New Proof Techniques for DLIN-Based Adaptively Secure Attribute-Based Encryption

Katsuyuki Takashima(✉)

Mitsubishi Electric, Kamakura, Japan
Takashima.Katsuyuki@aj.MitsubishiElectric.co.jp

Abstract. We propose *adaptively secure* attribute-based encryption (ABE) schemes for boolean formulas over large universe attributes from the *decisional linear (DLIN) assumption*, which allow *attribute reuse* in an available formula *without the previously employed redundant multiple encoding technique*. Thus our KP-(resp. CP-)ABE has non-redundant ciphertexts (resp. secret keys). For achieving the results, we develop a new encoding method for access policy matrix for ABE, by *decoupling linear secret sharing (LSS)* into its matrix and randomness, and *partially randomizing* the LSS shares in simulation. The new techniques are of independent interest and we expect it will find another application than ABE.

Keywords: Attribute-based encryption · Multi-use attributes in policy · Adaptive security · Static assumption

1 Introduction

1.1 Backgrounds

Attribute-based encryption (ABE) introduced by Sahai and Waters [21] presents an advanced vision for encryption and provides more flexible and fine-grained access control in sharing and distributing sensitive data than traditional symmetric and public-key encryption as well as recent identity-based encryption. In ABE systems, either one of the parameters for encryption and secret key is a set of attributes, and the other is an access policy (structure) over a universe of attributes, e.g., a secret key for a user is associated with an access policy and a ciphertext is associated with a set of attributes. A secret key with a policy can decrypt a ciphertext associated with a set of attributes, iff the attribute set satisfies the policy. If the access policy is for a secret key (resp. for encryption), it is called key-policy ABE (KP-ABE) (resp. ciphertext-policy ABE (CP-ABE)).

All the existing *practical* ABE schemes have been constructed by (bilinear) pairing groups, and the largest class of relations supported by the ABE schemes is (non-monotone or arithmetic) span programs [3,9,12,13] (or (non-monotone) span programs with inner-product relations [18]). While general polynomial size circuits are supported [8,11] recently, they are much less efficient than the

J. Pieprzyk and S. Suriadi (Eds.): ACISP 2017, Part I, LNCS 10342, pp. 85–105, 2017.
DOI: 10.1007/978-3-319-60055-0_5

pairing-based ABE schemes and non-practical when the relations are limited to span programs. Hereafter, we focus on pairing-based ABE with span program access structures. An example of such span program predicate over attributes is given by (Institute = Univ. A) AND ((Department = Biology) OR (Position = Professor)), which we simply denote by $\mathcal{X}_1 \wedge (\mathcal{X}_2 \vee \mathcal{X}_3)$ where $\mathcal{X}_1 :=$ Univ. A, $\mathcal{X}_2 :=$ Biology and $\mathcal{X}_3 :=$ Professor. We define attribute-multiplicity k for a predicate as the maximum number of appearances of attribute variables, i.e., $k = 2$ for predicate $(\mathcal{X}_1 \wedge \mathcal{X}_2) \vee (\mathcal{X}_1 \wedge \mathcal{X}_3) \vee (\mathcal{X}_2 \wedge \mathcal{X}_4)$ since $\mathcal{X}_1$ and $\mathcal{X}_2$ appear twice and others appear just once. While adaptive security for ABE is the standard, realistic and desirable security notion, previously, either efficiency or security is sacrificed for achieving the "multi-use" property in adaptively secure ABE. See adaptively secure ABE in Tables 1 and 2. Our aim is to achieve *short (i.e., non-redundant) ciphertexts (resp. keys)* in *adaptively secure multi-use* KP-ABE (resp. CP-ABE) from *static assumptions*.

In previous *static* assumption based schemes [9,14,18], for allowing reuse of attributes in a policy in the adaptive security setting, for example, in KP-ABE, multiple ciphertext components whose number is linear in the product kn' of the number n' of attributes for the ciphertext and the attribute multiplicity k for available policies are necessary, which leads to a very long ciphertext. More precisely, the same information representing attribute set Γ is duplicated over *multiple* ciphertext components depending linearly on the multiplicity k. (See OT10 and CGW15 KP-ABE schemes in Table 1.)

Lewko-Waters [16] first constructed adaptively-secure CP-ABE and KP-ABE schemes for span programs with allowing reuse of attributes in a policy *without the above redundant multiple encoding technique*. While Lewko-Waters's (CP-) ABE scheme ([16] and subsequent work [2,3] in Table 1) shows an interesting approach to allowing reuse of attributes in a policy, the security is proven only based on *q-type assumptions* with q the maximum number of attribute-multiplicities in access structures. However, the assumptions (and also the associated schemes) suffered a special attack which was presented by Cheon [10] at Eurocrypt 2006, which leads to inefficiency. Consequently, it is very desirable that the q-type assumption should be replaced by a *static* (non-q type) assumption with keeping compact ciphertexts.

Moreover, we note that there exist *no multi-use* CP-ABE scheme with short, i.e., non-redundant, secret keys *even in the selective security setting* from *a static assumption* (Table 2). Now, an important open question is:

> *Is there an adaptively secure KP-(resp. CP-)ABE scheme for span programs from a static (standard) assumption whose ciphertext (resp. secret key) size is not linear in kn' for the attribute number n' in ciphertext (resp. secret key) and the maximum attribute-multiplicity k of available policies ?*

This work makes a significant step for addressing the problem.

1.2 Our Results

We obtain the following results.

Table 1. Comparison with the existing pairing-based multi-use KP-ABE schemes, where PK, SK, CT stand for public key, secret key, ciphertext, respectively, and n' represents the number of attributes in CT, n the max of n', ℓ the number of rows in access matrix in SK, r the max of the number of columns in access matrix in SK, k (the max of) the "attribute-multiplicity" of an access matrix in SK, respectively. The fourth row describes the warm-up scheme in Sect. 5.3.

	Security	Assump.	PK size	SK size	CT size
GPSW06 [12]	Selective	DBDH	$O(n)\|\mathbb{G}\|$	$O(\ell)\|\mathbb{G}\|$	$O(n')\|\mathbb{G}\|$
Tak14 [22]	Semi-adaptive	DLIN	$O(n)\|\mathbb{G}\|$	$O(\ell n)\|\mathbb{G}\|$	$O(1)\|\mathbb{G}\|$
(Warm-up)				$O(\ell)\|\mathbb{G}\|$	$O(n)\|\mathbb{G}\|$
OT10 [18]	Adaptive	DLIN	$O(n)\|\mathbb{G}\|$	$O(\ell)\|\mathbb{G}\|$	$O(kn')\|\mathbb{G}\|$
LW12 [16]		ℓ-Parallel BDHE $(+\alpha)$	$O(n)\|\mathbb{G}\|$	$O(\ell)\|\mathbb{G}\|$	$O(n')\|\mathbb{G}\|$
Att15 [2,3]		EDHE3 & 4 parametrized by n, ℓ, r	$O(n)\|\mathbb{G}\|$	$O(\ell n)\|\mathbb{G}\|$	$O(1)\|\mathbb{G}\|$
CGW15 [9]		s-Lin for $\forall s$	$O(n)\|\mathbb{G}\|$ for $s = 2$	$O(\ell)\|\mathbb{G}\|$ for $s = 2$	$O(kn')\|\mathbb{G}\|$ for $s = 2$
Proposed	Adaptive	DLIN	$O(n + r)\|\mathbb{G}\|$	$O(\ell)\|\mathbb{G}\|$	$O(n + r)\|\mathbb{G}\|$

- We propose an adaptively secure *multi-use* KP-ABE construction for boolean formulas (or span programs) over large universe attribute matching predicates *with non-redundant ciphertexts from the DLIN assumption* (in Sect. 5). The size of a ciphertext for attributes *is not linear in the product kn' of the number of ciphertext attributes n' and the attribute multiplicity k in available access structures*, but has only a linear dependence on some size parameter r of access structures. For comparison with existing ones, refer to Table 1.
- We also propose an adaptively secure multi-use CP-ABE construction for the same access structures as the above KP-ABE with short (non-redundant) keys from DLIN. The CP-ABE scheme is obtained from the above KP-ABE by the natural dual conversion, in particular, the key size *is not linear in kn' for the number n' of key attributes and the attribute multiplicity k in available access structures*. We note that it is *the first multi-use CP-ABE construction with short keys from a static assumption even including the selective secure schemes* (Table 2). For the concrete scheme, see Appendix B.

We used two techniques, decoupling of linear secret sharing (LSS) into two (dual) components, i.e., span program matrix and randomness, and the partial randomization of LSS. A new sparse matrix machinery (Sect. 4) underlies them. The techniques can be extended naturally to arithmetic span programs (ASP), then, our results can be extended to ASP based ABE proposed by Ishai and Wee [13].

Table 2. Comparison with the existing pairing-based multi-use CP-ABE schemes, where PK, SK, CT stand for public key, secret key, ciphertext, respectively, and n' represents the number of attributes in SK, n the max of n', ℓ the number of rows in access matrix in CT, r the max of the number of columns in access matrix in CT, k (the max of) the "attribute-multiplicity" of an access matrix in CT, respectively.

	Security	Assump.	PK size	SK size	CT size
Wat11 [25] Scheme 2	Selective	ν-BDHE	$O(n)\|\mathbb{G}\|$	$O(kn')\|\mathbb{G}\|$	$O(\ell)\|\mathbb{G}\|$
Wat11 [25] Scheme 3		DBDH	$O(nr)\|\mathbb{G}\|$	$O(kn'+r)\|\mathbb{G}\|$	$O(\ell^2)\|\mathbb{G}\|$
AHY15 [4][a]		Parameterized	$O((n\ell)^2\lambda)\|\mathbb{G}\|$	$O((n\ell)^4\lambda^2)\|\mathbb{G}\|$	$O(1)\|\mathbb{G}\|$
OT10 [18]	Adaptive	DLIN	$O(n)\|\mathbb{G}\|$	$O(kn')\|\mathbb{G}\|$	$O(\ell)\|\mathbb{G}\|$
LW12 [16]		ℓ-Parallel BDHE $(+\alpha)$	$O(n)\|\mathbb{G}\|$	$O(n')\|\mathbb{G}\|$	$O(\ell)\|\mathbb{G}\|$
CGW15 [9]		s-Lin for $\forall s$	$O(n)\,\|\mathbb{G}\|$ for $s=2$	$O(kn')\|\mathbb{G}\|$ for $s=2$	$O(\ell)\|\mathbb{G}\|$ for $s=2$
Proposed	Adaptive	DLIN	$O(n+r)\|\mathbb{G}\|$	$O(n+r)\|\mathbb{G}\|$	$O(\ell)\|\mathbb{G}\|$

[a] Since $k \leq \ell$, the size of secret keys of the AHY15 scheme [4] is very large compared with others. Also, in [1], a *selective-secure* constant-size ciphertext, but, large secret keys CP-ABE scheme was proposed, recently

1.3 Key Techniques

Our results are related to KP- and CP-ABEs, however, for simplicity, we mainly treat on KP-ABE. According to a new framework introduced by Attrapadung, doubly selective security (i.e., selective and co-selective) leads to achieving adaptive one. Since selective security is easily obtained in KP-ABE, we should concentrate on achieving *co-selectively* secure KP-ABE below.

Based on the technique in [5,22], we have DLIN-based, multi-use and *semi-adaptively* secure KP-ABE with short ciphertext size. We give the underlying scheme in Sect. 5.3 (as a warm-up) and extend it to our adaptive one. Here, access structure $\mathbb{S}$ is given by $\ell \times r$ matrix M and each row $M_i \in \mathbb{F}_q^r$ of the matrix is associated to an attribute value by a map ρ, i.e., labeled with attributes $v_i := \rho(i)$. An attribute set Γ satisfies $\mathbb{S}$ iff $\vec{1} \in \mathsf{span}\langle M_i \,|\, v_i \in \Gamma\rangle$ for a fixed special (all-one) vector $\vec{1}$. First, to achieve short ciphertexts in the underlying KP-ABE, attributes $\Gamma := \{x_j\}_{j=1,\ldots,n'}$ are encoded in an n-dimensional (with $n \geq n'+1$) vector $\vec{y} := (y_1, \ldots, y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \prod_{j=1}^{n'} (z - x_j)$. Each (non-zero) attribute value v_i (for $i = 1, \ldots, \ell$) associated with a row of access structure matrix M (in $\mathbb{S}$) is encoded as $\vec{v}_i := (v_i^{n-1}, \ldots, v_i, 1)$, so $\vec{y} \cdot \vec{v}_i = v_i^{n-1-n'} \prod_{j=1}^{n'} (v_i - x_j)$, and the value of inner product is equal to zero if and only if $v_i = x_j$ for some j, i.e., $v_i \in \Gamma$. Here, the relation between $\mathbb{S}$ and Γ is determined by the multiple inner product values $\vec{y} \cdot \vec{v}_i$ for one vector $\vec{y}$ which is equivalent to Γ. As in previous works (e.g., [5,22]), a ciphertext element $\boldsymbol{c}_1$ is encoded with $\omega\vec{y}$ (for random ω), and key elements $\boldsymbol{k}_i^*$ are encoded with $\vec{v}_i$ and shared secret values $M_i \cdot \vec{f}$ $(i = 1, \ldots, \ell)$ for a central secret $\vec{1} \cdot \vec{f}$ with uniformly random $\vec{f}$, respectively. We change the encoding method for our new proof method as indicated below.

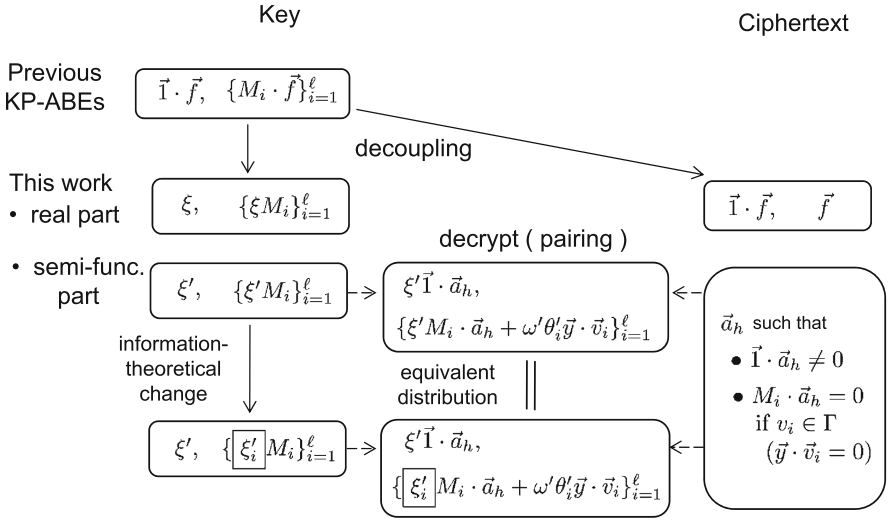

Fig. 1. Decoupling of LSS matrix from randomness and partial LSS randomization in semi-functional parts. Here, $(M=(M_i),\rho)$ is an access structure, uniformly random $\vec{f}\xleftarrow{\cup}\mathbb{F}_q^r, \xi, \xi', \xi_i', \theta_i'\xleftarrow{\cup}\mathbb{F}_q, \vec{y}:=(y_1,\ldots,y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j}z^j = z^{n-1-n'}\prod_{j=1}^{n'}(z-x_j)$, and $\vec{v}_i:=(v_i^{n-1},\ldots,v_i,1)$ for $v_i:=\rho(i)$.

Basic Idea: Decoupling of LSS Matrix from Randomness. Secret keys in all previous KP-ABE schemes contain shared secret values $s_0:=\vec{1}\cdot\vec{f}$ and $s_i:=M_i\cdot\vec{f}$, which means that randomness $\vec{f}$ is fixed at the key generation phase. Moreover, since, for *pre-challenge* queried keys (in simulation), the challenge $\vec{y}$ is not yet revealed to the challenger, i.e., simulator, at the query phase, we have never had a co-selective simulation strategy for achieving compact ciphertexts together with multi-use leaf attributes v_i in the queried access matrix.

For addressing the problem, we change an encoding method of LSS (Fig. 1). First, we decouple LSS encoding into LSS matrix and randomness, and randomness is encoded on the ciphertext side. (Then, the simulation of the randomness is delayed until the challenge phase.) Precisely, in the secret key, concatenated $V_i:=(\theta_i\vec{v}_i,\xi M_i)\in\mathbb{F}_q^{n+r}$ are encoded in the i-th component $\boldsymbol{k}_i^*$ for $i=1,..,\ell$ with random θ_i,ξ. We note that the key component $\boldsymbol{k}_i^*$ has no randomness for LSS (except for connecting randomness ξ), instead, LSS matrix $M:=(M_i)_{i=1}^{\ell}$ is directly encoded in $\{\boldsymbol{k}_i^*\}$. In ciphertext, $Y:=(\omega\vec{y},\vec{f})\in\mathbb{F}_q^{n+r}$ is encoded. Hence, in decryption, inner-product values are

$$Y\cdot V_i=\omega\theta_i(\vec{y}\cdot\vec{v}_i)+\xi M_i\cdot\vec{f}=\omega\theta_i(\vec{y}\cdot\vec{v}_i)+\xi s_i\ \ \text{for } i=1,\ldots,\ell,$$

therefore, if $\vec{y}\cdot\vec{v}_i=0$, secret share ξs_i for central secret ξs_0 is obtained, and if $\vec{y}\cdot\vec{v}_i\neq 0$, s_i is totally hidden from the decryptor since θ_i is freshly random.

New Proof Techniques: Partial LSS Randomization in Simulation and New Underlying Lemma. At the top level of strategy of the security proof,

we follow the dual system encryption methodology proposed by Waters [24]. The above change of encoding enables the simulator to simulate the randomness of LSS depending on both of the h-th queried access structure $\mathbb{S} := (M, \rho)$ and attributes $\Gamma := \{x_t\}$ (equivalently, vector $\vec{y}$). We use the simulated randomness $\vec{a}_h$, which is *not fully random in* $\mathbb{F}_q^r$, but satisfies $M_i \cdot \vec{a}_h = 0$ if $v_i \in \Gamma$ and $\vec{1} \cdot \vec{a}_h \neq 0$. Such a vector exists since Γ does not satisfy $\mathbb{S}$, and it has been used for security in previous works, for example, in [12]. In ciphertext, the concatenated vector $Y' := (\omega' \vec{y}, \vec{a}_h) \in \mathbb{F}_q^{n+r}$ is encoded in the semi-functional space. And, in the semi-functional space of the h-th queried key, $V_i' := (\theta_i' \vec{v}_i, \xi' M_i) \in \mathbb{F}_q^{n+r}$ are encoded in the i-th component $\boldsymbol{k}_i^*$ for $i = 1, .., \ell$. Since V_i' is *independent of* Γ, it can be simulated for the *pre-challenge* key. Then,

$$Y' \cdot V_i' = \omega' \theta_i' (\vec{y} \cdot \vec{v}_i) + \xi' M_i \cdot \vec{a_h} = \begin{cases} 0 & \text{if } \vec{y} \cdot \vec{v}_i = 0, \\ \omega' \theta_i' (\vec{y} \cdot \vec{v}_i) + \xi' M_i \cdot \vec{a_h} & \text{if } \vec{y} \cdot \vec{v}_i \neq 0, \end{cases}$$

for $i = 1, \ldots, \ell$. Here, if $\vec{y} \cdot \vec{v}_i \neq 0$, $Y' \cdot V_i'$ is uniformly random and independent from other variables since θ_i' are freshly random. Let $V_i'' := (\theta_i' \vec{v}_i, \xi_i' M_i) \in \mathbb{F}_q^{n+r}$ with uniformly random ξ_i' which are independent of each other for $i = 1, \ldots, \ell$.

$$Y' \cdot V_i'' = \omega' \theta_i' (\vec{y} \cdot \vec{v}_i) + \xi_i' M_i \cdot \vec{a_h} = \begin{cases} 0 & \text{if } \vec{y} \cdot \vec{v}_i = 0, \\ \omega' \theta_i' (\vec{y} \cdot \vec{v}_i) + \xi_i' M_i \cdot \vec{a_h} & \text{if } \vec{y} \cdot \vec{v}_i \neq 0, \end{cases}$$

for $i = 1, \ldots, \ell$. Again, if $\vec{y} \cdot \vec{v}_i \neq 0$, $Y' \cdot V_i''$ is uniformly random and independent of other variables. That is, $Y' \cdot V_i'$ and $Y' \cdot V_i''$ are equivalently distributed. Therefore, we can conceptually change V_i' which contains variable ξ' to V_i'' with *no* ξ' by using the pairwise independence lemma (Lemma 3) as in the previous dual system encryption proofs. We stress that V_i'' *are also independent of the challenge attributes* Γ, and then can be used in the pre-challenge key simulation. In this way, we can sequentially eliminate the randomness ξ' from all key components, $\boldsymbol{k}_i^*$ for $i = 1, .., \ell$, *except for* $\boldsymbol{k}_0^*$, and finally, ξ' remains only in the central element $\boldsymbol{k}_0^*$, and the inner-product of the semi-functional parts of $\boldsymbol{k}_0^*$ and the corresponding ciphertext component is uniformly random value $\xi' \vec{1} \cdot \vec{a}_h$ since $\vec{1} \cdot \vec{a}_h \neq 0$. So, the proof proceeds successfully (See Sect. 5.4 for proof outline).

We extend the sparse matrix technique on dual pairing vector spaces (DPVS) developed in [19,22] for achieving compact ciphertexts. Refer to Sect. 5.1 for the details.

1.4 Notations

When A is a random variable or distribution, $y \xleftarrow{\mathsf{R}} A$ denotes that y is randomly selected from A according to its distribution. When A is a set, $y \xleftarrow{\mathsf{U}} A$ denotes that y is uniformly selected from A. We denote the finite field of order q by $\mathbb{F}_q$, and $\mathbb{F}_q \setminus \{0\}$ by $\mathbb{F}_q^\times$. A vector symbol denotes a vector representation over $\mathbb{F}_q$, e.g., $\vec{y}$ denotes $(y_1, \ldots, y_n) \in \mathbb{F}_q^n$. For two vectors $\vec{y} = (y_1, \ldots, y_n)$ and $\vec{v} = (v_1, \ldots, v_n)$, $\vec{y} \cdot \vec{v}$ denotes the inner-product $\sum_{i=1}^n y_i v_i$. X^{T} denotes the transpose of matrix X. A bold face letter denotes an element of vector space $\mathbb{V}$, e.g.,

$\boldsymbol{x} \in \mathbb{V}$. When $\boldsymbol{b}_i \in \mathbb{V}$ $(i = 1, \ldots, n)$, $\mathsf{span}\langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \rangle \subseteq \mathbb{V}$ (resp. $\mathsf{span}\langle \vec{x}_1, \ldots, \vec{x}_n \rangle$) denotes the subspace generated by $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ (resp. $\vec{x}_1, \ldots, \vec{x}_n$). For bases $\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N)$ and $\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_N^*)$, $(x_1, \ldots, x_N)_{\mathbb{B}} := \sum_{i=1}^{N} x_i \boldsymbol{b}_i$ and $(y_1, \ldots, y_N)_{\mathbb{B}^*} := \sum_{i=1}^{N} y_i \boldsymbol{b}_i^*$. $\vec{e}_j$ denotes the canonical basis vector $(\overbrace{0 \cdots 0}^{j-1}, 1, \overbrace{0 \cdots 0}^{n+r-j}) \in \mathbb{F}_q^{n+r}$ for positive integers n and r. $GL(n, \mathbb{F}_q)$ denotes the general linear group of degree n over $\mathbb{F}_q$.

2 Dual Pairing Vector Spaces (DPVS)

In this paper, for simplicity of description, we will present the proposed schemes on the symmetric version of dual pairing vector spaces (DPVS) [17] constructed using symmetric bilinear pairing groups given in Definition 1. Owing to the abstraction of DPVS, the presentation and the security proof of the proposed schemes are essentially the same as those on the asymmetric version of DPVS.

Definition 1. *"Symmetric bilinear pairing groups"* $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ *are a tuple of a prime* q*, cyclic additive group* $\mathbb{G}$ *and multiplicative group* $\mathbb{G}_T$ *of order* q*,* $G \neq 0 \in \mathbb{G}$*, and a polynomial-time computable nondegenerate bilinear pairing* $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ *i.e.,* $e(sG, tG) = e(G, G)^{st}$ *and* $e(G, G) \neq 1$*. Let* $\mathcal{G}_{\mathsf{bpg}}$ *be an algorithm that takes input* 1^λ *and outputs a description of bilinear pairing groups* $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ *with security parameter* λ*.*

"Dual pairing vector spaces (DPVS)" of dimension N *by a direct product of symmetric pairing groups* $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ *are given by prime* q*,* N*-dimensional vector space* $\mathbb{V} := \overbrace{\mathbb{G} \times \cdots \times \mathbb{G}}^{N}$ *over* $\mathbb{F}_q$*, cyclic group* $\mathbb{G}_T$ *of order* q*, and pairing* $e : \mathbb{V} \times \mathbb{V} \to \mathbb{G}_T$*. The pairing is defined by* $e(\boldsymbol{x}, \boldsymbol{y}) := \prod_{i=1}^{N} e(G_i, H_i) \in \mathbb{G}_T$ *where* $\boldsymbol{x} := (G_1, \ldots, G_N) \in \mathbb{V}$ *and* $\boldsymbol{y} := (H_1, \ldots, H_N) \in \mathbb{V}$*. This is nondegenerate bilinear i.e.,* $e(s\boldsymbol{x}, t\boldsymbol{y}) = e(\boldsymbol{x}, \boldsymbol{y})^{st}$ *and if* $e(\boldsymbol{x}, \boldsymbol{y}) = 1$ *for all* $\boldsymbol{y} \in \mathbb{V}$*, then* $\boldsymbol{x} = \boldsymbol{0}$*.*

3 Definition of KP-ABE

3.1 Span Programs and Access Structures

Definition 2 (Span Programs [6] and Access Structures). $\mathcal{U}$ $(\subset \{0,1\}^*)$ *is a universe, a set of attributes, which is expressed by a value of attribute, i.e.,* $v \in \mathbb{F}_q^\times (:= \mathbb{F}_q \setminus \{0\})$*. A span program over* $\mathbb{F}_q$ *is a labeled matrix* $\mathbb{S} := (M, \rho)$ *where* M *is a* $(\ell \times r)$ *matrix over* $\mathbb{F}_q$ *and* ρ *is a labeling of the rows of* M *by literals from* $\{v, v', \ldots\}$ *(every row is labeled by one literal), i.e.,* $\rho : \{1, \ldots, \ell\} \to \{v, v', \ldots\}$*. A span program accepts or rejects an input by the following criterion. Let* Γ *be a set of attributes, i.e.,* $\Gamma := \{x_j\}_{1 \leq j \leq n'}$ $(x_j \in \mathbb{F}_q^\times)$*. The span program* $\mathbb{S}$ *accepts* Γ *if and only if* $\vec{1} \in \mathsf{span}\langle (M_i)_{\rho(i) = v_i \in \Gamma} \rangle$*, i.e., some linear combination of the rows* $(M_i)_{\rho(i) \in \Gamma}$ *gives the all one vector* $\vec{1}$*.*

No row M_i $(i = 1, \ldots, \ell)$ of the matrix M is $\vec{0}$.
We now construct a secret-sharing scheme for a (monotone) span program.

Definition 3. *A secret-sharing scheme for span program $\mathbb{S} := (M, \rho)$ is:*

1. *Let M be $\ell \times r$ matrix. Let column vector $\vec{f} := (f_1, \ldots, f_r) \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$. Then, $s_0 := \vec{1} \cdot \vec{f} = \sum_{k=1}^{r} f_k$ is the secret to be shared, and $\vec{s} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$ is the ℓ shares of the secret s_0 and the share s_i belongs to $\rho(i)$.*
2. *If span program $\mathbb{S} := (M, \rho)$ accepts Γ, i.e., $\vec{1} \in \mathsf{span}\langle (M_i)_{\rho(i) \in \Gamma} \rangle$, there exist constants $\{\alpha_i \in \mathbb{F}_q \mid i \in I\}$ such that $I \subseteq \{i \in \{1, \ldots, \ell\} \mid \rho(i) \in \Gamma\}$ and $\sum_{i \in I} \alpha_i s_i = s_0$. Furthermore, these constants $\{\alpha_i\}$ can be computed in time polynomial in the size of the matrix M.*

3.2 Key-Policy Attribute-Based Encryption (KP-ABE)

In key-policy attribute-based encryption (KP-ABE), encryption (resp. a secret key) is associated with attributes Γ (resp. access structure $\mathbb{S}$). Relation R for KP-ABE is defined as $R(\mathbb{S}, \Gamma) = 1$ iff access structure $\mathbb{S}$ accepts Γ.

Definition 4 (Key-Policy Attribute-Based Encryption: KP-ABE). *A key-policy attribute-based encryption scheme consists of probabilistic polynomial-time algorithms* $\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}$ *and* Dec. *They are given as follows:*

Setup *takes as input security parameter 1^λ, a bound n on the number of attributes per ciphertext and a bound r on the number of columns of an access matrix in a secret key. It outputs public parameters* pk *and master secret key* sk.

KeyGen *takes as input public parameters* pk, *master secret key* sk, *and access structure $\mathbb{S} := (M, \rho)$. It outputs a corresponding secret key* $\mathsf{sk}_{\mathbb{S}}$.

Enc *takes as input public parameters* pk, *message m in some associated message space* msg, *and a set of attributes, $\Gamma := \{x_j\}_{j=1}^{n'}$. It outputs a ciphertext* ct_Γ.

Dec *takes as input public parameters* pk, *secret key* $\mathsf{sk}_{\mathbb{S}}$ *for access structure $\mathbb{S}$, and ciphertext* ct_Γ *that was encrypted under a set of attributes Γ. It outputs either $m' \in \mathsf{msg}$ or the distinguished symbol $\perp$.*

A KP-ABE scheme should have the correctness: for all $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda, n, r)$, all access structures $\mathbb{S}$, all secret keys $\mathsf{sk}_{\mathbb{S}} \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \mathbb{S})$, all messages m, all attribute sets Γ, all ciphertexts $\mathsf{ct}_\Gamma \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, m, \Gamma)$, it holds that $m = \mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_{\mathbb{S}}, \mathsf{ct}_\Gamma)$ if $\mathbb{S}$ accepts Γ. Otherwise, it holds with negligible probability.

Definition 5 (Adaptive Security). *The model for defining the adaptively payload-hiding security of KP-ABE under chosen plaintext attack is given by the following game:*

Setup. *In the adaptive security, the challenger runs the setup,* $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda, n, r)$, *and gives public parameters* pk *to the adversary.*

Phase 1. *The adversary is allowed to adaptively issue a polynomial number of key queries,* $\mathbb{S}$*, to the challenger. The challenger gives* $\mathsf{sk}_{\mathbb{S}} \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \mathbb{S})$ *to the adversary.*

Challenge. *The adversary submits two messages* $m^{(0)}, m^{(1)}$*, and a challenge attribute set,* Γ*, provided that no* $\mathbb{S}$ *queried to the challenger in Phase 1 accepts* Γ*. The challenger flips a coin* $b \xleftarrow{\mathsf{U}} \{0,1\}$*, and computes* $\mathsf{ct}_{\Gamma}^{(b)} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, m^{(b)}, \Gamma)$*. It gives* $\mathsf{ct}_{\Gamma}^{(b)}$ *to the adversary.*

Phase 2. *Phase 1 is repeated with the restriction that no queried* $\mathbb{S}$ *accepts challenge* Γ*.*

Guess. *The adversary outputs a guess* b' *of* b*, and wins if* $b' = b$*.*

The advantage of adversary $\mathcal{A}$ *in the adaptive game is defined as* $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{KP\text{-}ABE}}(\lambda) := \Pr[\mathcal{A} \text{ wins}] - 1/2$ *for any* λ*. A KP-ABE scheme is adaptively payload-hiding secure if all poly-time adversaries have at most a negligible advantage in the game.*

Remark 1. The challenge Γ is declared by the adversary just before **Phase 1** (resp. before **Setup**) in the semi-adaptive (resp. selective) game, and the corresponding security notions are defined in the similar manner as above.

4 Special Matrix Subgroups

Let $n \geq 2$ and $\tilde{n} := n + r$. Lemmas 1, 2 and 3 are key lemmas for the security proof for our KP- and CP-ABE schemes.

We start by a motivational argument for introducing our new sparse matrix technique. Previous sparse matrices in DPVS [19,22] are given by the form whose diagonal element except for the first one is the same denoted by u. (For the sparse-matrix DPVS and modified pairwise independence lemma, refer to Sect. 5.4 in [20].) For achieving our information theoretical change from (Y', V_i') to (Y', V_i'') described in Sect. 1.3, we use one more randomness in diagonal elements, i.e., two random u_1 and u_2, as given in Eq. (1). More precisely, random $U \xleftarrow{\mathsf{U}} \mathcal{H}(n, r, \mathbb{F}_q)$ acts on $\mathbb{F}_q^{n+r} = \mathbb{F}_q^n \times \mathbb{F}_q^r$ by using different scalars u_1 and u_2 on the first $\mathbb{F}_q^n$ and the second $\mathbb{F}_q^r$ respectively. The new sparse matrix action is the key fact for proving Lemma 3. For positive integers n and r, let

$$\mathcal{H}(n, r, \mathbb{F}_q) := \left\{ \left(\begin{array}{ccccccc} u_1' & & & & & & \\ u_2' & u_1 & & & & & \\ \vdots & & \ddots & & & & \\ u_n' & & & u_1 & & & \\ u_{n+1}' & & & & u_2 & & \\ \vdots & & & & & \ddots & \\ u_{n+r}' & & & & & & u_2 \end{array} \right) \middle| \begin{array}{l} u_1, u_2, u_l' \in \mathbb{F}_q \\ \quad \text{for } l = 1, \ldots, n+r, \\ \text{a blank element} \\ \text{in the matrix} \\ \text{denotes } 0 \in \mathbb{F}_q \end{array} \right\}, \quad (1)$$

and $\mathcal{H}(n, r, \mathbb{F}_q)^{\times} := \mathcal{H}(n, r, \mathbb{F}_q) \cap GL(\tilde{n}, \mathbb{F}_q)$.

Lemma 1. *$\mathcal{H}(n, r, \mathbb{F}_q)^\times$ is a subgroup of $GL(\tilde{n}, \mathbb{F}_q)$, where $\tilde{n} := n + r$.*

Lemma 1 is directly verified from the definition of groups. □

Let

$$X_{i,j} := \begin{pmatrix} \mu'_{i,j,1} & & & & & & & & \\ \mu'_{i,j,2} & \mu_{i,j,1} & & & & & & & \\ \vdots & & \ddots & & & & & & \\ \mu'_{i,j,n} & & & \mu_{i,j,1} & & & & & \\ \mu'_{i,j,n+1} & & & & \mu_{i,j,2} & & & & \\ \vdots & & & & & \ddots & & & \\ \mu'_{i,j,n+r} & & & & & & \mu_{i,j,2} & & \end{pmatrix} \in \mathcal{H}(n, r, \mathbb{F}_q) \text{ for } i, j = 1, \ldots, 5 \quad (2)$$

and using $X_{i,j}$, we define

$$\mathcal{L}(5, n, r, \mathbb{F}_q) := \left\{ X := \begin{pmatrix} X_{1,1} \cdots X_{1,5} \\ \vdots \quad\quad \vdots \\ X_{5,1} \cdots X_{5,5} \end{pmatrix} \middle| \begin{array}{l} X_{i,j} \in \mathcal{H}(n, r, \mathbb{F}_q) \\ \text{for } i, j = 1, \ldots, 5 \end{array} \right\} \bigcap GL(5\tilde{n}, \mathbb{F}_q). \quad (3)$$

Lemma 2. *$\mathcal{L}(5, n, r, \mathbb{F}_q)$ is a subgroup of $GL(5\tilde{n}, \mathbb{F}_q)$.*

Lemma 2 is given in a similar manner as Lemma 2 in the full version of [19]. For the proof, see the full version of this paper [23]. Next is a generalization of Lemma 6 in [19].

Lemma 3. *Let $\vec{e}_j := (0, \ldots, 0, \overset{j}{1}, 0, \ldots, 0) \in \mathbb{F}_q^{n+r}$.*

For all $\vec{v} = (v_1, \ldots, v_n, 0, \ldots, 0) \in \mathsf{span}\langle \vec{e}_1, .., \vec{e}_n \rangle \setminus \mathsf{span}\langle \vec{e}_1 \rangle$, $\vec{\kappa} = (0, \ldots, 0, \kappa_1, \ldots, \kappa_r) \in \mathsf{span}\langle \vec{e}_{n+1}, .., \vec{e}_{n+r} \rangle$ and $\pi \in \mathbb{F}_q$, let

$$W_{\vec{v},\vec{\kappa},\pi} := \{(\vec{w}, \vec{z}) \in (\mathsf{span}\langle \vec{e}_1, \vec{v}, \vec{\kappa} \rangle \setminus \mathsf{span}\langle \vec{e}_1 \rangle) \times (\mathbb{F}_q^{n+r} \setminus \mathsf{span}\langle \vec{e}_1 \rangle^\perp) \mid \vec{w} \cdot \vec{z} = \pi\}.$$

For all $(\vec{v}, \vec{\kappa}, \vec{x}) \in (\mathsf{span}\langle \vec{e}_1, .., \vec{e}_n \rangle \setminus \mathsf{span}\langle \vec{e}_1 \rangle) \times \mathsf{span}\langle \vec{e}_{n+1}, .., \vec{e}_{n+r} \rangle \times \left(\mathbb{F}_q^{n+r} \setminus \mathsf{span}\langle \vec{e}_1 \rangle^\perp\right)$, and $U \xleftarrow{\cup} \mathcal{H}(n, r, \mathbb{F}_q)^\times, Z := (U^{-1})^{\mathrm{T}}$, the pair $((\vec{v}+\vec{\kappa})U, \vec{x}Z)$ is uniformly distributed in $W_{\vec{v},\vec{\kappa},(\vec{v}+\vec{\kappa})\cdot\vec{x}}$ except with negligible probability.

For the proof, see the full version of this paper [23].

5 Adaptively Secure Multi-Use KP-ABE Scheme with Short Ciphertexts

5.1 Key Ideas in Constructing the Proposed KP-ABE Scheme

We extend the techniques developed in [22], where the author presented a semi-adaptively secure KP-ABE with constant-size ciphertexts by using sparse matrix DPVS approach. An underlying construction of our proposed one is given in Sect. 5.3, which is a dual form of the scheme in [22] since the $5n \times 5n$ sparse basis matrix is used in a dual manner. Hence, while [22] scheme has size $O(1)$

ciphertexts and size $O(\ell n)$ keys, the underlying one has size $O(n)$ ciphertexts and size $O(\ell)$ keys (Table 1), where ℓ, n are the number of rows in access structure matrix M and the max of the number of attributes in Γ, respectively. In other words, the dual conversion of the scheme in [22] to the underlying scheme increases ciphertext size $O(n)$-times and then decreases key size $O(n)$-times.

As mentioned in Introduction, the top level idea of our construction is the decoupling technique of LSS encoding. The underlying scheme has a usual encoding of LSS, i.e., encoding a central secret s_0 and shares s_i. Therefore, the comprehension of the construction idea of the underlying one is necessary for understanding our proposed one. In this section, we will explain key ideas of constructing the underlying and our KP-ABE schemes. First, we will show how size $O(n)$ ciphertexts and size $O(\ell)$ keys can be achieved in the underlying scheme, where the IPE scheme given in [19] is used as a building block. Here, we will use a simplified (or toy) version of the underlying KP-ABE scheme, for which the security is no more ensured in the standard model under the DLIN assumption.

A ciphertext in the simplified KP-ABE scheme consists of two vector elements, $(\boldsymbol{c}_0, \boldsymbol{c}_1) \in \mathbb{G}^5 \times \mathbb{G}^n$, and $c_T \in \mathbb{G}_T$. A secret key consists of $\ell + 1$ vector elements, $(\boldsymbol{k}_0^*, \boldsymbol{k}_1^*, \ldots, \boldsymbol{k}_\ell^*) \in \mathbb{G}^5 \times (\mathbb{G}^n)^\ell$ for access structure $\mathbb{S} := (M, \rho)$, where the number of rows of M is ℓ and $\boldsymbol{k}_i^*$ with $i \geq 1$ corresponds to the i-th row. Therefore, to achieve shorter secret keys, we have to compress $\boldsymbol{k}_i^* \in \mathbb{G}^n$ to a constant size in n. We now employ a special form of basis generation matrix, $X := \begin{pmatrix} \mu_1' & & \\ \mu_2' & \mu & \\ \vdots & & \ddots \\ \mu_n' & & & \mu \end{pmatrix} \in \mathcal{H}(n, 0, \mathbb{F}_q)$ of Eq. (1) in Sect. 4, where $\mu, \mu_1', \ldots, \mu_n' \xleftarrow{\cup} \mathbb{F}_q$ and a blank in the matrix denotes $0 \in \mathbb{F}_q$. The master secret key (DPVS basis) is $\mathbb{B}^* := \begin{pmatrix} \boldsymbol{b}_1^* \\ \vdots \\ \boldsymbol{b}_n^* \end{pmatrix} := \begin{pmatrix} \mu_1' G & & & \\ \mu_2' G & \mu G & & \\ \vdots & & \ddots & \\ \mu_n' G & & & \mu G \end{pmatrix}$. Let the i-th component of a secret key associated with $\mathbb{S} := (M := (M_i)_{i=1}^{\ell},\ \rho)$ consists of $\boldsymbol{k}_i^* := (\theta_i v_i^{n-1} + s_i,\ \theta_i v_i^{n-2}, \ldots, \theta_i v_i, \theta_i)_{\mathbb{B}^*} = (\theta_i v_i^{n-1} + s_i)\boldsymbol{b}_1^* + \theta_i(v_i^{n-2}\boldsymbol{b}_2^* + \cdots + v_i \boldsymbol{b}_{n-1}^* + \boldsymbol{b}_n^*) = \left(\left(\theta_i(\sum_{j=1}^n v_i^{n-j}\mu_j') + s_i\mu_1'\right) G,\ v_i^{n-2}\theta_i\mu G, \ldots, \theta_i \mu G\right)$, where $v_i := \rho(i), \theta_i \xleftarrow{\cup} \mathbb{F}_q, \vec{f} \xleftarrow{\cup} \mathbb{F}_q^r$ and $s_i := M_i \cdot \vec{f}$. Then, $\boldsymbol{k}_i^*$ can be compressed to only *two* group elements $\left(K_{i,1}^* := \left(\theta_i(\sum_{j=1}^n v_i^{n-j}\mu_j') + s_i\mu_1'\right) G,\ K_{i,2}^* := \theta_i \mu G\right)$ as well as v_i, since $\boldsymbol{k}_i^*$ can be obtained by $(K_{i,1}^*, v_i^{n-2}K_{i,2}^*, \ldots, v_i K_{i,2}^*, K_{i,2}^*)$ (note that $v_i^j K_{i,2}^* = v_i^j \theta_i \mu G$ for $j = 0, \ldots, n-2$). That is, the i-th component of a secret key (excluding v_i) can be just two group elements, or the size is constant in n, then $(\boldsymbol{k}_i^*)_{i=0}^{\ell}$ can be compressed into size $O(\ell)$.

Let $\mathbb{B} := (\boldsymbol{b}_i)$ be the dual orthonormal basis of $\mathbb{B}^* := (\boldsymbol{b}_i^*)$, and $\mathbb{B}$ be the public key in the simplified KP-ABE scheme. We specify $(\boldsymbol{c}_0, \boldsymbol{k}_0^*, c_T)$ such that $e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) = g_T^{\zeta - \xi s_0}$ and $c_T := g_T^{\zeta} m \in \mathbb{G}_T$ with s_0 is a center secret of shares $\{s_i\}_{i=1,\ldots,\ell}$ associated with access structure $\mathbb{S}$, which are embedded into

$\{\boldsymbol{k}_i^*\}_{i=1,\ldots,\ell}$ as indicated above. We also set a ciphertext for $\Gamma := \{x_1, \ldots, x_{n'}\}$ as $\boldsymbol{c}_1 := (\omega\vec{y})_{\mathbb{B}}$ where $\vec{y} := (y_1, \ldots, y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \prod_{j=1}^{n'} (z - x_j)$, and $\omega \xleftarrow{\cup} \mathbb{F}_q$. From the dual orthonormality of $\mathbb{B}$ and $\mathbb{B}^*$, if $\mathbb{S}$ accepts Γ, there exists a system of coefficients $\{\alpha_i\}_{\rho(i)\in\Gamma}$ such that $e(\boldsymbol{c}_1, \boldsymbol{k}'^*) = g_T^{\xi s_0}$, where $\boldsymbol{k}'^* := \sum_{\rho(i)\in\Gamma} \alpha_i \boldsymbol{k}_i^*$. Hence, a decryptor can compute $g_T^{\xi s_0}$ if and only if $\mathbb{S}$ accepts Γ, i.e., can obtain plaintext m. We can extend the simplified KP-ABE to a *semi-adaptively* secure KP-ABE scheme under the DLIN assumption just by enlarging the dimension of the underlying vector space, which is shown in Sect. 5.3. The security proof is based on the Waters's dual system technique and given in a similar manner to [22]. The provably secure scheme has the same asymptotic sizes of keys and ciphertexts, i.e., $O(\ell)$-sized keys and $O(n)$-sized ciphertexts.

Our goal is to construct an *adaptively* secure KP-ABE with a comparable asymptotic data sizes, i.e., $O(\ell)$-sized keys and $O(n + r)$-sized ciphertexts, from the underlying one. We use a decoupling technique of LSS matrix from randomness for achieving the goal. First, we enlarge the space from $O(n)$ to $O(n + r)$ dimension. As described in Fig. 1, a uniformly random vector $\vec{f} \in \mathbb{F}_q^r$ for LSS is encoded on the ciphertext component $\boldsymbol{c}_1$. In the simplified scheme, $\boldsymbol{c}_1 := (\omega\vec{y}, \vec{f})_{\mathbb{B}} \in \mathbb{G}^{n+r}$ where $\vec{y} \in \mathbb{F}_q^r$ is defined as above. For encoding each row M_i of access matrix M on $\boldsymbol{k}_i^*$, the above matrix X is extended to a $(n+r)\times(n+r)$ matrix in $\mathcal{H}(n, r, \mathbb{F}_q)$ (Eq. (1)), then the master secret key is given by

$$\mathbb{B}^* := \begin{pmatrix} \boldsymbol{b}_1^* \\ \vdots \\ \\ \boldsymbol{b}_n^* \\ \boldsymbol{b}_{n+1}^* \\ \vdots \\ \boldsymbol{b}_{n+r}^* \end{pmatrix} := \begin{pmatrix} \mu_1' G & & & & & \\ \mu_2' G & \mu_1 G & & & & \\ \vdots & & \ddots & & & \\ \mu_n' G & & & \mu_1 G & & \\ \mu_{n+1}' G & & & & \mu_2 G & \\ \vdots & & & & & \ddots \\ \mu_{n+r}' G & & & & & \mu_2 G \end{pmatrix} \quad \text{where}$$

$\mu_1, \mu_2, \mu_1', \ldots, \mu_{n+r}' \xleftarrow{\cup} \mathbb{F}_q$. Here, note that two independent diagonal elements μ_1, μ_2 are used for the first n-dimension and the second r-dimension. (Refer to the argument given in the beginning of Sect. 4.) Hence, $\boldsymbol{k}_i^*$ is given by $\boldsymbol{k}_i^* := (\theta_i \vec{v}_i, \xi M_i)_{\mathbb{B}^*}$. We note $\boldsymbol{k}_i^*$ is compressed to three group elements as before, i.e., $K_{i,1}^* := \left(\theta_i(\sum_{l=1}^{n} v_i^{n-l}\mu_l') + \xi(\sum_{l=1}^{r} M_{i,l}\mu_{n+l}')\right) G$, $K_{i,2}^* := \theta_i \mu_1 G$, $K_{i,3}^* := \xi\mu_2 G$ for $i = 1, .., \ell$, and the secret key size is $O(\ell)$. The pairing value of $\boldsymbol{c}_1$ and $\boldsymbol{k}_i^*$ is $e(\boldsymbol{c}_1, \boldsymbol{k}_i^*) = g_T^{\omega\theta_i \vec{y}\cdot\vec{v}_i + \xi M_i \cdot \vec{f}} = g_T^{\omega\theta_i \vec{y}\cdot\vec{v}_i + \xi s_i}$ where $s_i := M_i \cdot \vec{f}$. These values are equivalent to the previous underlying scheme. Therefore, the decryption algorithm is the same as before.

We then explain how our *full* KP-ABE scheme is constructed on the above-mentioned simplified KP-ABE scheme. The target of designing the full KP-ABE scheme is to achieve the adaptive security *under the DLIN assumption*. Here, we adopt and extend a strategy initiated in [18], in which the dual system encryption methodology is employed in a modular or hierarchical manner. That is, three top level assumptions, the security of Problems 1–3, are directly used in the dual system encryption methodology and the assumptions are reduced to a primitive assumption, the DLIN assumption. To meet the requirements for applying to the

dual system encryption methodology and reducing to the DLIN assumption, the underlying vector space is five times greater than that of the above-mentioned simplified scheme. For example, $\boldsymbol{k}_i^* := (\ \theta_i \vec{v}_i,\ \xi M_i,\ 0^{2n+2r},\ \psi_i \vec{v}_i,\ \eta_i M_i,\ 0^{n+r}\ )_{\mathbb{B}^*}$ for $\rho(i) = v_i$, $\boldsymbol{c}_1 = (\ \omega\vec{y},\ \vec{f},\ 0^{2n+2r},\ 0^{n+r},\ \vec{\varphi}_1\ )_{\mathbb{B}}$ with $\vec{\varphi}_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n+r}$, and $X := \begin{pmatrix} X_{1,1} \cdots X_{1,5} \\ \vdots \quad\quad \vdots \\ X_{5,1} \cdots X_{5,5} \end{pmatrix} \in \mathcal{L}(5, n, r, \mathbb{F}_q)$ of Eq. (3) in Sect. 4, where each $X_{i,j}$ is of the form of $X \in \mathcal{H}(n, r, \mathbb{F}_q)$ in the simplified scheme. The vector space consists of four orthogonal subspaces, i.e., real encoding part, hidden part, secret key randomness part, and ciphertext randomness part. The simplified KP-ABE scheme corresponds to the first real encoding part.

A key fact in the security reduction is that $\mathcal{L}(5, n, r, \mathbb{F}_q)$ is a *subgroup* of $GL(5(n+r), \mathbb{F}_q)$ (Lemma 2), which enables a *random-self-reducibility* argument for reducing the intractability of Problems 1–3 to the DLIN assumption. For the reduction, see [19]. We employ a new simulation technique in dual system encryption using random vector $\vec{f}$ in $\boldsymbol{c}_1$. For the details, refer to the proof outline in Sect. 5.4.

5.2 Dual Orthonormal Basis Generator

We describe random dual orthonormal basis generator $\mathcal{G}_{\mathsf{ob}}^{\mathsf{KP}}$ below, which is used as a subroutine in the proposed KP-ABE scheme.

$$
\begin{aligned}
&\mathcal{G}_{\mathsf{ob}}^{\mathsf{KP}}(1^\lambda, 5, (n, r)) : \mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda), N_0 := 5, N_1 := 5(n+r), \\
&\quad \mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N_t, \mathsf{param}_{\mathbb{G}}) \ \text{ for } t = 0, 1, \\
&\quad \psi \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,\ g_T := e(G, G)^\psi,\ \mathsf{param}_{(n,r)} := ((n, r),\ \{\mathsf{param}_{\mathbb{V}_t}\}_{t=0,1},\ g_T), \\
&\quad X_0 := (\chi_{0,i,j})_{i,j=1,\ldots,5} \xleftarrow{\mathsf{U}} GL(N_0, \mathbb{F}_q),\ X_1 \xleftarrow{\mathsf{U}} \mathcal{L}(5, n, r, \mathbb{F}_q),\ \text{hereafter}, \\
&\quad \{\mu_{i,j,\iota}, \mu'_{i,j,l}\}_{l=1,\ldots,n+r}^{i,j=1,\ldots,5;\iota=1,2} \text{ denotes non-zero entries of } X_1 \text{ as in Eq. (2)}, \\
&\quad \boldsymbol{b}_{0,i}^* := (\chi_{0,i,1}, .., \chi_{0,i,5})_{\mathbb{A}} = \textstyle\sum_{j=1}^5 \chi_{0,i,j} \boldsymbol{a}_j \ \text{ for } i = 1, .., 5,\ \mathbb{B}_0^* := (\boldsymbol{b}_{0,1}^*, .., \boldsymbol{b}_{0,5}^*), \\
&\quad B_{i,j,\iota}^* := \mu_{i,j,\iota} G,\ B'^*_{i,j,l} := \mu'_{i,j,l} G \ \text{ for } i, j = 1, \ldots, 5; \iota = 1, 2; l = 1, \ldots, n+r, \\
&\quad \text{for } t = 0, 1,\ (\vartheta_{t,i,j})_{i,j=1,\ldots,N_t} := \psi \cdot (X_t^{\mathrm{T}})^{-1}, \\
&\quad \boldsymbol{b}_{t,i} := (\vartheta_{t,i,1}, .., \vartheta_{t,i,N_t})_{\mathbb{A}} = \textstyle\sum_{j=1}^{N_t} \vartheta_{t,i,j} \boldsymbol{a}_j \ \text{ for } i = 1, .., N_t,\ \mathbb{B}_t := (\boldsymbol{b}_{t,1}, .., \boldsymbol{b}_{t,N_t}), \\
&\quad \text{return } \ (\mathsf{param}_{(n,r)}, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1, \{B_{i,j,\iota}^*, B'^*_{i,j,l}\}_{l=1,\ldots,n+r}^{i,j=1,\ldots,5;\iota=1,2}).
\end{aligned}
$$

Remark 2. Let sparse block matrix $\begin{pmatrix} \boldsymbol{b}^*_{1,(i-1)(n+r)+1} \\ \vdots \\ \boldsymbol{b}^*_{1,i(n+r)} \end{pmatrix} := (X_{i,1} \cdot G \cdots X_{i,5} \cdot G)$ for $i = 1, \ldots, 5$, and $\mathbb{B}_1^* := (\boldsymbol{b}^*_{1,1}, \ldots, \boldsymbol{b}^*_{1,5(n+r)})$, where $X_{i,j} \cdot G$ means the componentwise multiplication. $\mathbb{B}_1$ is the dual orthonormal basis of $\mathbb{B}_1^*$, i.e., $e(\boldsymbol{b}_{1,i}, \boldsymbol{b}^*_{1,i}) = g_T$ and $e(\boldsymbol{b}_{1,i}, \boldsymbol{b}^*_{1,j}) = 1$ for $1 \le i \ne j \le 5(n+r)$.

5.3 Warm-Up: Underlying Semi-adaptively Secure Construction

As a warm-up, we describe a semi-adaptively secure KP-ABE scheme, which is a dual construction of [22] whose secret keys are compressed by using a sparse matrix while [22] scheme has compressed ciphertexts. Namely, we use the sparse matrix in a dual manner of [22]. We refer to Sect. 1.4 for notations on DPVS.

$\mathsf{Setup}(1^\lambda,\ n)$: / * $N_0 := 5,\ N_1 := 5n$ * /

$(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1, \{B^*_{i,j,\iota}, B'^*_{i,j,l}\}_{l=1,\ldots,n}^{i,j=1,\ldots,5;\ \iota=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}^{\mathsf{KP}}(1^\lambda, 5, (n,0))$,

$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,2}, \boldsymbol{b}_{0,5}),\ \widehat{\mathbb{B}}_0^* := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,2}, \boldsymbol{b}^*_{0,4})$,

$\widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, .., \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,4n+1}, .., \boldsymbol{b}_{1,5n})$,

return $\mathsf{pk} := (1^\lambda, \mathsf{param}_n, \{\widehat{\mathbb{B}}_t\}_{t=0,1}),\ \ \mathsf{sk} := (\widehat{\mathbb{B}}_0^*, \{B^*_{i,j,\iota}, B'^*_{i,j,l}\}_{\iota=1,2;\ l=1,\ldots,n}^{i=1,4;j=1,\ldots,5})$.

$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \mathbb{S} := (M, \rho))$: $\vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r,\ s_0 := \vec{1} \cdot \vec{f},\ \eta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

$\boldsymbol{k}_0^* := (1,\ s_0,\ 0,\ \eta_0,\ 0)_{\mathbb{B}_0^*}$,

for $i = 1, \ldots, \ell$, if $\rho(i) = v_i$, $\vec{v}_i := (v_{i,l})_{l=1}^n := (v_i^{n-1}, .., v_i, 1)$,

$s_i := M_i \cdot \vec{f},\ \theta_i, \psi_i, \eta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

for $j = 1, \ldots, 5$, $K^*_{i,1,j} := \sum_{l=1}^n v_{i,l}(\theta_i B'^*_{1,j,l} + \psi_i B'^*_{5,j,l}) + s_i B'^*_{1,j,1} + \eta_i B'^*_{5,j,1}$,

$K^*_{i,2,j} := \theta_i B^*_{1,j,1} + \psi_i B^*_{5,j,1}$,

return $\mathsf{sk}_{\mathbb{S}} := (\mathbb{S},\ \boldsymbol{k}_0^*,\ \{K^*_{i,1,j}, K^*_{i,2,j}\}_{i=1,\ldots,\ell;j=1,\ldots,5})$.

$\mathsf{Enc}(\mathsf{pk},\ m,\ \Gamma := \{x_1, \ldots, x_{n'} \,|\, x_j \in \mathbb{F}_q^\times, n' \le n-1\})$:

$\vec{y} := (y_1, \ldots, y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \prod_{j=1}^{n'} (z - x_j)$,

$\omega, \varphi_0, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \ \vec{\varphi}_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q^n,\ \ \boldsymbol{c}_0 := (\zeta,\ \omega,\ 0,\ 0,\ \varphi_0)_{\mathbb{B}_0}$,

$\boldsymbol{c}_1 := (\overbrace{\quad\omega\vec{y},\quad}^{n}\ \overbrace{\quad 0^{2n},\quad}^{2n}\ \overbrace{\quad 0^n,\quad}^{n}\ \overbrace{\quad\vec{\varphi}_1\quad}^{n})_{\mathbb{B}_1}$

$c_T := g_T^\zeta m,\ \ \mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \boldsymbol{c}_1, c_T),\ \ \text{return}\ \ \mathsf{ct}_\Gamma$.

$\mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_{\mathbb{S}} := (\mathbb{S},\ \boldsymbol{k}_0^*, \{K^*_{i,1,j}, K^*_{i,3,j}\}_{j=1,\ldots,5}^{i=1,\ldots,\ell}), \mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \boldsymbol{c}_1, c_T))$:

If $\mathbb{S} := (M, \rho)$ accepts Γ, then compute I and $\{\alpha_i\}_{i \in I}$ such that

$\vec{1} = \sum_{i \in I} \alpha_i M_i$, where M_i is the i-th row of M, and

$I \subseteq \{i \in \{1, \ldots, \ell\} \ \ | \ \ [\rho(i) = v_i \ \wedge\ v_i \in \Gamma]\ \}$.

for $i \in I$, if $\rho(i) = v_i$, $\vec{v}_i := (v_{i,l})_{l=1}^n := (v_i^{n-1}, \ldots, v_i, 1)$,

$\boldsymbol{k}_i^* := (\overbrace{\quad K^*_{i,1,1},\ v_{i,2}K^*_{i,2,1}, .., v_{i,n}K^*_{i,2,1},\quad}^{n}\ \cdots\ \overbrace{\quad K^*_{i,1,5},\ v_{i,2}K^*_{i,2,5}, .., v_{i,n}K^*_{i,2,5}\quad}^{n})$,

that is, $\boldsymbol{k}_i^* := (\overbrace{\quad\theta_i\vec{v}_i + s_i\vec{e}_1,\quad}^{n}\ \overbrace{\quad 0^{2n},\quad}^{2n}\ \overbrace{\quad\psi_i\vec{v}_i + \eta_i\vec{e}_1,\quad}^{n}\ \overbrace{\quad 0^n\quad}^{n})_{\mathbb{B}_1^*}$,

$\boldsymbol{k}'^* := \sum_{i \in I} \alpha_i \boldsymbol{k}_i^*,\ \ K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \cdot e(\boldsymbol{c}_1, \boldsymbol{k}'^*),\ \ \text{return}\ \ m' := c_T / K$.

[Correctness] If $\mathbb{S} := (M, \rho)$ accepts Γ, $K = e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \cdot e(\boldsymbol{c}_1, \boldsymbol{k}'^*) = g_T^{-\omega s_0 + \zeta} g_T^{\omega \sum_{i \in I} \alpha_i s_i} = g_T^{\zeta}$ where $s_0 := \vec{1} \cdot \vec{f}$, $s_i := M_i \cdot \vec{f}$ for $i = 1, \ldots, \ell$.

We note that secret key $\mathsf{sk}_{\mathbb{S}}$ consists of $5\ell + 5$ group elements and ciphertext ct_{Γ} consists of $5n + 5$ group elements (and one $\mathbb{G}_T$ element).

The standard DLIN assumption is defined in Appendix A.

Theorem 1. *The above multi-use KP-ABE scheme is semi-adaptively payload-hiding against chosen plaintext attacks under the DLIN assumption.*

Theorem 1 is proven in a similar manner as in [22].

In the semi-adaptive security model, the challenge attribute set Γ is declared by the adversary at the start of the game, but after receiving the public key pk from the challenger. Therefore, for each key query $\mathbb{S} := (M, \rho)$, the challenger can determine whether $\rho(i) \in \Gamma$ or not for $i = 1, \ldots, \ell$. The challenger in the security proof makes use of this information to simulate a component $\boldsymbol{k}_i^*$ of a queried key for each $i = 1, \ldots, \ell$ in a refined dual system encryption proof. The main part of the game sequence is similar (but not equal) to the Game 3 sequence in the proof of Theorem 2 below.

5.4 Proposed Adaptively Secure Construction

By decoupling LSS coefficients $s_i := M_i \cdot \vec{f} \in \mathbb{F}_q$ to $M_i \in \mathbb{F}_q^r$ in the key side and $\vec{f} \in \mathbb{F}_q^r$ in the ciphertext side (of the underlying scheme in Sect. 5.3), we obtain our proposed adaptively secure KP-ABE scheme.

$\mathsf{Setup}(1^\lambda,\ (n, r)) :$ / * $N_0 := 5,\ N_1 := 5(n + r)$ * /

$(\mathsf{param}_{(n,r)}, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1, \{B_{i,j,\iota}^*, B_{i,j,l}'^*\}_{l=1,\ldots,n+r}^{i,j=1,\ldots,5;\, \iota=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}^{\mathsf{KP}}(1^\lambda, 5, (n, r))$,

$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,2}, \boldsymbol{b}_{0,5})$, $\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,2}^*, \boldsymbol{b}_{0,4}^*)$,

$\widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, .., \boldsymbol{b}_{1,n+r}, \boldsymbol{b}_{1,4(n+r)+1}, .., \boldsymbol{b}_{1,5(n+r)})$,

return $\mathsf{pk} := (1^\lambda, \mathsf{param}_{(n,r)}, \{\widehat{\mathbb{B}}_t\}_{t=0,1})$,

$\mathsf{sk} := (\widehat{\mathbb{B}}_0^*, \{B_{i,j,\iota}^*, B_{i,j,l}'^*\}_{\iota=1,2;\, l=1,..,n+r}^{i=1,4;j=1,..,5})$.

$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \mathbb{S} := (M, \rho)) :\quad \xi, \eta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q, \qquad \boldsymbol{k}_0^* := (1,\ \xi,\ 0,\ \eta_0,\ 0)_{\mathbb{B}_0^*}$,

for $i = 1, .., \ell$, if $\rho(i) = v_i$, $\vec{v}_i := (v_{i,l})_{l=1}^n := (v_i^{n-1}, .., v_i, 1)$, $\theta_i, \psi_i, \eta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

for $j = 1, \ldots, 5$,

$K_{i,1,j}^* := \sum_{l=1}^n v_{i,l}(\theta_i B_{1,j,l}'^* + \psi_i B_{5,j,l}'^*) + \sum_{l=1}^r M_{i,l}(\xi B_{1,j,n+l}'^* + \eta_i B_{5,j,n+l}'^*)$,

$K_{i,2,j}^* := \theta_i B_{1,j,1}^* + \psi_i B_{5,j,1}^*, \quad K_{i,3,j}^* := \xi B_{1,j,2}^* + \eta_i B_{5,j,2}^*$,

return $\mathsf{sk}_{\mathbb{S}} := (\mathbb{S},\ \boldsymbol{k}_0^*,\ \{K_{i,1,j}^*, K_{i,2,j}^*, K_{i,3,j}^*\}_{i=1,\ldots,\ell;j=1,\ldots,5})$.

$\mathsf{Enc}(\mathsf{pk},\ m,\ \Gamma := \{x_1,\ldots,x_{n'} \,|\, x_j \in \mathbb{F}_q^\times, n' \le n-1\}):$

$\vec{y} := (y_1,\ldots,y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \prod_{j=1}^{n'}(z - x_j)$,

$\vec{f} \xleftarrow{\cup} \mathbb{F}_q^r,\ \omega, \varphi_0, \zeta \xleftarrow{\cup} \mathbb{F}_q,\ \ \vec{\varphi}_1 \xleftarrow{\cup} \mathbb{F}_q^{n+r},\quad \boldsymbol{c}_0 := (\zeta,\ \vec{1}\cdot\vec{f},\ 0,\ 0,\ \varphi_0)_{\mathbb{B}_0},$

$$\boldsymbol{c}_1 := (\overbrace{\quad\omega\vec{y},\ \vec{f},\quad}^{n+r}\ \overbrace{\quad 0^{2n+2r},\quad}^{2n+2r}\ \overbrace{\quad 0^{n+r},\quad}^{n+r}\ \overbrace{\quad\vec{\varphi}_1\quad}^{n+r})_{\mathbb{B}_1}$$

$c_T := g_T^\zeta m,\ \ \mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \boldsymbol{c}_1, c_T),\quad$ return ct_Γ.

$\mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_\mathbb{S} := (\mathbb{S},\ \boldsymbol{k}_0^*, \{K_{i,1,j}^*, K_{i,2,j}^*, K_{i,3,j}^*\}_{j=1,\ldots,5}^{i=1,\ldots,\ell}), \mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \boldsymbol{c}_1, c_T)):$

If $\mathbb{S} := (M, \rho)$ accepts Γ, then compute I and $\{\alpha_i\}_{i\in I}$ such that

$\vec{1} = \sum_{i\in I} \alpha_i M_i$, where M_i is the i-th row of M, and

$I \subseteq \{i \in \{1,..,\ell\} \mid [\rho(i) = v_i \wedge\ v_i \in \Gamma]\ \}$.

for $i \in I$, if $\rho(i) = v_i$, $\vec{v}_i := (v_{i,l})_{l=1}^n := (v_i^{n-1},\ldots,v_i,1)$,

$$\boldsymbol{k}_i^* := (\overbrace{\begin{matrix} K_{i,1,1}^*,\ v_{i,2}K_{i,2,1}^*,..,v_{i,n}K_{i,2,1}^*,\ M_{i,1}K_{i,3,1}^*,..,M_{i,r}K_{i,3,1}^*,\ \cdots \\ K_{i,1,5}^*,\ v_{i,2}K_{i,2,5}^*,..,v_{i,n}K_{i,2,5}^*,\ M_{i,1}K_{i,3,5}^*,..,M_{i,r}K_{i,3,5}^* \end{matrix}}^{n+r}),$$

that is, $\boldsymbol{k}_i^* := (\overbrace{\quad\theta_i\vec{v}_i,\ \xi M_i,\quad}^{n+r}\ \overbrace{\quad 0^{2n+2r},\quad}^{2n+2r}\ \overbrace{\quad\psi_i\vec{v}_i,\ \eta_i M_i,\quad}^{n+r}\ \overbrace{\quad 0^{n+r}\quad}^{n+r})_{\mathbb{B}_1^*},$

$\boldsymbol{k}'^* := \sum_{i\in I} \alpha_i \boldsymbol{k}_i^*,\ \ K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \cdot e(\boldsymbol{c}_1, \boldsymbol{k}'^*),\quad$ return $m' := c_T/K$.

[Correctness] If $\mathbb{S} := (M,\rho)$ accepts Γ, $K = e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \cdot e(\boldsymbol{c}_1, \boldsymbol{k}'^*) = g_T^{-\xi s_0 + \zeta} g_T^{\xi \sum_{i\in I} \alpha_i s_i} = g_T^\zeta$ where $s_0 := \vec{1}\cdot\vec{f},\ s_i := M_i \cdot \vec{f}$ for $i = 1,\ldots,\ell$.

We note that secret key $\mathsf{sk}_\mathbb{S}$ consists of $5\ell + 5$ group elements and ciphertext ct_Γ consists of $5(n+r)+5$ group elements (and one $\mathbb{G}_T$ element).

While our adaptively secure KP- and CP-ABE schemes have the maximum of size r as one of public parameters, they allow several useful class of access structures. According to the explicit construction of span programs from boolean formulas (e.g., Appendix of [15]), while appending AND gate gets r (and ℓ) larger, appending OR gate gets only ℓ larger. Therefore, for example, available access structures for our adaptive ABE include any r-CNF formula with any arbitrarily long disjunctions (for a bounded r), i.e., length r conjunctions of length $t_1,\ldots,t_r$ disjunctions for arbitrarily large $t_1,\ldots,t_r$ like $(\mathcal{X}_1 \vee \overset{\text{arb. long}}{\cdots\cdots} \vee \mathcal{X}_{t_1}) \wedge \cdots \wedge (\mathcal{Z}_1 \vee \overset{\text{arb. long}}{\cdots\cdots} \vee \mathcal{Z}_{t_r})$, where multi-use of attributes for $\mathcal{X}_1,\ldots,\mathcal{X}_{t_1},\ldots,\mathcal{Z}_1,\ldots,\mathcal{Z}_{t_r}$ is allowed. The j-th column of the LSS matrix M is given by $(\overbrace{0,\ldots,0}^{\sum_{\iota=1}^{j-1} t_\iota}, \overbrace{1,\ldots,1}^{t_j}, 0,\ldots,0)^{\mathrm{T}}$ with length $\ell = \sum_{\iota=1}^r t_\iota$ for $j = 1,\ldots,r$ when the target is all 1 vector $\vec{1} \in \mathbb{F}_q^r$.

The standard DLIN assumption is defined in Appendix A.

Theorem 2. *The proposed multi-use KP-ABE scheme is adaptively payload-hiding against chosen plaintext attacks under the DLIN assumption.*

The proof of Theorem 2 is given in the full version of this paper [23].

Acknowledgement. This work was supported by JST CREST Grant Number JPMJCR14D6.

A Decisional Linear (DLIN) Assumption

Definition 6 (DLIN: Decisional Linear Assumption [7]). *The DLIN problem is to guess* $\beta \in \{0,1\}$*, given* $(\mathsf{param}_{\mathbb{G}}, G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, S_\beta) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda)$*, where* $\mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda)$: $\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda), \kappa, \delta, \xi, \sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q, S_0 := (\delta + \sigma)G, S_1 \xleftarrow{\mathsf{U}} \mathbb{G}, \mathrm{return}\ (\mathsf{param}_{\mathbb{G}}, G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, S_\beta)$*, for* $\beta \xleftarrow{\mathsf{U}} \{0,1\}$*. For a probabilistic machine* $\mathcal{E}$*, we define the advantage of* $\mathcal{E}$ *for the DLIN problem as:* $\mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) := \left|\Pr\left[\mathcal{E}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{DLIN}}(1^\lambda)\right] - \Pr\left[\mathcal{E}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{DLIN}}(1^\lambda)\right]\right|$*. The DLIN assumption is: For any probabilistic polynomial-time adversary* $\mathcal{E}$*, the advantage* $\mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda)$ *is negligible in* λ*.*

B Adaptively Secure Multi-Use CP-ABE Scheme with Short Secret Keys

B.1 Definition of CP-ABE

Definition 7 (Ciphertext-Policy Attribute-Based Encryption: CP-ABE). *A ciphertext-policy attribute-based encryption scheme consists of four algorithms.*

- Setup *takes as input security parameter. It outputs the public parameters* pk *and a master key* sk.
- KeyGen *takes as input a set of attributes,* $\Gamma := \{x_j\}_{1 \le j \le n'}$*,* pk *and* sk*. It outputs a decryption key.*
- Enc *takes as input public parameters* pk*, message* m *in some associated message space* msg*, and access structure* $\mathbb{S} := (M, \rho)$*. It outputs the ciphertext.*
- Dec *takes as input public parameters* pk*, decryption key* sk_Γ *for a set of attributes* Γ*, and ciphertext* $\mathsf{ct}_\mathbb{S}$ *that was encrypted under access structure* $\mathbb{S}$*. It outputs either* $m' \in \mathsf{msg}$ *or the distinguished symbol* $\perp$*.*

A CP-ABE scheme should have the correctness property: for all $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda)$, all attribute sets Γ, all decryption keys $\mathsf{sk}_\Gamma \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \Gamma)$, all messages m, all access structures $\mathbb{S}$, all ciphertexts $\mathsf{ct}_\mathbb{S} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, m, \mathbb{S})$, it holds that $m = \mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_\Gamma, \mathsf{ct}_\mathbb{S})$ with overwhelming probability, if $\mathbb{S}$ accepts Γ.

Definition 8. *The model for proving the adaptively payload-hiding security of CP-ABE under chosen plaintext attack is:*

Setup. *The challenger runs the setup algorithm,* $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda)$*, and gives the public parameters* pk *to the adversary.*

Phase 1. *The adversary is allowed to issue a polynomial number of queries,* Γ*, to the challenger or oracle* $\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \cdot)$ *for private keys,* sk_Γ *associated with* Γ*.*

Challenge. *The adversary submits two messages* $m^{(0)}, m^{(1)}$ *and an access structure,* $\mathbb{S} := (M, \rho)$*, provided that the* $\mathbb{S}$ *does not accept any* Γ *sent to the challenger in Phase 1. The challenger flips a random coin* $b \xleftarrow{\mathsf{U}} \{0,1\}$*, and computes* $\mathsf{ct}_{\mathbb{S}}^{(b)} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, m^{(b)}, \mathbb{S})$*. It gives* $\mathsf{ct}_{\mathbb{S}}^{(b)}$ *to the adversary.*

Phase 2. *The adversary is allowed to issue a polynomial number of queries,* Γ*, to the challenger or oracle* $\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \cdot)$ *for private keys,* sk_Γ *associated with* Γ*, provided that* $\mathbb{S}$ *does not accept* Γ*.*

Guess. *The adversary outputs a guess* b' *of* b*.*

The advantage of an adversary $\mathcal{A}$ *in the above game is defined as* $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{CP\text{-}ABE,PH}}(\lambda) := \Pr[b' = b] - 1/2$ *for any security parameter* λ*. A CP-FE scheme is adaptively payload-hiding secure if all polynomial time adversaries have at most a negligible advantage in the above game.*

B.2 Dual Orthonormal Basis Generator

We describe random dual orthonormal basis generator $\mathcal{G}_{\mathsf{ob}}^{\mathsf{CP}}$ below, which is used as a subroutine in the proposed CP-ABE scheme, where $\mathcal{G}_{\mathsf{ob}}^{\mathsf{KP}}$ is defined in Sec. 5.2.

$\mathcal{G}_{\mathsf{ob}}^{\mathsf{CP}}(1^\lambda, 5, (n,r)) :$

$(\mathsf{param}_{(n,r)}, \mathbb{D}_0, \mathbb{D}_0^*, \mathbb{D}_1, \{D_{i,j,\iota}^*, D_{i,j,l}'^*\}_{l=1,\ldots,n+r}^{i,j=1,\ldots,5;\iota=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}^{\mathsf{KP}}(1^\lambda, 5, (n,r)),$

$\mathbb{B}_0 := \mathbb{D}_0^*,\ \mathbb{B}_0^* := \mathbb{D}_0,\ \mathbb{B}_1^* := \mathbb{D}_1,\ B_{i,j,\iota} := D_{i,j,\iota}^*,\ B_{i,j,l}' := D_{i,j,l}'^*$ for all $i, j, l, \iota,$

return $(\mathsf{param}_{(n,r)}, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1^*, \{B_{i,j,\iota}, B_{i,j,l}'\}_{l=1,\ldots,n+r}^{i,j=1,\ldots,5;\iota=1,2}).$

B.3 Construction

$\mathsf{Setup}(1^\lambda,\ (n,r)) : / *\ N_0 := 5,\ N_1 := 5(n+r)\ * /$

$(\mathsf{param}_{(n,r)}, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1^*, \{B_{i,j,\iota}, B_{i,j,l}'\}_{l=1,\ldots,n+r}^{i,j=1,\ldots,5;\iota=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}^{\mathsf{CP}}(1^\lambda, 5, (n,r)),$

$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,2}, \boldsymbol{b}_{0,4}),\ \widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,2}^*, \boldsymbol{b}_{0,5}^*),$

$\widehat{\mathbb{B}}_1^* := (\boldsymbol{b}_{1,1}^*, .., \boldsymbol{b}_{1,n+r}^*, \boldsymbol{b}_{1,3(n+r)+1}^*, .., \boldsymbol{b}_{1,4(n+r)}^*),$

return $\mathsf{pk} := (1^\lambda, \mathsf{param}_{(n,r)}, \widehat{\mathbb{B}}_0, \{B_{i,j,\iota}, B_{i,j,l}'\}_{\iota=1,2;\, l=1,\ldots,n+r}^{i=1,4;j=1,\ldots,5}),$

$\mathsf{sk} := \{\widehat{\mathbb{B}}_t^*\}_{t=0,1}.$

$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \Gamma := \{x_1, \ldots, x_{n'} \,|\, x_j \in \mathbb{F}_q^\times, n' \le n-1\}) :$

$\vec{y} := (y_1, \ldots, y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \prod_{j=1}^{n'} (z - x_j)$,

$\vec{f} \xleftarrow{\cup} \mathbb{F}_q^r,\ \omega, \varphi_0 \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\varphi}_1 \xleftarrow{\cup} \mathbb{F}_q^{n+r},\ \boldsymbol{k}_0^* := (1,\ \vec{1} \cdot \vec{f},\ 0,\ \varphi_0)_{\mathbb{B}_0^*}$,

$$\boldsymbol{k}_1^* := (\overbrace{\quad \omega\vec{y},\ \vec{f},}^{n+r}\ \overbrace{\quad 0^{2n+2r},}^{2n+2r}\ \overbrace{\quad 0^{n+r},}^{n+r}\ \overbrace{\quad \vec{\varphi}_1 \quad}^{n+r})_{\mathbb{B}_1^*}$$

$\mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}_0^*,\ \boldsymbol{k}_1^*)$. return sk_Γ.

$\mathsf{Enc}(\mathsf{pk},\ m,\ \mathbb{S} := (M, \rho))$: $\zeta, \xi, \eta_0 \xleftarrow{\cup} \mathbb{F}_q$, $\boldsymbol{c}_0 := (\zeta,\ \xi,\ 0,\ \eta_0,\ 0)_{\mathbb{B}_0}$,

for $i = 1, ..., \ell$, if $\rho(i) = v_i$, $\vec{v}_i := (v_{i,l})_{l=1}^n := (v_i^{n-1}, .., v_i, 1), \theta_i, \psi_i, \eta_i \xleftarrow{\cup} \mathbb{F}_q$,

for $j = 1, \ldots, 5$,

$C_{i,1,j} := \sum_{l=1}^n v_{i,l}(\theta_i B'_{1,j,l} + \psi_i B'_{4,j,l}) + \sum_{l=1}^r M_{i,l}(\xi B'_{1,j,n+l} + \eta_i B'_{4,j,n+l})$,

$C_{i,2,j} := \theta_i B_{1,j,1} + \psi_i B_{4,j,1}$, $C_{i,3,j} := \xi B_{1,j,2} + \eta_i B_{4,j,2}$,

$c_T := g_T^\zeta m$, return $\mathsf{ct}_\mathbb{S} := (\mathbb{S}, \boldsymbol{c}_0, \{C_{i,1,j}, C_{i,2,j}, C_{i,3,j}\}_{j=1,\ldots,5}^{i=1,\ldots,\ell}, c_T)$.

$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}_0^*,\ \boldsymbol{k}_1^*),\ \mathsf{ct}_\mathbb{S} := (\mathbb{S}, \boldsymbol{c}_0, \{C_{i,1,j}, C_{i,2,j}, C_{i,3,j}\}_{j=1,\ldots,5}^{i=1,\ldots,\ell}, c_T))$:

If $\mathbb{S} := (M, \rho)$ accepts Γ, then compute I and $\{\alpha_i\}_{i \in I}$ such that

$\vec{1} = \sum_{i \in I} \alpha_i M_i$, where M_i is the i-th row of M, and

$I \subseteq \{i \in \{1, \ldots, \ell\} \mid \rho(i) \in \Gamma\}$.

for $i \in I$, if $\rho(i) = v_i$, $\vec{v}_i := (v_{i,l})_{l=1}^n := (v_i^{n-1}, \ldots, v_i, 1)$,

$$\boldsymbol{c}_i := (\overbrace{\begin{array}{l} C_{i,1,1},\ v_{i,2}C_{i,2,1}, .., v_{i,n}C_{i,2,1},\ M_{i,1}C_{i,3,1}, .., M_{i,r}C_{i,3,1}, \\ C_{i,1,5},\ v_{i,2}C_{i,2,5}, .., v_{i,n}C_{i,2,5},\ M_{i,1}C_{i,3,5}, .., M_{i,r}C_{i,3,5} \end{array}}^{n+r} \cdots),$$

that is, $\boldsymbol{c}_i := (\overbrace{\quad \theta_i\vec{v}_i,}^{n+r}\ \overbrace{\quad \xi M_i,}^{2n+2r}\ \overbrace{\quad 0^{2n+2r},}^{n+r}\ \overbrace{\quad \psi_i\vec{v}_i,\ \eta_i M_i,}^{n+r}\ \overbrace{\quad 0^{n+r} \quad}^{n+r})_{\mathbb{B}_1}$,

$\boldsymbol{c}' := \sum_{i \in I} \alpha_i \boldsymbol{c}_i$, $K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \cdot e(\boldsymbol{c}', \boldsymbol{k}_1^*)$, return $m' := c_T / K$.

[Correctness] If Γ satisfies $\mathbb{S}$, $K = e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \cdot e(\boldsymbol{c}', \boldsymbol{k}_1^*) = g_T^{-\xi s_0 + \zeta} g_T^{\xi \sum_{i \in I} \alpha_i s_i} = g_T^\zeta$ where $s_0 := \vec{1} \cdot \vec{f}$, $s_i := M_i \cdot \vec{f}$ for $i = 1, \ldots, \ell$.

Theorem 3. *The proposed multi-use CP-ABE scheme is adaptively payload-hiding against chosen plaintext attacks under the DLIN assumption.*

Theorem 3 is similarly proven to Theorem 2.

References

1. Agrawal, S., Chase, M.: A study of pair encodings: predicate encryption in prime order groups. In: Kushilevitz, E., Malkin, T. (eds.) TCC 2016. LNCS, vol. 9563, pp. 259–288. Springer, Heidelberg (2016). doi:10.1007/978-3-662-49099-0_10
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). doi:10.1007/978-3-642-55220-5_31

3. Attrapadung, N.: Dual system encryption framework in prime-order groups via computational pair encodings. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10032, pp. 591–623. Springer, Heidelberg (2016). doi:10.1007/978-3-662-53890-6_20
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., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9452, pp. 575–601. Springer, Heidelberg (2015). doi:10.1007/978-3-662-48797-6_24
5. Attrapadung, N., Libert, B., 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). doi:10.1007/978-3-642-19379-8_6
6. Beimel, A.: Secure schemes for secret sharing and key distribution. Ph.D. thesis, Israel Institute of Technology, Technion, Haifa (1996)
7. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004). doi:10.1007/978-3-540-28628-8_3
8. Boneh, D., Gentry, C., Gorbunov, S., Halevi, S., Nikolaenko, V., Segev, G., Vaikuntanathan, V., Vinayagamurthy, D.: Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 533–556. Springer, Heidelberg (2014). doi:10.1007/978-3-642-55220-5_30
9. 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). doi:10.1007/978-3-662-46803-6_20
10. Cheon, J.H.: Security analysis of the strong diffie-hellman problem. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 1–11. Springer, Heidelberg (2006). doi:10.1007/11761679_1
11. Gorbunov, S., Vaikuntanathan, V., Wee, H.: Attribute-based encryption for circuits. In: STOC 2013, pp. 545–554 (2013)
12. 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)
13. Ishai, Y., Wee, H.: Partial garbling schemes and their applications. In: Esparza, J., Fraigniaud, P., Husfeldt, T., Koutsoupias, E. (eds.) ICALP 2014. LNCS, vol. 8572, pp. 650–662. Springer, Heidelberg (2014). doi:10.1007/978-3-662-43948-7_54
14. 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). doi:10.1007/978-3-642-13190-5_4
15. Lewko, A., Waters, B.: Decentralizing attribute-based encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 568–588. Springer, Heidelberg (2011). doi:10.1007/978-3-642-20465-4_31
16. 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). doi:10.1007/978-3-642-32009-5_12
17. Okamoto, T., Takashima, K.: Hierarchical predicate encryption for inner-products. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 214–231. Springer, Heidelberg (2009). doi:10.1007/978-3-642-10366-7_13

18. 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). doi:10.1007/978-3-642-14623-7_11
19. Okamoto, T., Takashima, K.: Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. Des. Codes Crypt. **77**(2–3), 725–771 (2015). the preliminary version appeared in CANS 2011
20. Okamoto, T., Takashima, K.: Dual pairing vector spaces and their applications. In: IEICE Transactions 98-A(1), pp. 3–15 (2015)
21. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005). doi:10.1007/11426639_27
22. Takashima, K.: Expressive attribute-based encryption with constant-size ciphertexts from the decisional linear assumption. In: Abdalla, M., Prisco, R. (eds.) SCN 2014. LNCS, vol. 8642, pp. 298–317. Springer, Cham (2014). doi:10.1007/978-3-319-10879-7_17
23. Takashima, K.: New proof techniques for DLIN-based adaptively secure attribute-based encryption. IACR Cryptology ePrint Archive 2015, 1021 (2015)
24. Waters, B.: Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Heidelberg (2009). doi:10.1007/978-3-642-03356-8_36
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). doi:10.1007/978-3-642-19379-8_4