and functionality.

To this end, we consider the following important open problem:

> Is it possible to achieve fully-secure *unbounded* ABE with *short ciphertext size* (less than t group elements)?

We note that constructing even only *selectively* secure ABE with the above property is also an open problem.

Our Contribution. In this paper, we answer the above question affirmatively by proposing a new fully-secure unbounded ABE scheme with a *direct tradeoff* between ciphertext and key size: the ciphertext size is $O(t/d)$ and the key size is $O(md)$, where the "adjusting parameter" d is any positive integer which can be arbitrarily chosen at setup. The efficiency comparison is shown in Table 1 below.

Table 1. Comparison among fully-secure KP-ABE

Scheme	|secret key|	|ciphertext|
Unbounded ABE of [2,3]	$O(m)$	$O(t)$
Constant-size-ciphertext ABE of [2,3]	$O(mT)$	$O(1)$
Our new schemes	$O(md)$	$O(t/d)$

† m is the size of policy associated to a private key.
t is the attribute set size associated to a ciphertext.
T is the maximum bound of t (if bounded).

Our tradeoff scheme can be thought of a generalization that includes both the unbounded ABE and the constant-size-ciphertext ABE of [2,3] as the two extreme cases on the spectrum over the tradeoff parameter d. That is, when setting $d = 1$, we recover the unbounded ABE, while setting $d = T$ (and thus posing the maximum bound of t) gives us back the constant-size-ciphertext ABE.

Adjusting d also consequently results in a tradeoff between encryption time and decryption time. We give the performance estimation in Sect. 4, where we show the efficiency comparison in details and more concretely in Tables 2, 3 and 4. Interestingly, as shown in Fig. 1, when estimating efficiency using numerical parameters, *e.g.,* from the 254-bit Barreto-Naehrig (BN) curve, the decryption time is minimized at d being somewhere in the middle of the spectrum.

Our Approach. Our new scheme is constructed based on Key-Policy over Doubly Spatial Encryption (KP-DSE) scheme, which is a primitive introduced also in [2] (with a prime-order version subsequently proposed in [3]). KP-DSE was shown to imply both the unbounded ABE and the constant-size-ciphertext ABE in [2]. We extend these implications by showing a new conversion from KP-DSE to KP-ABE with tradeoff, which is our goal. Applying this new conversion to

the KP-DSE schemes of [2] and [3], we obtain a new KP-ABE with tradeoff in composite-order groups and prime-order groups, respectively.

Our idea for achieving the ciphertext of size $O(t/d)$ is to first partition the attribute set (of size t) associated to a ciphertext to t/d disjoint subsets each of size d. We then associate each subset by encoding it to an affine subspace in KP-DSE. Due to the efficiency of the concrete KP-DSE scheme of [2] where each affine space requires a corresponding ciphertext portion of constant size, the total ciphertext size is thus $O(t/d)$, the number of partitioned subsets. The fact that we require an affine subspace to encode a set of size d results in an increasing factor d for the key size, hence the tradeoff.

We describe our approach in details in Sect. 3. Before that, we give the definition of KP-DSE in Sect. 2.

Perspective. We believe that the tradeoff property of our scheme can provide advantages in real-world applications where size and/or time resources are concretely fixed in advance, as we can flexibly adjust d to match available resources and thus make the most of them. Such situations include, but are not limited to, implementations of ABE in tiny hardware tokens, such as secure applications for the Internet of Things.

2 Preliminaries

2.1 Definitions for ABE

Predicate Family. Let $R = \{R_\kappa : \mathbb{X}_\kappa \times \mathbb{Y}_\kappa \to \{0,1\} | \kappa \in \mathbb{N}^c\}$ be a predicate family where $\mathbb{X}_\kappa$ and $\mathbb{Y}_\kappa$ denote "key attribute" and "ciphertext attribute" spaces and c is some fixed constant. The index $\kappa = (n_1, n_2, \ldots, n_c)$ denotes some bounds for parameters specific to each predicate family.

ABE Syntax. An attribute-based encryption (ABE) scheme for predicate family R is defined by the following algorithms:

- $\mathsf{Setup}(1^\lambda, \kappa) \to (\mathsf{PK}, \mathsf{MSK})$: takes as input a security parameter 1^λ and a family index κ of predicate family R, and outputs a master public key PK and a master secret key MSK.
- $\mathsf{Encrypt}(Y, M, \mathsf{PK}) \to \mathsf{CT}$: takes as input a ciphertext attribute $Y \in \mathbb{Y}_\kappa$, a message $M \in \mathcal{M}$, and public key PK. It outputs a ciphertext CT.
- $\mathsf{KeyGen}(X, \mathsf{MSK}, \mathsf{PK}) \to \mathsf{SK}$: takes as input a key attribute $X \in \mathbb{X}_\kappa$ and the master key MSK. It outputs a secret key SK.
- $\mathsf{Decrypt}(\mathsf{CT}, \mathsf{SK}) \to M$: given a ciphertext CT with its attribute Y and the decryption key SK with its attribute X, it outputs a message M or $\perp$.

Correctness. Consider all indexes κ, all $M \in \mathcal{M}$, $X \in \mathbb{X}_\kappa$, $Y \in \mathbb{Y}_\kappa$ such that $R_\kappa(X, Y) = 1$. If $\mathsf{Encrypt}(Y, M, \mathsf{PK}) \to \mathsf{CT}$ and $\mathsf{KeyGen}(X, \mathsf{MSK}, \mathsf{PK}) \to \mathsf{SK}$ where $(\mathsf{PK}, \mathsf{MSK})$ is generated from $\mathsf{Setup}(1^\lambda, \kappa)$, then $\mathsf{Decrypt}(\mathsf{CT}, \mathsf{SK}) \to M$.

Security. The standard notion for ABE is called full security. We refer its definition to [2], as we do not work directly on it but rather use the embedding lemma for implications below (Lemma 1).

KP-ABE for Monotone Span Program Predicates. Let $\mathcal{U}$ be the universe of attributes. If $|\mathcal{U}|$ is of super-polynomial size, it is called large universe [13,22], otherwise, it is small universe. This predicate is indexed by $N \in \mathbb{N}$. In this predicate, the key attribute domain $\mathbb{X}_N$ is the set of all policies. A policy is specified by a monotone span program (or access structure) (A, π) where A is a matrix in $\mathbb{Z}_N^{m \times k}$ for some $m, k \in \mathbb{N}$, and π is a map $\pi : [1, m] \to \mathcal{U}$. The ciphertext attribute domain is the collection of all sets, S, of attributes in $\mathcal{U}$. For a set $S \subseteq \mathcal{U}$, let $A|_S$ be the sub-matrix of A that takes all the rows j such that $\pi(j) \in S$. We say that (A, π) accepts S if $(1, 0, \ldots, 0) \in \mathsf{rspan}(A|_S)$, where $\mathsf{rspan}()$ denotes the row span. That is,

$$R_N^{\mathsf{KP\text{-}ABE}}((A, \pi), S) = 1 \iff (1, 0, \ldots, 0) \in \mathsf{span}\{A_i | \pi(i) \in S\}.$$

In this paper, we consider unbounded KP-ABE, which is KP-ABE with large universe such that all parameters $|S|, m, k$ and the number of attribute re-use (the repetition in the range $\pi([1, m])$) are unbounded. It is well known that ABE for monotone span program implies ABE for monotone Boolean formulae [13].

2.2 KP-DSE

Our new KP-ABE scheme will use an implication from KP-DSE [2]. We briefly review it here.

Notions for Affine Spaces. Let $N, n, d \in \mathbb{N}$ where $0 \leq d \leq n$. Let $\boldsymbol{t}^\top$ be a vertical vector in $\mathbb{Z}_N^n$. Let $\boldsymbol{M} \in \mathbb{Z}_N^{n \times d}$ be a matrix whose columns are all linearly independent. An affine space in $\mathbb{Z}_N^n$ specified by a pair $(\boldsymbol{t}, \boldsymbol{M})$ is defined as $\boldsymbol{t}^\top + \mathsf{cspan}(\boldsymbol{M})$, where $\mathsf{cspan}()$ denotes the column span; more precisely, it is

$$\boldsymbol{t}^\top + \mathsf{cspan}(\boldsymbol{M}) = \{\boldsymbol{t}^\top + \boldsymbol{M}\boldsymbol{v}^\top | \boldsymbol{v} \in \mathbb{Z}_N^d\}.$$

Key-Policy over Doubly Spatial Encryption (KP-DSE). The predicate for KP-DSE is defined as follows. The predicate family is indexed by $(N, n) \in \mathbb{N}^2$. Define the key attribute domain $\mathbb{X}_{(N,n)}$ as the set of all pairs of an access matrix $A \in \mathbb{Z}_N^{m \times k}$ for any polynomial-size $m, k \in \mathbb{N}$ and a labelling map π that maps each row in $[1, m]$ to an affine space in $\mathbb{Z}_N^n$. Define the ciphertext attribute domain $\mathbb{Y}_{(N,n)}$ as the collection of all sets, T, of affine spaces in $\mathbb{Z}_N^n$. The predicate evaluation is defined by

$$R_{(N,n)}^{\mathsf{KP\text{-}DSE}}\big((A, \pi), T\big) = 1 \iff (1, 0, \ldots, 0) \in \mathsf{span}\{A_i | \exists Y \in T \text{ s.t. } \pi(i) \cap Y \neq \emptyset\}.$$

2.3 Embedding Lemma

The following useful lemma from [4,9] describes a sufficient criterion for implication from ABE for a given predicate to ABE for another predicate. We will use this lemma in Sect. 3.1 for showing that KP-DSE implies KP-ABE with tradeoff, which is our main proposal.

The lemma considers two arbitrary predicate families:

$$R^{\mathsf{F}}_{\kappa} : \mathbb{X}_{\kappa} \times \mathbb{Y}_{\kappa} \to \{0,1\}, \qquad R^{\mathsf{F}'}_{\kappa'} : \mathbb{X}'_{\kappa'} \times \mathbb{Y}'_{\kappa'} \to \{0,1\},$$

which is parametrized by $\kappa \in \mathbb{N}^c$ and $\kappa' \in \mathbb{N}^{c'}$ respectively. Suppose that there exists three efficient mappings

$$f_{\mathsf{p}} : \mathbb{Z}^{c'} \to \mathbb{Z}^{c} \qquad f_{\mathsf{e}} : \mathbb{X}'_{\kappa'} \to \mathbb{X}_{f_{\mathsf{p}}(\kappa')} \qquad f_{\mathsf{k}} : \mathbb{Y}'_{\kappa'} \to \mathbb{Y}_{f_{\mathsf{p}}(\kappa')}$$

which maps parameters, ciphertext attributes, and key attributes, respectively, such that for all $X' \in \mathbb{X}'_{\kappa'}, Y' \in \mathbb{Y}'_{\kappa'}$,

$$R^{\mathsf{F}'}_{\kappa'}(X', Y') = 1 \quad \Leftrightarrow \quad R^{\mathsf{F}}_{f_{\mathsf{p}}(\kappa')}(f_{\mathsf{e}}(X'), f_{\mathsf{k}}(Y')) = 1. \tag{1}$$

We can then construct an ABE scheme

$$\Pi' = \{\mathsf{Setup}', \mathsf{Encrypt}', \mathsf{KeyGen}', \mathsf{Decrypt}'\} \text{ for predicate } R^{\mathsf{F}'}_{\kappa'}$$

from an ABE scheme

$$\Pi = \{\mathsf{Setup}, \mathsf{Encrypt}, \mathsf{KeyGen}, \mathsf{Decrypt}\} \text{ for predicate } R^{\mathsf{F}}_{\kappa}$$

by letting

$$\begin{aligned}
\mathsf{Setup}'(\lambda, \kappa') &= \mathsf{Setup}(\lambda, f_{\mathsf{p}}(\kappa')) \\
\mathsf{Encrypt}'(\mathsf{PK}, M, X') &= \mathsf{Encrypt}(\mathsf{PK}, M, f_{\mathsf{e}}(X')), \\
\mathsf{KeyGen}'(\mathsf{MSK}, \mathsf{PK}, Y') &= \mathsf{KeyGen}(\mathsf{MSK}, \mathsf{PK}, f_{\mathsf{k}}(Y')), \\
\mathsf{Decrypt}'(\mathsf{CT}_{X'}, \mathsf{SK}_{Y'}) &= \mathsf{Decrypt}(\mathsf{CT}_{f_{\mathsf{e}}(X')}, \mathsf{SK}_{f_{\mathsf{k}}(Y')}).
\end{aligned}$$

Lemma 1 (Embedding lemma [4,9]). *If Π is correct and secure, then so is Π'. This holds for both the cases of selective security and full security.*

2.4 Notations

Notation for Matrix in the Exponents. Vectors will be treated as either row or column matrices. When unspecified, we shall let it be a row vector. Let $\mathbb{G}$ be a group. Let $\boldsymbol{a} = (a_1, \ldots, a_n)$ and $\boldsymbol{b} = (b_1, \ldots, b_n) \in \mathbb{G}^n$. We denote $\boldsymbol{a} \cdot \boldsymbol{b} = (a_1 \cdot b_1, \ldots, a_n \cdot b_n)$, where '$\cdot$' is the group operation of $\mathbb{G}$. For $g \in \mathbb{G}$ and $\boldsymbol{c} = (c_1, \ldots, c_n) \in \mathbb{Z}^n$, we denote $g^{\boldsymbol{c}} = (g^{c_1}, \ldots, g^{c_n})$. We denote by $\mathbb{GL}_{p,n}$ the group of invertible matrices (the general linear group) in $\mathbb{Z}_p^{n \times n}$. Consider $\boldsymbol{M} \in \mathbb{Z}_p^{d \times n}$

(the set of all $d \times n$ matrices in $\mathbb{Z}_p$). Denote the transpose of $\boldsymbol{M}$ as $\boldsymbol{M}^\top$. Denote $\boldsymbol{M}^{-\top} = (\boldsymbol{M}^\top)^{-1}$. We denote by $g^{\boldsymbol{M}}$ the matrix in $\mathbb{G}^{d\times n}$ of which its (i,j) entry is $g^{\boldsymbol{M}_{i,j}}$, where $\boldsymbol{M}_{i,j}$ is the (i,j) entry of $\boldsymbol{M}$. For $\boldsymbol{Q} \in \mathbb{Z}_p^{\ell\times d}$, we denote $(g^{\boldsymbol{Q}})^{\boldsymbol{M}} = g^{\boldsymbol{QM}}$. Note that from $\boldsymbol{M}$ and $g^{\boldsymbol{Q}} \in \mathbb{G}^{\ell\times d}$, we can compute $g^{\boldsymbol{QM}}$ without knowing $\boldsymbol{Q}$, since its (i,j) entry is $\prod_{k=1}^{d}(g^{\boldsymbol{Q}_{i,k}})^{\boldsymbol{M}_{k,j}}$. The same goes for $g^{\boldsymbol{M}}$ and $\boldsymbol{Q}$. For $\boldsymbol{X} \in \mathbb{Z}_p^{r\times c_1}$ and $\boldsymbol{Y} \in \mathbb{Z}_p^{r\times c_2}$, we denote its pairing as:

$$e(g_1^{\boldsymbol{X}}, g_2^{\boldsymbol{Y}}) = e(g_1, g_2)^{\boldsymbol{Y}^\top \boldsymbol{X}} \in \mathbb{G}_T^{c_2\times c_1}.$$

Projection Maps. As used in [3], $\left(\begin{smallmatrix}\boldsymbol{I}_b\\0\end{smallmatrix}\right)$ denotes the $(b+1)\times b$ matrix where the first b rows comprise the identity matrix while the last row is zero. It functions as a left-projection map. That is, $X\left(\begin{smallmatrix}\boldsymbol{I}_b\\0\end{smallmatrix}\right) \in \mathbb{Z}_p^{(d+1)\times d}$ is the matrix consisting of all left d columns of X for any $X \in \mathbb{Z}_p^{(d+1)\times(d+1)}$. Similarly, $\left(\begin{smallmatrix}\boldsymbol{0}\\1\end{smallmatrix}\right)$ is the $(b+1)\times 1$ matrix where the last row is 1; it functions as a right-projection map.

3 Our Key-Policy ABE Schemes

Main Idea for Our Scheme. The main idea for our new KP-ABE scheme is that we set an parameter d and partition the attribute set S to a disjoint union[5] as $S = S_1 \sqcup \cdots \sqcup S_\ell$ where $|S_j| \le d$ for all $j \in [1,\ell]$ and $\ell = \lceil |S|/d \rceil$. We then represent each subset S_j by an affine space using an embedding method similar to the KP-ABE with constant-size ciphertext of [2] (which extends [6]). This method results in KP-DSE with the set of ℓ affine spaces in $\mathbb{Z}_N^{d+1}$. An implementation using the KP-DSE of [2] requires $O(\ell)$-size ciphertext for the set of ℓ affine spaces. Hence, we will achieve the ciphertext size of $O(\ell) = O(|S|/d)$ as desired.

Partitioned KP-ABE. As an intermediate predicate family, we define "partitioned KP-ABE" (for monotone span program). The purpose is only syntactic: to have a predicate family that is indexed also by the adjustable integer d. (The original definition has only index N specifying $\mathbb{Z}_N$). More precisely, it is indexed by $(N,d) \in \mathbb{N}^2$. The key attribute domain is the same as normal KP-ABE. The ciphertext attribute domain is the set of all collections of disjointed subsets of $\mathcal{U}$ each with size $\le d$. The predicate evaluation is defined by

$$R_{(N,d)}^{\mathsf{Partition\text{-}KP\text{-}ABE}}\big((A,\pi),U\big) = 1 \iff (1,0,\ldots,0) \in \mathsf{span}\{A_i | \exists W \in U \ \text{ s.t. } \pi(i) \in W\}.$$

(Here, U is a collection of disjointed subsets of $\mathcal{U}$ each with size $\le d$.)

Partitioned KP-ABE implies Normal KP-ABE. Partitioned KP-ABE immediately implies KP-ABE by mapping ciphertext attribute as

$$S \mapsto \{S_1, \cdots S_\ell\}$$

[5] We denote by '$\sqcup$' the union of disjointed sets.

where $S = S_1 \sqcup \cdots \sqcup S_\ell$ where $|S_j| \leq d$ for all $j \in [1, \ell]$ and $\ell = \lceil |S|/d \rceil$. To obtain a unique partition, we can arrange attributes in S in a lexicographical order as $S = \{b_1, \ldots, b_{|S|}\}$ and let $S_j = \{b_{(j-1)d+1}, \ldots, b_{jd}\}$ for all $j \in [1, \ell - 1]$ (and hence, $S_\ell = \{b_{(\ell-1)d+1}, \ldots, b_{|S|}\}$). Straightforwardly, we have the following lemma:

Lemma 2. *For any monotone access structure $\mathbb{A} = (A, \pi)$, any attribute set S, and $\{S_j\}_j$ defined as above, we have*

$$R_N^{\mathsf{KP\text{-}ABE}}\big((A,\pi), S\big) = 1 \quad \Longleftrightarrow \quad R_{(N,d)}^{\mathsf{Partition\text{-}KP\text{-}ABE}}\big((A,\pi), \{S_1, \cdots S_\ell\}\big) = 1.$$

Proof. This trivially holds since $\pi(i) \in S$ iff there exists $j \in [1, \ell]$ such that $\pi(i) \in S_j$.

3.1 Implication of Partitioned KP-ABE from KP-DSE

We now show that partitioned KP-ABE is implied from KP-DSE. The conversion is as follows.

- **Mapping Parameters.** We map $f_{\mathsf{p}} : (N, d) \mapsto (N, d+1)$. That is, we let the full dimension of affine spaces be $n = d + 1$.
- **Mapping Key Attributes.** Consider an access structure $\mathbb{A} = (A, \pi)$. Let m be the number of rows of the access matrix A. We map

  $$f_{\mathsf{k}} : \mathbb{A} = (A, \pi) \mapsto \mathbb{A}' = (A, \pi')$$

  where for $i = 1, \ldots, m$, we let $\pi'(i) = \mathsf{cspan}(\boldsymbol{X}^{(i)})$ where

  $$\boldsymbol{X}^{(i)} := \begin{pmatrix} -\pi(i) & -\pi(i)^2 & \cdots & -\pi(i)^d \\ 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}.$$

  In particular, each $\pi'(i)$ is an affine space passing through the point $\mathbf{0}^\top$ (*i.e.,* it is a vector space).
- **Mapping Ciphertext Attributes.** Consider a disjoint collection $\{S_1, \ldots, S_\ell\}$ where $|S_j| \leq d$ for all $j \in [1, \ell]$. We map

  $$f_{\mathsf{c}} : \{S_1, \ldots, S_\ell\} \mapsto \{\boldsymbol{y}^{(1)}, \ldots, \boldsymbol{y}^{(\ell)}\}$$

  where for $j = 1, \ldots, \ell$, we let $\boldsymbol{y}^{(i)}$ be 0-dimensional affine space (a point) as

  $$\boldsymbol{y}^{(j)} := (a_{j,0}, a_{j,1}, \ldots, a_{j,d})^\top.$$

  where we define $a_{j,\iota}$ to be the coefficient of z^ι in $p_j(z) := \prod_{y \in S_j}(z - y) = a_{j,0} + a_{j,1}z + \cdots + a_{j,d}z^d$.

We show the following lemma for the above conversion. The implication from KP-DSE to KP-ABE will then follow from the embedding lemma.

Lemma 3. *For any monotone access structure* $\mathbb{A} = (A, \pi)$ *and a collection* $\{S_1, \ldots, S_\ell\}$ *where each* $|S_j| \leq d$*, we have*

$$R_d^{\mathsf{Partition\text{-}KP\text{-}ABE}}(\mathbb{A}, \{S_1, \ldots, S_\ell\}) = 1 \iff R_{f_\mathsf{p}(d)}^{\mathsf{KP\text{-}DSE}}(f_\mathsf{k}(\mathbb{A}), f_\mathsf{c}(\{S_1, \ldots, S_\ell\})) = 1.$$

Proof. From the definition of the KP-DSE predicate, to prove the statement of the theorem, it suffices to prove that for all $i \in [1, m], j \in [1, \ell]$,

$$\pi(i) \in S_j \quad \Leftrightarrow \quad \boldsymbol{y}^{(j)} \in \mathsf{cspan}(\boldsymbol{X}^{(i)}) \tag{2}$$

Forward Direction ($\Rightarrow$). Suppose $\pi(i) \in S_j$. Thus, $p_j(\pi(i)) = 0$ (by the definition of p_j). Therefore,

$$\begin{aligned} \boldsymbol{X}^{(i)}(\boldsymbol{a}^{(j)})^\top &= \big(-(a_{j,1}\pi(i) + \cdots + a_{j,d}\pi(i)^d), a_{j,1}, \ldots, a_{j,d}\big)^\top \\ &= (a_{j,0}, a_{j,1}, \ldots, a_{j,d})^\top \\ &= \boldsymbol{y}^{(j)}, \end{aligned}$$

where we use the fact that $p_j(\pi(i)) = a_{j,0} + a_{j,1}\pi(i) + \cdots + a_{j,d}\pi(i)^d = 0$ in the second line. From this, we obtain that $\boldsymbol{y}^{(j)} \in \mathsf{cspan}(\boldsymbol{X}^{(i)})$, which is the the right-hand side of (2), as desired. This concludes the forward part.

Backward Direction ($\Leftarrow$). We prove by contrapositive. Suppose $\pi(i) \notin S_j$. Hence, $p_j(\pi(i)) \neq 0$. Suppose for contradiction that $\boldsymbol{y}^{(j)} \in \mathsf{cspan}(\boldsymbol{X}^{(i)})$. Hence there is a linear combination $\boldsymbol{v}^\top = (v_1, \ldots, v_d)^\top$ such that

$$\boldsymbol{X}^{(i)}\boldsymbol{v}^\top = \boldsymbol{y}^{(j)}. \tag{3}$$

Thus, by our definitions of $\boldsymbol{X}^{(i)}, \boldsymbol{y}^{(j)}$, we must have that

$$\big(-(v_1\pi(i) + \cdots + v_d\pi(i)^d), v_1, \ldots, v_d\big)^\top = (a_{j,0}, a_{j,1}, \ldots, a_{j,d})^\top$$

But this implies that $p_j(\pi(i)) = 0$, a contradiction. Therefore, $\boldsymbol{y}^{(j)} \notin \mathsf{cspan}(\boldsymbol{X}^{(i)})$. This concludes the proof for the backward part.

3.2 Our KP-ABE in Composite-Order Groups

In this subsection, we apply our KP-DSE-to-KP-ABE conversion above to the KP-DSE scheme in composite-order groups proposed in [2]. We use asymmetric groups instead of symmetric groups as defined for the original scheme in [2].

The scheme will use a composite-order asymmetric bilinear group generator $\mathcal{G}_{\mathsf{composite}}$ which outputs $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, N, p_1, p_2, p_3) \xleftarrow{\$} \mathcal{G}_{\mathsf{composite}}(\lambda)$, where $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are of order $N = p_1p_2p_3$. The bilinear map takes the form $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Let $\mathbb{G}_{1,p_i}, \mathbb{G}_{2,p_i}$ be the subgroup of order p_i of $\mathbb{G}_1, \mathbb{G}_2$ respectively. The scheme is as follows.

- $\mathsf{Setup}(1^\lambda, d)$: Generate a composite-order group parameter as $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, N, p_1, p_2, p_3) \xleftarrow{\$} \mathcal{G}_{\mathsf{composite}}(\lambda)$. Pick generators $g_1 \xleftarrow{\$} \mathbb{G}_{1,p_1}$, $g_2 \in \mathbb{G}_{2,p_1}$, and $Z_3 \xleftarrow{\$} \mathbb{G}_{2,p_3}$. Pick $\boldsymbol{h} = (h_0, h_1, \ldots, h_{d+1}, \phi_1, \phi_2, \phi_3, \eta) \xleftarrow{\$} \mathbb{Z}_N^{d+6}$ and $\alpha \xleftarrow{\$} \mathbb{Z}_N$. The public key is $\mathsf{PK} = \big(g_1, g_2, e(g_1, g_2)^\alpha, g_1^{\boldsymbol{h}}, Z_3\big)$. The master secret key is $\mathsf{MSK} = \alpha$.
- $\mathsf{Encrypt}(S, M, \mathsf{PK})$: Upon input a set $S \subseteq \mathbb{Z}_N$, do as follows.
  1. Let $\ell = \lceil |S|/d \rceil$. Partition S to a disjoint union as $S = S_1 \sqcup \cdots \sqcup S_\ell$ where $|S_j| \leq d$ for all $j \in [1, \ell]$. For all $j \in [1, \ell]$, let $a_{j,\iota}$ be the coefficient of z^ι in $p_j(z) := \prod_{y \in S_j}(z - y)$.
  2. Pick $s, w, s_1, \ldots, s_\ell \xleftarrow{\$} \mathbb{Z}_N$. Output a ciphertext $\mathsf{CT} = (C_0, C_1, C_2, C_3, C_4, \{C_{5,j}, C_{6,j}\}_{j \in [1,\ell]})$ where we let $C_0 = (e(g_1, g_2)^\alpha)^s M \in \mathbb{G}_T$ and

$$\begin{aligned} C_1 &= g_1^s, & C_2 &= g_1^{s\eta}, \\ C_3 &= g_1^{s\phi_1 + w\phi_2}, & C_4 &= g_1^w, \\ C_{5,j} &= g_1^{w\phi_3 + s_j(h_0 + h_1 a_{j,0} + \cdots + h_{d+1} a_{j,d})}, & C_{6,j} &= g_1^{s_j} \end{aligned}$$

- $\mathsf{KeyGen}((A, \pi), \mathsf{MSK}, \mathsf{PK})$: Upon input an access structure (A, π), where $A \in \mathbb{Z}_N^{m \times k}$ and $\pi : [1, m] \to \mathbb{Z}_N$ for some $m, k \in \mathbb{N}$, do as follows. Parse $\mathsf{MSK} = \alpha$. Pick randomly $r, u, r_1, \ldots, r_m, v_2, \ldots, v_k \xleftarrow{\$} \mathbb{Z}_N$. Define $v_1 = r\phi_2$ and let $\boldsymbol{v} = (v_1, \ldots, v_k)$. Compute a secret key $\boldsymbol{K} = \big(K_1, K_2, K_3, \{K_{4,i}, K_{5,i}, \boldsymbol{K}_{6,i}\}_{i \in [1,m]}\big)$ as

$$\begin{aligned} K_1 &= g_2^{\alpha + r\phi_1 + u\eta}, \\ K_2 &= g_2^u, \\ K_3 &= g_2^r, \\ K_{4,i} &= g_2^{A_i \boldsymbol{v}^\top + r_i \phi_3}, \\ K_{5,i} &= g_2^{r_i}, \\ \boldsymbol{K}_{6,i} &= \Big(g_2^{r_i h_0}, g_2^{r_i\left(h_2 - h_1 \pi(i)\right)}, \ldots, g_2^{r_i\left(h_{d+1} - h_1 \pi(i)^d\right)}\Big). \end{aligned}$$

  Pick a randomness mask $\boldsymbol{R} \xleftarrow{\$} \mathbb{G}_{2,p_3}^{3+(d+3)m}$ (hence, $\boldsymbol{R}$ is of the same length as $\boldsymbol{K}$). Output a secret key $\mathsf{SK} = \boldsymbol{K} \cdot \boldsymbol{R}$ (here, '$\cdot$' denotes the component-wise multiplication).
- $\mathsf{Decrypt}(\mathsf{CT}, \mathsf{SK})$: Parse $(S, (A, \pi))$ from CT, SK. Assume (A, π) accepts S, so that the decryption can be performed. Let $I := \{i \in [1, m] | \pi(i) \in S\}$. From the property of LSSS, we have reconstruction coefficients $\{\mu_i\}_{i \in I}$ such that $\sum_{i \in I} \mu_i A_i \boldsymbol{v}^\top = v_1 (= r\phi_2)$. Do as follows
  1. For all $i \in I$, do as follows. Let j_i be the index such that $\pi(i) \in S_{j_i}$. (There is such an index since $\pi(i) \in S$ for all $i \in I$). Parse $\boldsymbol{K}_{6,i} = (K_{6,i,0}, \ldots, K_{6,i,d})$. Compute

$$D_{6,i} := K_{6,i,0} \cdot K_{6,i,1}^{a_{j_1}} \cdots K_{6,i,d}^{a_{j_d}}.$$

  (Also recall that $a_{j,\iota}$ be the coefficient of z^ι in $p_j(z) := \prod_{y \in S_j}(z - y)$).

2. Compute $e(g_1, g_2)^{\alpha s} = L_1 L_2$ where

$$L_1 := e(C_1, K_1) e(C_2, K_2)^{-1} e(C_3, K_3)^{-1},$$
$$L_2 := \prod_{i \in I} \left(e(C_4, K_{4,i}) e(C_{5,j_i}, K_{5,i})^{-1} e(C_{6,j_i}, D_{6,i}) \right)^{\mu_i}. \tag{4}$$

3. Finally compute $M \leftarrow C_0 / e(g_1, g_2)^{\alpha s}$.

Security. The full security of the above scheme follows from the full security of the KP-DSE scheme in [2] and the embedding lemma for our KP-DSE-to-KP-ABE conversion. This is captured in the theorem below. We refer the Subgroup Decision Assumptions and the Expanded Diffie-Hellman Exponent (EDHE3, EDHE4) Assumptions to [2]. The notation $\mathsf{Adv}^{P}_{\mathcal{A}}(\lambda)$ denotes the advantage of an adversary $\mathcal{A}$ against the security of primitive or assumption P, in function of the security parameter λ. We also refer its precise definition for each assumption in [2].

Theorem 1. *The above KP-ABE is fully-secure under the Subgroup Decision Assumption 1,2,3, the* $(d+1, \ell)$-EDHE3*, and the* $(d+1, m, k)$-EDHE4 *Assumption (in asymmetric composite-order groups), where* d *is the adjustable integer,* $\ell = \lceil |S|/d \rceil$*, where* S *is the ciphertext query, and* m, k *are the maximum numbers of rows and columns of access matrices among all key queries, respectively. More precisely, for any ppt adversary* $\mathcal{A}$*, let* q_1 *denote the number of queries in phase 1, there exist ppt algorithms* $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3, \mathcal{B}_4, \mathcal{B}_5$*, whose running times are the same as* $\mathcal{A}$ *plus some polynomial times, such that for any* λ*,*

$$\mathsf{Adv}^{\mathsf{KP\text{-}ABE}}_{\mathcal{A}}(\lambda) \leq 2\mathsf{Adv}^{\mathsf{SD1}}_{\mathcal{B}_1}(\lambda) + (2q_1 + 3)\mathsf{Adv}^{\mathsf{SD2}}_{\mathcal{B}_2}(\lambda) + \mathsf{Adv}^{\mathsf{SD3}}_{\mathcal{B}_3}(\lambda) + q_1 \mathsf{Adv}^{(d+1,m,k)\text{-EDHE4}}_{\mathcal{B}_4}(\lambda) + \mathsf{Adv}^{(d+1,\ell)\text{-EDHE3}}_{\mathcal{B}_5}(\lambda).$$

Proof. This follows immediately from the KP-DSE-to-KP-ABE implication (*i.e.,* Lemma 1 via Lemmas 2 and 3) and the security of KP-DSE of [2] (*i.e.,* Theorems 1, 11 and 12 in [2]).

3.3 Our KP-ABE in Prime-Order Groups

In this subsection, we apply our KP-DSE-to-KP-ABE conversion to the KP-DSE scheme in prime-order groups proposed in [3] (which is then converted from [2]). The security is based on the Matrix Diffie-Hellman Assumption with parameter $b \in \mathbb{N}$. When $b = 1$, we can use the SXDH Assumption, and when $b = 2$, we can use the Decision Linear Assumption.

The scheme will use a prime-order asymmetric bilinear group generator $\mathcal{G}_{\mathsf{prime}}$ which outputs $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, p) \xleftarrow{\$} \mathcal{G}_{\mathsf{prime}}(\lambda)$, where $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are of order p. The bilinear map takes the form $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. The scheme is as follows.

- $\mathsf{Setup}(1^\lambda, d)$: Run $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, p) \xleftarrow{\$} \mathcal{G}_{\mathsf{prime}}(\lambda)$. Pick generators $g_1 \xleftarrow{\$} \mathbb{G}_1$, $g_2 \xleftarrow{\$} \mathbb{G}_2$. Pick $\boldsymbol{H}_0, \boldsymbol{H}_1, \ldots, \boldsymbol{H}_{d+5}, \xleftarrow{\$} \mathbb{Z}_p^{(b+1)\times(b+1)}$. Pick $\boldsymbol{B} \xleftarrow{\$} \mathbb{GL}_{p,b+1} \subset$

$\mathbb{Z}_p^{(b+1)\times(b+1)}$. Choose $\tilde{\boldsymbol{D}} \xleftarrow{\$} \mathbb{GL}_{p,b}$, define $\boldsymbol{D} := \left(\begin{smallmatrix} \tilde{\boldsymbol{D}} & \boldsymbol{0} \\ \boldsymbol{0} & 1 \end{smallmatrix}\right) \in \mathbb{GL}_{p,b+1}$ and $\boldsymbol{Z} := \boldsymbol{B}^{-\top}\boldsymbol{D}$. Choose $\boldsymbol{\alpha} \xleftarrow{\$} \mathbb{Z}_p^{(b+1)\times 1}$. Output

$$\mathsf{PK} = \left(e(g_1,g_2)^{\boldsymbol{\alpha}^\top \boldsymbol{B}\left(\begin{smallmatrix}\boldsymbol{I}_b\\ \boldsymbol{0}\end{smallmatrix}\right)}, g_1^{\boldsymbol{B}\left(\begin{smallmatrix}\boldsymbol{I}_b\\ \boldsymbol{0}\end{smallmatrix}\right)}, \left\{ g_1^{\boldsymbol{H}_i \boldsymbol{B}\left(\begin{smallmatrix}\boldsymbol{I}_b\\ \boldsymbol{0}\end{smallmatrix}\right)} \right\}_{i\in[0,d+5]} \right),$$

$$\mathsf{MSK} = \left(g_2^{\boldsymbol{\alpha}}, g_2^{\boldsymbol{Z}\left(\begin{smallmatrix}\boldsymbol{I}_b\\ \boldsymbol{0}\end{smallmatrix}\right)}, \left\{ g_2^{\boldsymbol{H}_i^\top \boldsymbol{Z}\left(\begin{smallmatrix}\boldsymbol{I}_b\\ \boldsymbol{0}\end{smallmatrix}\right)} \right\}_{i\in[0,d+5]} \right).$$

- $\mathsf{Encrypt}(S \subset \mathbb{Z}_p, M, \mathsf{PK})$: Upon input a set $S \subseteq \mathbb{Z}_p$, do as follows.
  1. Let $\ell = \lceil |S|/d \rceil$. Partition S to a disjoint union as $S = S_1 \sqcup \cdots \sqcup S_\ell$ where $|S_j| \le d$ for all $j \in [1,\ell]$. For all $j \in [1,\ell]$, let $a_{j,\iota}$ be the coefficient of z^ι in $p_j(z) := \prod_{y\in S_j}(z-y)$.
  2. Pick $\boldsymbol{s}_0, \boldsymbol{w}, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_\ell \xleftarrow{\$} \mathbb{Z}_p^{b\times 1}$. Output a ciphertext as $\mathsf{CT} = (\boldsymbol{C}_1, \boldsymbol{C}_2, \boldsymbol{C}_3, \boldsymbol{C}_4, \{\boldsymbol{C}_{5,j}, \boldsymbol{C}_{6,j}\}_{j\in[1,\ell]}, C_0)$ where

$$\begin{aligned}
\boldsymbol{C}_1 &= g_1^{\boldsymbol{B}\left(\begin{smallmatrix}\boldsymbol{s}_0\\ 0\end{smallmatrix}\right)},\\
\boldsymbol{C}_2 &= g_1^{\boldsymbol{H}_{d+5}\boldsymbol{B}\left(\begin{smallmatrix}\boldsymbol{s}_0\\ 0\end{smallmatrix}\right)},\\
\boldsymbol{C}_3 &= g_1^{\boldsymbol{H}_{d+2}\boldsymbol{B}\left(\begin{smallmatrix}\boldsymbol{s}_0\\ 0\end{smallmatrix}\right)+\boldsymbol{H}_{d+3}\boldsymbol{B}\left(\begin{smallmatrix}\boldsymbol{w}\\ 0\end{smallmatrix}\right)},\\
\boldsymbol{C}_4 &= g_1^{\boldsymbol{B}\left(\begin{smallmatrix}\boldsymbol{w}\\ 0\end{smallmatrix}\right)},\\
\boldsymbol{C}_{5,j} &= g_1^{\boldsymbol{H}_{d+4}\boldsymbol{B}\left(\begin{smallmatrix}\boldsymbol{w}\\ 0\end{smallmatrix}\right)+(\boldsymbol{H}_0\boldsymbol{B}+a_{j,0}\boldsymbol{H}_1\boldsymbol{B}+\cdots+a_{j,d}\boldsymbol{H}_{d+1}\boldsymbol{B})\left(\begin{smallmatrix}\boldsymbol{s}_j\\ 0\end{smallmatrix}\right)},\\
\boldsymbol{C}_{6,j} &= g_1^{\boldsymbol{B}\left(\begin{smallmatrix}\boldsymbol{s}_j\\ 0\end{smallmatrix}\right)},
\end{aligned}$$

     and $C_0 = e(g_1,g_2)^{\boldsymbol{\alpha}^\top \boldsymbol{B}\left(\begin{smallmatrix}\boldsymbol{s}_0\\ 0\end{smallmatrix}\right)} \cdot M \in \mathbb{G}_T$.
- $\mathsf{KeyGen}((A,\pi), \mathsf{MSK})$: Upon input an access structure (A,π), where $A \in \mathbb{Z}_N^{m\times k}$ and $\pi : [1,m] \to \mathbb{Z}_N$ for some $m,k \in \mathbb{N}$, do as follows. Parse $\mathsf{MSK} = \alpha$. Pick randomly $\boldsymbol{r}, \boldsymbol{u}, \boldsymbol{r}_1, \ldots, \boldsymbol{r}_m, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k \xleftarrow{\$} \mathbb{Z}_p^{b\times 1}$. Output a secret key $\mathsf{SK} = (\boldsymbol{K}_1, \boldsymbol{K}_2, \boldsymbol{K}_3, \{\boldsymbol{K}_{4,i}, \boldsymbol{K}_{5,i}, \boldsymbol{K}_{6,i,j}\}_{i\in[1,m], j\in[0,d]})$ where

$$\begin{aligned}
\boldsymbol{K}_1 &= g_2^{\boldsymbol{\alpha}+\boldsymbol{H}_{d+2}^\top \boldsymbol{Z}\left(\begin{smallmatrix}\boldsymbol{r}\\ 0\end{smallmatrix}\right)+\boldsymbol{H}_{d+5}^\top \boldsymbol{Z}\left(\begin{smallmatrix}\boldsymbol{u}\\ 0\end{smallmatrix}\right)},\\
\boldsymbol{K}_2 &= g_2^{\boldsymbol{Z}\left(\begin{smallmatrix}\boldsymbol{u}\\ 0\end{smallmatrix}\right)},\\
\boldsymbol{K}_3 &= g_2^{\boldsymbol{Z}\left(\begin{smallmatrix}\boldsymbol{r}\\ 0\end{smallmatrix}\right)},\\
\boldsymbol{K}_{4,i} &= g_2^{A_{i,1}\boldsymbol{H}_{d+3}^\top \boldsymbol{Z}\left(\begin{smallmatrix}\boldsymbol{r}\\ 0\end{smallmatrix}\right)+\sum_{j=2}^{k} A_{i,j}\boldsymbol{Z}\left(\begin{smallmatrix}\boldsymbol{v}_j\\ 0\end{smallmatrix}\right)+\boldsymbol{H}_{d+4}^\top \boldsymbol{Z}\left(\begin{smallmatrix}\boldsymbol{r}_i\\ 0\end{smallmatrix}\right)},\\
\boldsymbol{K}_{5,i} &= g_2^{\boldsymbol{Z}\left(\begin{smallmatrix}\boldsymbol{r}_i\\ 0\end{smallmatrix}\right)},\\
\boldsymbol{K}_{6,i,0} &= g_2^{\boldsymbol{H}_0^\top \boldsymbol{Z}\left(\begin{smallmatrix}\boldsymbol{r}_i\\ 0\end{smallmatrix}\right)},\\
\forall_{j\in[1,d]}\ \boldsymbol{K}_{6,i,j} &= g_2^{\left(\boldsymbol{H}_{j+1}^\top - \pi(i)^j \boldsymbol{H}_1^\top\right)\boldsymbol{Z}\left(\begin{smallmatrix}\boldsymbol{r}_i\\ 0\end{smallmatrix}\right)}.
\end{aligned}$$

- $\mathsf{Decrypt}(\mathsf{CT}, \mathsf{SK})$: Suppose (A, π) accepts the set S. Let $I = \{i \in [1, m] | \pi(i) \in S\}$. Compute coefficients $\{\mu_i\}_{i \in I}$ such that $\sum_{i \in I} \mu_i A_i = (1, 0, \ldots, 0)$.
  Do as follows
  1. For all $i \in I$, do as follows. Let j_i be the index such that $\pi(i) \in S_{j_i}$. (There is such an index since $\pi(i) \in S$ for all $i \in I$). Compute
  $$\boldsymbol{D}_{6,i} := \boldsymbol{K}_{6,i,0} \cdot \boldsymbol{K}_{6,i,1}^{a_{j_1}} \cdots \boldsymbol{K}_{6,i,d}^{a_{j_d}}.$$
  (Also recall that $a_{j,\iota}$ be the coefficient of z^ι in $p_j(z) := \prod_{y \in S_j}(z - y)$).
  2. Compute $e(g_1, g_2)^{\boldsymbol{\alpha}^\top \boldsymbol{B} \binom{\boldsymbol{s}_0}{0}} = L_1 \cdot L_2$ where
  $$L_1 := e(\boldsymbol{C}_1, \boldsymbol{K}_1) e(\boldsymbol{C}_2, \boldsymbol{K}_2)^{-1} e(\boldsymbol{C}_3, \boldsymbol{K}_3)^{-1},$$
  $$L_2 := \prod_{i \in I} \left(e(\boldsymbol{C}_4, \boldsymbol{K}_{4,i}) e(\boldsymbol{C}_{5,\pi(i)}, \boldsymbol{K}_{5,i})^{-1} e(\boldsymbol{C}_{6,\pi(i)}, \boldsymbol{D}_{6,i}) \right)^{\mu_i}.$$
  3. Finally compute $M \leftarrow C_0 / e(g_1, g_2)^{\boldsymbol{\alpha}^\top \boldsymbol{B} \binom{\boldsymbol{s}_0}{0}}$.

Security. The full security of the above scheme follows from the full security of the KP-DSE scheme in [3] and the embedding lemma for our KP-DSE-to-KP-ABE conversion. This is captured in the theorem below. We refer the Matrix Diffie-Hellman Assumption and the Expanded Diffie-Hellman Exponent Assumptions in prime-order subgroups (EDHE3p, EDHE4p) to [3,12], respectively.

Theorem 2. *The above KP-ABE is fully-secure under the $\mathcal{D}_b$-Matrix-DH, $(d+1, \ell)$-$\mathsf{EDHE3p}$, and $(d+1, m, k)$-$\mathsf{EDHE4p}$ Assumptions (in asymmetric prime-order groups), where d is the adjustable integer, $\ell = \lceil |S|/d \rceil$, where S is the ciphertext query, and m, k are the maximum numbers of rows and columns of access matrices among all key queries, respectively. More precisely, for any ppt adversary $\mathcal{A}$, let q_1 denote the number of queries in phase 1, there exist ppt algorithms $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$, whose running times are the same as $\mathcal{A}$ plus some polynomial times, such that for any λ,*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{KP\text{-}ABE}}(\lambda) \leq (2q_1 + 3)\mathsf{Adv}_{\mathcal{B}_1}^{\mathcal{D}_b\text{-}\mathsf{MatDH}}(\lambda) + q_1 \mathsf{Adv}_{\mathcal{B}_2}^{(d+1,m,k)\text{-}\mathsf{EDHE4p}}(\lambda) + \mathsf{Adv}_{\mathcal{B}_3}^{(d+1,\ell)\text{-}\mathsf{EDHE3p}}(\lambda).$$

Proof. This follows immediately from the KP-DSE-to-KP-ABE implication (*i.e.,* Lemma 1 via Lemma 2,3) and the security of the prime-order KP-DSE of [3] (*i.e.,* Theorem 3 in [3] via Theorem 11,12 in [2]).

4 Efficiency Performance

Optimizing Decryption Time. The decryption time of our scheme can be optimized by reducing the number of pairings, which are the dominant operations. This is done by using the identity $\prod_i e(a_i, b) = e(\prod_i a_i, b)$, where we

Table 2. Comparison for asymptotic efficiency among KP-ABE

Scheme	$\|\mathsf{PK}\|$	$\|\mathsf{SK}\|$	$\|\mathsf{CT}\|$	Enc time	Dec time		Unbounded?
					expo.	pair.	
Unbounded ABE of [2,3]	$O(1)$	$O(m)$	$O(t)$	$O(t)$	$O(m)$	$O(m)$	yes
Const.-$\|\mathsf{CT}\|$ ABE of [2,3]	$O(T)$	$O(mT)$	$O(1)$	$O(T)$	$O(mT)$	$O(1)$	no, $T = \max t$
Our new schemes	$O(d)$	$O(md)$	$O(t/d)$	$O(t)$	$O(md)$	$O(\min\{m, t/d\})$	yes

bundle the group-$\mathbb{G}_1$ elements a_i that are paired to the same element of group $\mathbb{G}_2$ (here, it is b).

For simplicity here, we consider the composite-order scheme. The prime-order scheme can be done in a similar manner. In decryption, we can compute the element L_2 also as:

$$L_2 = e(C_4, \prod_{i\in I} K_{4,i}) \cdot \prod_{x=1}^{\ell} \left(e(C_{5,x}, \prod_{\substack{i\in I \\ \text{s.t.} j_i = x}} K_{5,i}^{-\mu_i}) e(C_{6,x}, \prod_{\substack{i\in I \\ \text{s.t.} j_i = x}} D_{6,i}^{\mu_i})\right). \quad (5)$$

The original decryption as in Eq. (4) requires at most $2m+4$ pairings, while the above alternative via Eq. (5) requires $2\ell + 4 = 2t/d + 4$ pairings. To minimize the decryption time, we choose the method of which the cost is the minimum of both.

Beside pairings, the total decryption time also include the cost for exponentiations, which is at most $md+m$ times. Hence, the total decryption time for the composite-order scheme is $c_1(md+m) + c_2(\min\{2m+4, 2t/d+4\})$, where c_1, c_2 are the costs for one exponentiation and one pairing, respectively. When fixing all parameters except d, this amount becomes $k_1 d + k_2/d + k_3$ for some constants k_1, k_2, k_3. This is minimized at d being somewhere in the middle (which will depend on k_1, k_2, k_3). This minimization will be depicted in Fig. 1(d) below. We also note that the min function is reflected at the sharp rigs at the leftmost parts of the graphs in Fig. 1(d).

Comparison for Asymptotic Efficiency. We provide a comparison of asymptotic efficiency among ABE schemes in Table 2. We consider fully-secure schemes that are either completely unbounded or admitting constant-size ciphertexts. The schemes that satisfy this criteria are the unbounded ABE of [2,3] and the

Table 3. Efficiency of our prime-order KP-ABE with $b = 1$. Here we use an example with $m = 40, t = 60$.

Adjust d	$\|\mathsf{PK}\|$	$\|\mathsf{SK}\|$	$\|\mathsf{CT}\|$	Enc time		Dec time	
	(# of $\|\mathbb{G}_1\|$)	(# of $\|\mathbb{G}_2\|$)	(# of $\|\mathbb{G}_1\|$)	expo($\mathbb{G}_1$)	expo($\mathbb{G}_T$)	expo($\mathbb{G}_2$)	pair.
General	$2d + 12$	$2md + 6m + 6$	$4t/d + 8$	$2t + 6t/d$	1	$2md + 2m$	$\min\left\{\begin{smallmatrix} 4m+8, \\ 4t/d+8 \end{smallmatrix}\right\}$
$d = 1$	14	326	248	480	1	160	168
$d = 4$	20	566	68	210	1	400	68
$d = 20$	52	1846	20	138	1	1680	20

Table 4. Concrete efficiency of our KP-ABE from Table 3 when instantiated using BN curves.

Adjust d	|PK| (bits)	|SK| (bits)	|CT| (bits)	Enc time expo($\mathbb{G}_1$)	expo($\mathbb{G}_T$)	Dec time expo($\mathbb{G}_2$)	pair.	total
General	$(2d+12)$ $\times 509$	$(2md+6m+6)$ $\times 255$	$(4t/d+8)$ $\times 509$	$(2t+6t/d)$ $\times 104$	1 $\times 164$	$(2md+2m)$ $\times 57$	$\min\left\{\begin{smallmatrix}4m+8,\\ 4t/d+8\end{smallmatrix}\right\}$ $\times 342$	
$d=1$	7,126	83,130	126,232	49.8 ms	164 μs	9.1 ms	57.4 ms	66.5 ms
$d=4$	10,180	144,330	34,612	20 ms	164 μs	22.8 ms	23.2 ms	46 ms
$d=20$	26,468	470,730	10,180	14.2 ms	164 μs	95.7 ms	6.8 ms	102.5 ms

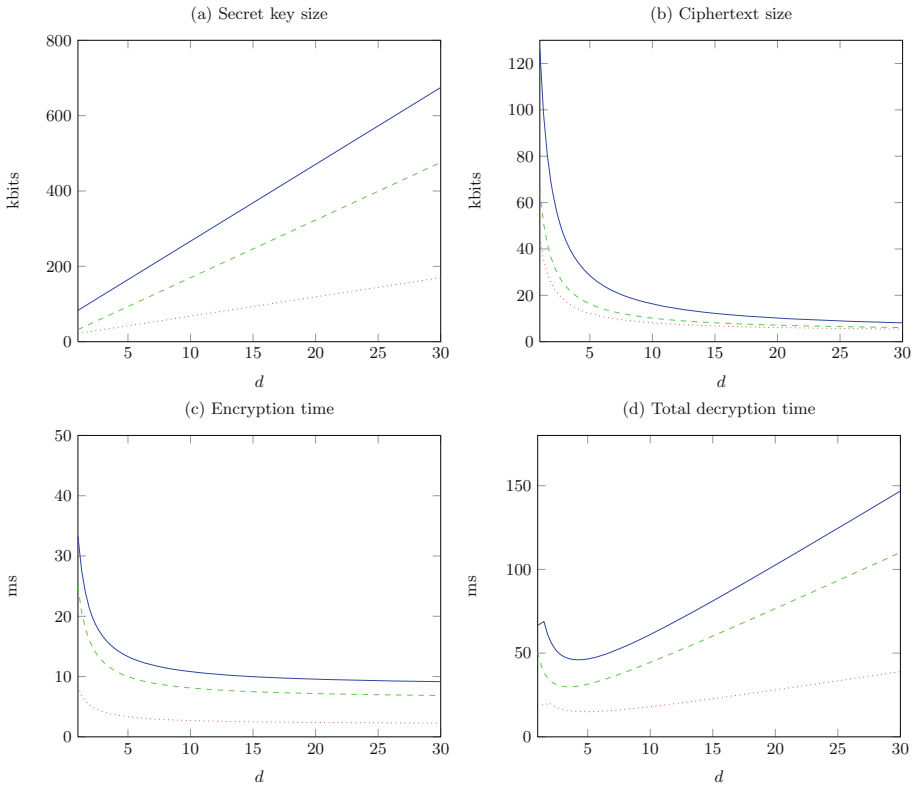

Fig. 1. Efficiency of our scheme when (1) $m = 40, t = 60$ (blue line), (2) $m = 30, t = 30$ (green dashed line), (3) $m = 10, t = 20$ (red dotted line). (Color figure online)

constant-size ciphertext scheme also of [2,3]. All the other schemes in the literature are either only selectively-secure or bounded in some parameters.

Concrete Efficiency. We provide the concrete efficiency of our KP-ABE scheme in prime-order groups. We use the instantiation where $b = 1$, to maximize the efficiency, hence the scheme can be based on the SXDH Assumption [3]. To show concrete performance, we use an example with $m = 40, t = 60$ and

vary $d = 1, 4, 20$ in Table 3. We note that we simply directly count the number of respective operations. This can be further improved by considering multi-exponentiation and multi-pairing algorithms (*e.g.,* [27]); we omit it here.

To obtain an even more concrete picture, we instantiate with the 254-bit Barreto-Naehrig (BN) curves in Table 4. Such curves admits the sizes of group elements as follows: $|\mathbb{G}_1| = 509$, $|\mathbb{G}_2| = 255$, and $|\mathbb{G}_T| = 2032$ bits [1]. As for the time performances in these curves, we refer to the implementation of [27], where exponentiations in $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ take $104, 57, 164$ microseconds, respectively, while a pairing operation takes 342 microseconds.

For ease of viewing, we also plot the graphs for the estimated efficiency in Fig. 1 in three cases: (1) $m = 40, t = 60$, (2) $m = 30, t = 30$, and (3) $m = 10, t = 20$, in blue, green, and red color, respectively.

We can observe that by adjusting d we obtain a tradeoff among size and time performances: the larger d tends to imply the larger public key and private keys but the smaller ciphertext size and the faster encryption time. Interestingly, the total decryption time is minimized somewhere in the middle (*e.g.,* in the case when $m = 40, t = 60$, it is optimized at $d = 4$).

5 Extensions

Ciphertext-Policy, Dual-Policy ABE with Tradeoff. By using the generic *dual conversion* of [7], we immediately obtain also the ciphertext-policy ABE schemes with a similar tradeoff (but somewhat dual) to our KP-ABE schemes. Moreover, by using the generic *dual-policy conversion* also of [7], we obtain the dual-policy ABE [5] with combined tradeoffs from both key-policy and ciphertext-policy parts.

Acknowledgement. A part of this study is supported by SECOM Science and Technology Foundation.

References

1. Aranha, D.F., Karabina, K., Longa, P., Gebotys, C.H., López, J.: Faster explicit formulas for computing pairings over ordinary curves. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 48–68. Springer, Heidelberg (2011)
2. Attrapadung, N.: Dual system encryption via doubly selective security: framework, fully secure functional encryption for regular languages, and more. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 557–577. Springer, Heidelberg (2014)
3. Attrapadung, N.: Dual System Encryption Framework in Prime-Order Groups. IACR Cryptology ePrint Archive, 2015: 390 (2015). https://eprint.iacr.org/2015/390.pdf
4. Attrapadung, N., Hanaoka, G., Yamada, S.: Conversions among several classes of predicate encryption and applications to ABE with various compactness tradeoffs. In: Iwata, T., et al. (eds.) ASIACRYPT 2015. LNCS, vol. 9452, pp. 574–600. Springer, Heidelberg (2015). doi:10.1007/978-3-662-48797-6_24

5. 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)
6. 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)
7. Attrapadung, N., Yamada, S.: Duality in ABE: converting attribute based encryption for dual predicate and dual policy via computational encodings. In: Nyberg, K. (ed.) CT-RSA 2015. LNCS, vol. 9048, pp. 87–105. Springer, Heidelberg (2015)
8. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy (S&P), pp. 321–334 (2007)
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. Chen, J., Gay, R., Wee, H.: Improved dual system abe in prime-order groups via predicate encodings. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 595–624. Springer, Heidelberg (2015)
11. Chen, J., Wee, H.: Semi-adaptive attribute-based encryption and improved delegation for boolean formula. In: Abdalla, M., De Prisco, R. (eds.) SCN 2014. LNCS, vol. 8642, pp. 277–297. Springer, Heidelberg (2014)
12. Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.: An algebraic framework for diffie-hellman assumptions. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 129–147. Springer, Heidelberg (2013)
13. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM CCS 2006, pp. 89–98 (2006)
14. Guillevic, A.: Comparing the pairing efficiency over composite-order and prime-order elliptic curves. In: Jacobson, M., Locasto, M., Mohassel, P., Safavi-Naini, R. (eds.) ACNS 2013. LNCS, vol. 7954, pp. 357–372. Springer, Heidelberg (2013)
15. 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)
16. Kowalczyk, L., Lewko, A.B.: Bilinear entropy expansion from the decisional linear assumption. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9216, pp. 524–541. Springer, Heidelberg (2015)
17. 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)
18. 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)
19. 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)
20. 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)
21. 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)

22. Rouselakis, Y., Waters, B.: Practical constructions and new proof methods for large universe attribute-based encryption. In: ACM CCS 2013, pp. 463–474 (2013)
23. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)
24. Takashima, K.: Expressive attribute-based encryption with constant-size ciphertexts from the decisional linear assumption. In: Abdalla, M., De Prisco, R. (eds.) SCN 2014. LNCS, vol. 8642, pp. 298–317. Springer, Heidelberg (2014)
25. 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)
26. Wee, H.: Dual system encryption via predicate encodings. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 616–637. Springer, Heidelberg (2014)
27. Zavattoni, E., Perez, L.D., Mitsunari, S., Sanchez-Ramirez, A., Teruya, T., Rodriguez-Henriquez, F.: Software implementation of an attribute-based encryption scheme. IEEE Trans. Comput. **64**(5), 1429–1441 (2015)