

Expressive Attribute-Based Encryption with Constant-Size Ciphertexts from the Decisional Linear Assumption

Katsuyuki Takashima (Mitsubishi Electric),
March 21, 2014

Abstract. We propose a key-policy attribute-based encryption (KP-ABE) scheme with *constant-size ciphertexts*, whose (selective) security is proven under the *decisional linear (DLIN) assumption* in the standard model. The access structure is expressive, that is given by *non-monotone span programs*. It also has fast decryption, i.e., a decryption includes only a constant number of pairing operations. As an application of our KP-ABE construction, we also propose a *fully secure* attribute-based signatures with constant-size secret (signing) key from the DLIN assumption. For achieving the above results, we employ a hierarchical reduction technique on dual pairing vector spaces (DPVS), where a high-level problem given on DPVS is used for proving the scheme security and then the security of the problem is reduced to that of the DLIN problem.

1 Introduction

1.1 Backgrounds

The notion of *attribute-based encryption* (ABE) introduced by Sahai and Waters [26] is an advanced class of encryption and provides more flexible and fine-grained functionalities 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, it is called key-policy ABE (KP-ABE), and if the access policy is for encryption, it is 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) span programs (or (non-monotone) span programs with inner-product relations [23]). While general (polynomial size) circuits are supported [11, 13] recently, they are much less efficient than the pairing-based ABE schemes and non-practical when the relations are limited to span programs. Since our aim is to achieve *constant-size ciphertexts* in the sizes of attribute set or access policy in expressive ABE, hereafter, we focus on pairing-based ABE with span program access structures. Here, “constant” is valid as long as the description of the attribute or policy is not considered a part of the ciphertext, which is a common assumption in the ABE application. Hence, we use “constant” in this sense hereafter.

While the expressive access control (span programs) is very attractive, it also requires additional cost in terms of ciphertext size and decryption time. Emura et al. [10], and Herranz et al. [14] constructed a CP-ABE with constant-size ciphertexts, but their access structures are very limited. Attrapadung, Libert and de Panafieu [1] first constructed a KP-ABE scheme for span programs with constant-size ciphertexts and fast decryption which needs only a constant-number of pairing

| | | ALdP11 [1] | HW13 [15] | Proposed |
|-------------------|-------------|-------------------------------------|---------------------------------------------|--------------------------------------|
| Security model | | selective & standard model | selective & random oracle | selective & standard model |
| Assumption | | n -DBDHE | q -DBDHE | DLIN |
| Access structures | | Non-monotone span program | Monotone span program | Non-monotone span program |
| Public-key size | | $O(n) \mathbb{G} $ | $O(1) \mathbb{G} $ | $O(n) \mathbb{G} $ |
| Secret-key size | | $O(\ell n) \mathbb{G} $ | $O(\ell^2) \mathbb{G} $ | $O(\ell n) \mathbb{G} $ |
| Ciphertext size | | $3 \mathbb{G} + 1 \mathbb{G}_T $ | $(I + 1) \mathbb{G} + 1 \mathbb{G}_T $ | $17 \mathbb{G} + 1 \mathbb{G}_T $ |
| Decryption cost | Pairing | 3 | 2 | 17 |
| | Scalar mul. | $O(\ell n)$ | $O(\ell^2)$ | $O(\ell n)$ |

Table 1. Comparison of our scheme with *large-universe* KP-ABE schemes in [1, 15], where $|\mathbb{G}|$, $|\mathbb{G}_T|$, $|I|$, n , ℓ , and q represent size of an element of a bilinear source group \mathbb{G} , that of a target group \mathbb{G}_T , the number of attributes per ciphertext, (the maximum of $|I|$ in the system) + 1, the number of rows in access structure matrix for the secret key (in decryption), and the maximum number of random oracle calls, respectively.

operations. Hohenberger and Waters [15] proposed an expressive KP-ABE scheme with fast decryption, but with no short ciphertexts, and their large universe scheme is secure only in the random oracle model.

While Attrapadung et al.’s KP-ABE scheme shows an interesting approach to achieving constant-size ciphertexts with expressive access structures, the security is proven only based on a q -type assumption (n -DBDHE assumption with n the maximum number of attributes per ciphertext). Previously, since the introduction by Mitsunari et al. [19] and Boneh et al. [4], various kinds of q -type assumptions have been widely used in order to achieve (drastically) efficient cryptographic primitives [3, 5, 12, 9, 14]. However, the assumptions (and also the associated schemes) suffered a special attack which was presented by Cheon [7] at Eurocrypt 2006. More recently, Sakemi et al. [27] have shown that the attack can be a real threat to q -type assumption-based cryptographic primitives by executing a successful experiment. Consequently, it is very desirable that the above schemes should be replaced by an efficiency-comparable alternative scheme based on a *static* (non- q type) assumption instead of a q -type assumption.

In particular, to construct an expressive KP-ABE scheme with constant-size ciphertexts *based on a static assumption* remains an interesting open problem in terms of practical and theoretical aspects on ABE. Moreover, since there exists no attribute-based signatures (ABS) [17, 18, 25] with constant-size secret keys, to construct ABS with constant-size secret keys is open.

1.2 Our Results

- We propose a KP-ABE scheme with constant-size ciphertexts, whose (selective) security is proven from the DLIN assumption in the standard model (Section 4). The access structure is expressive, that is given by non-monotone span programs. It also has fast decryption: a decryption includes only a constant number of pairing operations, i.e., 17 pairings independently on the sizes of attribute set in ciphertext and access structure in key. For the comparison of our scheme with previous works on such large universe KP-ABE schemes, see Table 1.

- As an application of our KP-ABE construction, we also propose a *fully secure* ABS scheme with constant-size secret (signing) key from the DLIN assumption (Section 5 and Appendix E).
- For achieving the above results, we employ a hierarchical reduction technique on dual pairing vector spaces (DPVS) [22, 23], where a high-level problem given on DPVS (Problem 1) is used for proving the scheme’s security and then the security of the problem is reduced to that of the DLIN problem in a hierarchical manner. For the details, see Sections 1.3 and 6.

1.3 Key Techniques

At the top level, we employ a sparse matrix key-generation on DPVS developed in [24], in which constant-size ciphertext zero/non-zero inner-product encryption are constructed from DLIN. Based on the basic construction [24], to achieve short ciphertexts in our KP-ABE, attributes $\Gamma := \{x_j\}_{j=1,\dots,n'}$ are encoded in an n -dimensional (with $n \geq n' + 1$) vector $\vec{y} := (y_1, \dots, y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \prod_{j=1}^{n'} (z - x_j)$ where $y_1 = 1$. Each attribute value v_i (for $i = 1, \dots, \ell$) associated with a row of access structure matrix M (in \mathbb{S}) is encoded as $\vec{v}_i := (v_i^{n-1}, \dots, v_i, 1)$, so $\vec{y} \cdot \vec{v}_i = \prod_{j=1}^{n-1} (v_i - x_j)$, i.e., the value of inner product is equal to zero iff $v_i = x_j$ for some j . Here, the relation between \mathbb{S} and Γ is based on the multiple inner product values $\vec{y} \cdot \vec{v}_i$ for one vector \vec{y} which is equivalent to Γ . Based on it, a ciphertext vector element \mathbf{c}_1 is encoded with $\omega \vec{y}$ (for random ω), which is represented by *twelve* (constant in n) group elements (as well as \vec{y}), and key vector elements \mathbf{k}_i^* are encoded with \vec{v}_i and shares s_i ($i = 1, \dots, \ell$) for a central secret s_0 , respectively (see Section 4.2 for the key idea). A standard dual system encryption (DSE) approach consists of isolations of a pair of vectors, $(\vec{y}, s_i \vec{e}_1 + \theta_i \vec{v}_i)$ or $(\vec{y}, s_i \vec{v}_i)$ with s_i are shares of a secret s_0 and random θ_i , and then randomness is amplified with *preserving* the inner product values based on a *pairwise* independence argument. Since we must deal with a *same* \vec{y} in all the above pairs, we should modify the original randomness amplification argument for our scheme. See Section 7 for the details.

For the purpose, we prove the security in a *hierarchical* manner. First, we establish an intermediate problem (Problem 1 in Section 4.5) to prove the scheme’s security, and then, the security of the problem is proven from the DLIN assumption. Problem 1 is made for proving the selective security of our KP-ABE, which takes a target vector \vec{y} as input. Applying the problem to the queried keys (and the challenge ciphertext) in the security game transforms them to semi-functional form in DSE framework as given in Eq. (7) (in particular, w_0 is uniformly distributed in \mathbb{F}_q) since the target attributes do not satisfy access structures for queried keys. Namely, the problem realizes a partitioning type proof based on the DSE approach. (See [20] for a simpler example of this type argument.)

Our main technical contribution is to prove that the security of the (intermediate) problem is reduced from that of DLIN through multiple reduction steps (Lemma 3). The security proof consists of hierarchical reductions as indicated in Figure 1 (Appendix B). A technical challenge for the security of Problem 1 is to insert a polynomial number of random (sparse) matrices $\{Z_j\}_{j=1,\dots,n}$ of size $n \times n$ which fix \vec{y} i.e., $\vec{y} = \vec{y} \cdot (Z_j)^T$ to key components $\{\mathbf{h}_{1,j,i}^*\}$ *in sequence* when the underlying matrix for the basis \mathbb{B}_1 is sparse. The randomness $\{Z_j\}_{j=1,\dots,n}$ are inserted consistently with the security condition on the target \vec{y} and key queries. It is accomplished also in a *dual system* manner using *two (dual) blocks* in the hidden subspace, in which, for $j = 1, \dots, n$ in turn, vectors $\rho \vec{e}_i$ in the first block of $\mathbf{h}_{\cdot,j,i}^*$ ($i = 1, \dots, n$) are *swapped* to the second block and then *conceptually changed* to $\rho \vec{e}_i Z_j$ based on a modified pairwise independence (or randomizing) lemma (Lemma 4). An outline of the iterated process is given in Section 6.

1.4 Notations

When A is a random variable or distribution, $y \stackrel{R}{\leftarrow} A$ denotes that y is randomly selected from A according to its distribution. When A is a set, $y \stackrel{U}{\leftarrow} A$ 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{x} denotes $(x_1, \dots, x_n) \in \mathbb{F}_q^n$. For two vectors $\vec{x} = (x_1, \dots, x_n)$ and $\vec{v} = (v_1, \dots, v_n)$, $\vec{x} \cdot \vec{v}$ denotes the inner-product $\sum_{i=1}^n x_i v_i$. The vector $\vec{0}$ is abused as the zero vector in \mathbb{F}_q^n for any n . X^T denotes the transpose of matrix X . A bold face letter denotes an element of vector space \mathbb{V} , e.g., $\mathbf{x} \in \mathbb{V}$. When $\mathbf{b}_i \in \mathbb{V}$ ($i = 1, \dots, n$), $\text{span}\langle \mathbf{b}_1, \dots, \mathbf{b}_n \rangle \subseteq \mathbb{V}$ (resp. $\text{span}\langle \vec{x}_1, \dots, \vec{x}_n \rangle$) denotes the subspace generated by $\mathbf{b}_1, \dots, \mathbf{b}_n$ (resp. $\vec{x}_1, \dots, \vec{x}_n$). For bases $\mathbb{B} := (\mathbf{b}_1, \dots, \mathbf{b}_N)$ and $\mathbb{B}^* := (\mathbf{b}_1^*, \dots, \mathbf{b}_N^*)$, $(x_1, \dots, x_N)_{\mathbb{B}} := \sum_{i=1}^N x_i \mathbf{b}_i$ and $(y_1, \dots, y_N)_{\mathbb{B}^*} := \sum_{i=1}^N y_i \mathbf{b}_i^*$.

\vec{e}_j denotes the canonical basis vector $(\overbrace{0 \cdots 0}^{j-1}, 1, \overbrace{0 \cdots 0}^{n-j}) \in \mathbb{F}_q^n$. $GL(n, \mathbb{F}_q)$ denotes the general linear group of degree n over \mathbb{F}_q .

2 Definition of Key-Policy Attribute-Based Encryption

2.1 Span Programs and Non-Monotone Access Structures

Definition 1 (Span Programs [2]). Let $\{p_1, \dots, p_n\}$ be a set of variables. A span program over \mathbb{F}_q is a labeled matrix $\hat{M} := (M, \rho)$ 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 $\{p_1, \dots, p_n, \neg p_1, \dots, \neg p_n\}$ (every row is labeled by one literal), i.e., $\rho : \{1, \dots, \ell\} \rightarrow \{p_1, \dots, p_n, \neg p_1, \dots, \neg p_n\}$.

A span program accepts or rejects an input by the following criterion. For every input sequence $\delta \in \{0, 1\}^n$ define the submatrix M_δ of M consisting of those rows whose labels are set to 1 by the input δ , i.e., either rows labeled by some p_i such that $\delta_i = 1$ or rows labeled by some $\neg p_i$ such that $\delta_i = 0$. (i.e., $\gamma : \{1, \dots, \ell\} \rightarrow \{0, 1\}$ is defined by $\gamma(j) = 1$ if $[\rho(j) = p_i] \wedge [\delta_i = 1]$ or $[\rho(j) = \neg p_i] \wedge [\delta_i = 0]$, and $\gamma(j) = 0$ otherwise. $M_\delta := (M_j)_{\gamma(j)=1}$, where M_j is the j -th row of M .)

The span program \hat{M} accepts δ if and only if $\vec{1} \in \text{span}\langle M_\delta \rangle$, i.e., some linear combination of the rows of M_δ gives the all one vector $\vec{1}$. (The row vector has the value 1 in each coordinate.) A span program computes a Boolean function f if it accepts exactly those inputs δ where $f(\delta) = 1$.

A span program is called monotone if the labels of the rows are only the positive literals $\{p_1, \dots, p_n\}$. Monotone span programs compute monotone functions. (So, a span program in general is “non”-monotone.)

We assume that no row M_i ($i = 1, \dots, \ell$) of the matrix M is $\vec{0}$. We now introduce a non-monotone access structure with evaluating map γ that is employed in the proposed attribute-based encryption schemes.

Definition 2 (Access Structures). $\mathcal{U} (\subset \{0, 1\}^*)$ is a universe, a set of attributes, which is expressed by a value of attribute, i.e., $v \in \mathbb{F}_q^\times (:= \mathbb{F}_q \setminus \{0\})$.

We now define such an attribute to be a variable p of a span program $\hat{M} := (M, \rho)$, i.e., $p := v$. An access structure \mathbb{S} is span program $\hat{M} := (M, \rho)$ along with variables $p := v, p' := v', \dots$, i.e., $\mathbb{S} := (M, \rho)$ such that $\rho : \{1, \dots, \ell\} \rightarrow \{v, v', \dots, \neg v, \neg v', \dots\}$.

Let Γ be a set of attributes, i.e., $\Gamma := \{x_j\}_{1 \leq j \leq n'}$. When Γ is given to access structure \mathbb{S} , map $\gamma : \{1, \dots, \ell\} \rightarrow \{0, 1\}$ for span program $\hat{M} := (M, \rho)$ is defined as follows: For $i = 1, \dots, \ell$, set $\gamma(i) = 1$ if $[\rho(i) = v_i] \wedge [v_i \in \Gamma]$ or $[\rho(i) = \neg v_i] \wedge [v_i \notin \Gamma]$. Set $\gamma(i) = 0$ otherwise.

Access structure $\mathbb{S} := (M, \rho)$ accepts Γ iff $\vec{1} \in \text{span}\langle (M_i)_{\gamma(i)=1} \rangle$.

We now construct a secret-sharing scheme for a non-monotone access structure or span program.

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

1. Let M be $\ell \times r$ matrix. Let column vector $\vec{f}^\top := (f_1, \dots, f_r)^\top \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q^r$. Then, $s_0 := \vec{1} \cdot \vec{f}^\top = \sum_{k=1}^r f_k$ is the secret to be shared, and $\vec{s}^\top := (s_1, \dots, s_\ell)^\top := M \cdot \vec{f}^\top$ is the vector of ℓ shares of the secret s_0 and the share s_i belongs to $\rho(i)$.
2. If span program $\hat{M} := (M, \rho)$ accepts δ , or access structure $\mathbb{S} := (M, \rho)$ accepts Γ , i.e., $\vec{1} \in \text{span}\langle (M_i)_{\gamma(i)=1} \rangle$ with $\gamma : \{1, \dots, \ell\} \rightarrow \{0, 1\}$, then there exist constants $\{\alpha_i \in \mathbb{F}_q \mid i \in I\}$ such that $I \subseteq \{i \in \{1, \dots, \ell\} \mid \gamma(i) = 1\}$ 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 .

2.2 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 **Setup**, **KeyGen**, **Enc** and **Dec**. They are given as follows:

Setup takes as input security parameter 1^λ and a bound on the number of attributes per ciphertext n . 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 $\text{sk}_{\mathbb{S}}$.

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

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

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

Definition 5. The model for defining the selectively payload-hiding security of KP-ABE under chosen plaintext attack is given by the following game:

Setup The adversary outputs a challenge attribute set, Γ . The challenger runs the setup algorithm, $(\text{pk}, \text{sk}) \stackrel{\text{R}}{\leftarrow} \text{Setup}(1^\lambda, n)$, 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 provided that \mathbb{S} does not accept Γ . The challenger gives $\text{sk}_{\mathbb{S}} \stackrel{\text{R}}{\leftarrow} \text{KeyGen}(\text{pk}, \text{sk}, \mathbb{S})$ to the adversary.

Challenge The adversary submits two messages $m^{(0)}, m^{(1)}$. The challenger flips a coin $b \xleftarrow{U} \{0, 1\}$, and computes $\text{ct}_\Gamma^{(b)} \xleftarrow{R} \text{Enc}(\text{pk}, m^{(b)}, \Gamma)$. It gives $\text{ct}_\Gamma^{(b)}$ 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 above game is defined as $\text{Adv}_{\mathcal{A}}^{\text{KP-ABE,PH}}(\lambda) := \Pr[\mathcal{A} \text{ wins}] - 1/2$ for any security parameter λ . A KP-ABE scheme is selectively payload-hiding secure if all polynomial time adversaries have at most a negligible advantage in the above game.

3 Special Matrix Subgroups

Lemmas 1 and 2 are key lemmas for the security proof for our KP-ABE and ABS schemes. For positive integers w, n and $\vec{y} := (y_1, \dots, y_n) \in \mathbb{F}_q^n - \text{span}(\vec{e}_n)$, let

$$\mathcal{H}(n, \mathbb{F}_q) := \left\{ \left(\begin{array}{ccc} u & & u'_1 \\ & \ddots & \vdots \\ & & u u'_{n-1} \\ & & & u'_n \end{array} \right) \middle| \begin{array}{l} u, u'_l \in \mathbb{F}_q \text{ for } l = 1, \dots, n, \\ \text{a blank element in the matrix} \\ \text{denotes } 0 \in \mathbb{F}_q \end{array} \right\}, \quad (1)$$

$$\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q) := \left\{ \left(\begin{array}{ccc} 1 & & u'_1 \\ & \ddots & \vdots \\ & & 1 u'_{n-1} \\ & & & u'_n \end{array} \right) \middle| \begin{array}{l} \vec{u}' := (u'_l)_{l=1, \dots, n} \in \mathbb{F}_q^n, \quad \vec{y} \cdot \vec{u}' = y_n \\ \text{a blank element in the matrix} \\ \text{denotes } 0 \in \mathbb{F}_q \end{array} \right\}. \quad (2)$$

Lemma 1. $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q) \subset \mathcal{H}(n, \mathbb{F}_q)$. $\mathcal{H}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q)$ and $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q)$ are subgroups of $GL(n, \mathbb{F}_q)$.

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

Let

$$\mathcal{L}(w, n, \mathbb{F}_q) := \left\{ X := \left(\begin{array}{ccc} X_{1,1} & \cdots & X_{1,w} \\ \vdots & & \vdots \\ X_{w,1} & \cdots & X_{w,w} \end{array} \right) \middle| X_{i,j} := \left(\begin{array}{ccc} \mu_{i,j} & & \mu'_{i,j,1} \\ & \ddots & \vdots \\ & & \mu_{i,j} \mu'_{i,j,n-1} \\ & & & \mu'_{i,j,n} \end{array} \right) \in \mathcal{H}(n, \mathbb{F}_q) \right. \\ \left. \cap GL(w, \mathbb{F}_q) \right\} \quad \text{for } i, j = 1, \dots, w \quad (3)$$

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

The proof of Lemma 2 is given in Appendix A in the full version of [24].

4 Proposed KP-ABE Scheme with Constant Size Ciphertexts

4.1 Dual Pairing Vector Spaces by Direct Product of Symmetric Pairing Groups

In this paper, for simplicity of description, we will present the proposed schemes on the symmetric version of dual pairing vector spaces (DPVS) [21, 22] constructed using symmetric bilinear pairing

groups given in Definition 6. 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, $(q, \mathbb{V}, \mathbb{V}^*, \mathbb{G}_T, \mathbb{A}, \mathbb{A}^*, e)$, for which see Appendix A.2 of the full version of [23]. The symmetric version is a specific (self-dual) case of the asymmetric version, where $\mathbb{V} = \mathbb{V}^*$ and $\mathbb{A} = \mathbb{A}^*$.

Definition 6. “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 $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ i.e., $e(sG, tG) = e(G, G)^{st}$ and $e(G, G) \neq 1$. Let \mathcal{G}_{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 .

Definition 7. “Dual pairing vector spaces (DPVS)” $(q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e)$ by a direct product of symmetric pairing groups $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ are a tuple of 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 , canonical basis $\mathbb{A} := (\mathbf{a}_1, \dots, \mathbf{a}_N)$ of \mathbb{V} , where $\mathbf{a}_i := (0, \dots, 0, G, \overbrace{0, \dots, 0}^{N-i})$, and pairing $e : \mathbb{V} \times \mathbb{V} \rightarrow \mathbb{G}_T$. The pairing is defined by $e(\mathbf{x}, \mathbf{y}) := \prod_{i=1}^N e(G_i, H_i) \in \mathbb{G}_T$ where $\mathbf{x} := (G_1, \dots, G_N) \in \mathbb{V}$ and $\mathbf{y} := (H_1, \dots, H_N) \in \mathbb{V}$. This is nondegenerate bilinear i.e., $e(s\mathbf{x}, t\mathbf{y}) = e(\mathbf{x}, \mathbf{y})^{st}$ and if $e(\mathbf{x}, \mathbf{y}) = 1$ for all $\mathbf{y} \in \mathbb{V}$, then $\mathbf{x} = \mathbf{0}$. For all i and j , $e(\mathbf{a}_i, \mathbf{a}_j) = e(G, G)^{\delta_{i,j}}$ where $\delta_{i,j} = 1$ if $i = j$, and 0 otherwise, and $e(G, G) \neq 1 \in \mathbb{G}_T$. DPVS generation algorithm $\mathcal{G}_{\text{dpvs}}$ takes input 1^λ ($\lambda \in \mathbb{N}$) and $N \in \mathbb{N}$, and outputs a description of $\text{param}_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e)$ with security parameter λ and N -dimensional \mathbb{V} . It can be constructed by using \mathcal{G}_{bpg} .

4.2 Key Ideas in Constructing the Proposed KP-ABE Scheme

In this section, we will explain key ideas of constructing and proving the security of the proposed KP-ABE scheme.

First, we will show how short ciphertexts and efficient decryption can be achieved in our scheme, where the IPE scheme given in [24] is used as a building block. Here, we will use a simplified (or toy) version of the proposed 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, $(\mathbf{c}_0, \mathbf{c}_1) \in \mathbb{G}^5 \times \mathbb{G}^n$, and $c_3 \in \mathbb{G}_T$. A secret-key consists of $\ell + 1$ vector elements, $(\mathbf{k}_0^*, \mathbf{k}_1^*, \dots, \mathbf{k}_\ell^*) \in \mathbb{G}^5 \times (\mathbb{G}^n)^\ell$ for access structure $\mathbb{S} := (M, \rho)$, where the number of rows of M is ℓ and \mathbf{k}_i^* with $i \geq 1$ corresponds to the i -th row. Therefore, to achieve constant-size ciphertexts, we have to compress $\mathbf{c}_1 \in \mathbb{G}^n$ to a constant size in n . We now employ a special form of basis generation matrix,

$$X := \begin{pmatrix} \mu & \mu'_1 \\ \ddots & \vdots \\ & \mu \mu'_{n-1} \\ & & \mu'_n \end{pmatrix} \in \mathcal{H}(n, \mathbb{F}_q) \text{ of Eq. (1) in Section 3, where } \mu, \mu'_1, \dots, \mu'_n \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q \text{ and a blank in}$$

$$\text{the matrix denotes } 0 \in \mathbb{F}_q. \text{ The public key (DPVS basis) is } \mathbb{B} := \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_n \end{pmatrix} := \begin{pmatrix} \mu G & \mu'_1 G \\ \ddots & \vdots \\ \mu G \mu'_{n-1} G & \mu'_n G \end{pmatrix}.$$

Let a ciphertext associated with $\Gamma := \{x_1, \dots, x_{n'}\}$ be $\mathbf{c}_1 := (\omega \vec{y})_{\mathbb{B}} = \omega(y_1 \mathbf{b}_1 + \dots + y_n \mathbf{b}_n) =$

$(y_1\omega\mu G, \dots, y_{n-1}\omega\mu G, \omega(\sum_{i=1}^n y_i\mu'_i)G)$, where $\omega \stackrel{\cup}{\leftarrow} \mathbb{F}_q$ and $\vec{y} := (y_1, \dots, y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j}z^j = z^{n-1-n'} \cdot \prod_{j=1}^n (z - x_j)$. Then, \mathbf{c}_1 can be compressed to only *two* group elements ($C_1 := \omega\mu G$, $C_2 := \omega(\sum_{i=1}^n y_i\mu'_i)G$) as well as \vec{y} , since \mathbf{c}_1 can be obtained by $(y_1C_1, \dots, y_{n-1}C_1, C_2)$ (note that $y_iC_1 = y_i\omega\mu G$ for $i = 1, \dots, n-1$). That is, a ciphertext (excluding \vec{y}) can be just two group elements, or the size is constant in n .

Let $\mathbb{B}^* := (\mathbf{b}_i^*)$ be the dual orthonormal basis of $\mathbb{B} := (\mathbf{b}_i)$, and \mathbb{B}^* be the master secret key in the simplified KP-ABE scheme. We specify $(\mathbf{c}_0, \mathbf{k}_0^*, c_3)$ such that $e(\mathbf{c}_0, \mathbf{k}_0^*) = g_T^{\zeta - \omega s_0}$ and $c_3 := g_T^{\zeta} m \in \mathbb{G}_T$ with s_0 is a center secret of shares $\{s_i\}_{i=1, \dots, \ell}$ associated with access structure \mathbb{S} . Using $\{s_i\}_{i=1, \dots, \ell}$, we also set a secret-key for \mathbb{S} as $\mathbf{k}_i^* := (s_i\vec{e}_1 + \theta_i\vec{v}_i)_{\mathbb{B}^*}$ if $\rho(i) = v_i$ and $\mathbf{k}_i^* := (s_i\vec{v}_i)_{\mathbb{B}^*}$ if $\rho(i) = -v_i$ where $\vec{v}_i := (v_i^{n-1}, \dots, v_i, 1)$ and $\theta_i \stackrel{\cup}{\leftarrow} \mathbb{F}_q$. From the dual orthonormality of \mathbb{B} and \mathbb{B}^* , if \mathbb{S} accepts Γ , there exist a system of coefficients $\{\alpha_i\}_{i \in \Gamma}$ such that $e(\mathbf{c}_1, \tilde{\mathbf{k}}^*) = g_T^{\omega s_0}$, where $\tilde{\mathbf{k}}^* := \sum_{i \in \Gamma \wedge \rho(i)=v_i} \alpha_i \mathbf{k}_i^* + \sum_{i \in \Gamma \wedge \rho(i)=-v_i} \alpha_i (\vec{y} \cdot \vec{v}_i)^{-1} \mathbf{k}_i^*$. Hence, a decryptor can compute $g_T^{\omega s_0}$ if and only if \mathbb{S} accepts Γ , i.e., can obtain plaintext m . Since \mathbf{c}_1 is expressed as $(y_1C_1, \dots, y_{n-1}C_1, C_2) \in \mathbb{G}^n$ and $\tilde{\mathbf{k}}^*$ is parsed as a n -tuple $(D_1^*, \dots, D_n^*) \in \mathbb{G}^n$, the value of $e(\mathbf{c}_1, \tilde{\mathbf{k}}^*)$ is $\prod_{i=1}^{n-1} e(y_iC_1, D_i^*) \cdot e(C_2, D_n^*) = \prod_{i=1}^{n-1} e(C_1, y_iD_i^*) \cdot e(C_2, D_n^*) = e(C_1, \sum_{i=1}^{n-1} y_iD_i^*) \cdot e(C_2, D_n^*)$. That is, $n-1$ scalar multiplications in \mathbb{G} and *two* pairing operations are enough for computing $e(\mathbf{c}_1, \tilde{\mathbf{k}}^*)$. Therefore, only a small (constant) number of pairing operations are required for decryption.

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 (selective) security *under the DLIN assumption*. Here, we adopt and extend a strategy initiated in [23], in which the dual system encryption methodology is employed in a modular or hierarchical manner. That is, one top level assumption, the security of Problem 1, is directly used in the dual system encryption methodology and the assumption is 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 six times greater than that of the above-mentioned simplified scheme. For example, $\mathbf{k}_i^* := (s_i\vec{e}_1 + \theta_i\vec{v}_i, 0^{2n}, \vec{\eta}_i, 0^n)_{\mathbb{B}_1^*}$ if $\rho(i) = v_i$, $\mathbf{k}_i^* := (s_i\vec{v}_i, 0^{2n}, \vec{\eta}_i, 0^n)_{\mathbb{B}_1^*}$ if $\rho(i) = -v_i$, $\mathbf{c}_1 = (\omega\vec{y}, 0^{2n}, 0^{2n}, \varphi_1\vec{y})_{\mathbb{B}_1}$, and $X := \begin{pmatrix} X_{1,1} & \cdots & X_{1,6} \\ \vdots & & \vdots \\ X_{6,1} & \cdots & X_{6,6} \end{pmatrix} \in \mathcal{L}(6, n, \mathbb{F}_q)$ of Eq. (3) in Section 3, where each $X_{i,j}$ is of the form of $X \in \mathcal{H}(n, \mathbb{F}_q)$ 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 $\mathcal{L}(6, n, \mathbb{F}_q)$ is a *subgroup* of $GL(6n, \mathbb{F}_q)$ (Lemma 2), which enables a *random-self-reducibility* argument for reducing the intractability of Problem 1 in Definition 8 to the DLIN assumption. The property that $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q)$ is a *subgroup* of $GL(n, \mathbb{F}_q)$ is also crucial for a special form of pairwise independence lemma in this paper (Lemma 4), where a super-group $\mathcal{H}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q) (\supset \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q))$ is specified in $\mathcal{L}(6, n, \mathbb{F}_q)$ or X . Our Problem 1 employs the special form matrices $\{U_j \stackrel{\cup}{\leftarrow} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q)\}$ and $\{Z_j := (U_j^{-1})^T\}$, and makes Lemma 4 applicable in our proof. Informally, our pairwise independence lemma implies that, for all (\vec{y}, \vec{v}) , a vector, $\vec{v}Z$, is uniformly distributed over $\mathbb{F}_q^n - \text{span}(\vec{e}_n)^\perp$ with preserving the inner-product value, $\vec{y} \cdot \vec{v}$, i.e., $\vec{v}Z$ reveal no information but $(\vec{y}$ and) $\vec{y} \cdot \vec{v}$.

4.3 Dual Orthonormal Basis Generator

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

$$\begin{aligned}
\mathcal{G}_{\text{ob}}^{\text{KP-ABE}}(1^\lambda, 6, n) : & \text{ param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\text{R}} \mathcal{G}_{\text{bpg}}(1^\lambda), \quad N_0 := 5, \quad N_1 := 6n, \\
& \text{ param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\text{dps}}(1^\lambda, N_t, \text{ param}_{\mathbb{G}}) \text{ for } t = 0, 1, \\
& \psi \xleftarrow{\text{U}} \mathbb{F}_q^\times, \quad g_T := e(G, G)^\psi, \quad \text{ param}_n := (\{\text{ param}_{\mathbb{V}_t}\}_{t=0,1}, g_T), \\
X_0 := & (\chi_{0,i,j})_{i,j=1,\dots,5} \xleftarrow{\text{U}} GL(N_0, \mathbb{F}_q), \quad X_1 \xleftarrow{\text{U}} \mathcal{L}(6, n, \mathbb{F}_q), \text{ hereafter,} \\
& \{\mu_{i,j}, \mu'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n} \text{ denotes non-zero entries of } X_1 \text{ as in Eq. (3),} \\
\mathbf{b}_{0,i} := & (\chi_{0,i,1}, \dots, \chi_{0,i,5})_{\mathbb{A}} = \sum_{j=1}^5 \chi_{0,i,j} \mathbf{a}_j \text{ for } i = 1, \dots, 5, \quad \mathbb{B}_0 := (\mathbf{b}_{0,1}, \dots, \mathbf{b}_{0,5}), \\
B_{i,j} := & \mu_{i,j} G, \quad B'_{i,j,l} := \mu'_{i,j,l} G \text{ for } i, j = 1, \dots, 6; l = 1, \dots, n, \\
\text{for } t = 0, 1, & (\vartheta_{t,i,j})_{i,j=1,\dots,N_t} := \psi \cdot (X_t^{\text{T}})^{-1}, \\
\mathbf{b}_{t,i}^* := & (\vartheta_{t,i,1}, \dots, \vartheta_{t,i,N_t})_{\mathbb{A}} = \sum_{j=1}^{N_t} \vartheta_{t,i,j} \mathbf{a}_j \text{ for } i = 1, \dots, N_t, \quad \mathbb{B}_t^* := (\mathbf{b}_{t,1}^*, \dots, \mathbf{b}_{t,N_t}^*), \\
\text{return } & (\text{ param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \mathbb{B}_1^*).
\end{aligned}$$

Remark 1 Let

$$\left. \begin{aligned}
\begin{pmatrix} \mathbf{b}_{1,(i-1)n+1} \\ \vdots \\ \mathbf{b}_{1,in} \end{pmatrix} & := \begin{pmatrix} B_{i,1} & & B'_{i,1,1} & B_{i,6} & & B'_{i,6,1} \\ & \ddots & \vdots & & \ddots & \vdots \\ & & B_{i,1} & B'_{i,1,n-1} & & B_{i,6} & B'_{i,6,n-1} \\ & & & B'_{i,1,n} & & & B'_{i,6,n} \end{pmatrix} \\
& \text{for } i = 1, \dots, 6, \\
\mathbb{B}_1 := & (\mathbf{b}_{1,1}, \dots, \mathbf{b}_{1,6n}),
\end{aligned} \right\} \quad (4)$$

where a blank element in the matrix denotes $0 \in \mathbb{G}$. \mathbb{B}_1 is the dual orthonormal basis of \mathbb{B}_1^* , i.e., $e(\mathbf{b}_{1,i}, \mathbf{b}_{1,i}^*) = g_T$ and $e(\mathbf{b}_{1,i}, \mathbf{b}_{1,j}^*) = 1$ for $1 \leq i \neq j \leq 6n$.

4.4 Construction

We note that attributes x_j, v_i are in \mathbb{F}_q^\times , i.e., nonzero.

$$\begin{aligned}
\text{Setup}(1^\lambda, n) : & (\text{ param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \mathbb{B}_1^*) \xleftarrow{\text{R}} \mathcal{G}_{\text{ob}}^{\text{KP-ABE}}(1^\lambda, 6, n), \\
\widehat{\mathbb{B}}_0 := & (\mathbf{b}_{0,1}, \mathbf{b}_{0,3}, \mathbf{b}_{0,5}), \quad \widehat{\mathbb{B}}_1 := (\mathbf{b}_{1,1}, \dots, \mathbf{b}_{1,n}, \mathbf{b}_{1,5n+1}, \dots, \mathbf{b}_{1,6n}) = \{B_{i,j}, B'_{i,j,l}\}_{i=1,6;j=1,\dots,6;l=1,\dots,n}, \\
\widehat{\mathbb{B}}_0^* := & (\mathbf{b}_{0,1}^*, \mathbf{b}_{0,3}^*, \mathbf{b}_{0,4}^*), \quad \widehat{\mathbb{B}}_1^* := (\mathbf{b}_{1,1}^*, \dots, \mathbf{b}_{1,n}^*, \mathbf{b}_{1,3n+1}^*, \dots, \mathbf{b}_{1,5n}^*), \\
\text{pk} := & (1^\lambda, \text{ param}_n, \{\widehat{\mathbb{B}}_t\}_{t=0,1}), \quad \text{sk} := \{\widehat{\mathbb{B}}_t^*\}_{t=0,1}, \quad \text{return pk, sk.} \\
\text{KeyGen}(\text{pk}, \text{sk}, \mathbb{S} := (M, \rho)) : & \vec{f} \xleftarrow{\text{U}} \mathbb{F}_q^r, \quad \vec{s}^{\text{T}} := (s_1, \dots, s_\ell)^{\text{T}} := M \cdot \vec{f}^{\text{T}}, \quad s_0 := \vec{1} \cdot \vec{f}^{\text{T}}, \quad \eta_0 \xleftarrow{\text{U}} \mathbb{F}_q, \\
\mathbf{k}_0^* := & (-s_0, 0, 1, \eta_0, 0)_{\mathbb{B}_0^*},
\end{aligned}$$

for $i = 1, \dots, \ell$, $\vec{v}_i := (v_i^{n-1}, \dots, v_i, 1)$ for $\rho(i) = v_i$ or $\neg v_i$, $\vec{\eta}_i \stackrel{\cup}{\leftarrow} \mathbb{F}_q^{2n}$,
if $\rho(i) = v_i \in \mathbb{F}_q^\times$, $\theta_i \stackrel{\cup}{\leftarrow} \mathbb{F}_q$, $\mathbf{k}_i^* := (\overbrace{s_i \vec{e}_1 + \theta_i \vec{v}_i}^n, \overbrace{0^{2n}}^{2n}, \overbrace{\vec{\eta}_i}^{2n}, \overbrace{0^n}^n)_{\mathbb{B}_1^*}$,
if $\rho(i) = \neg v_i$, $\mathbf{k}_i^* := (\overbrace{s_i \vec{v}_i}^n, \overbrace{0^{2n}}^{2n}, \overbrace{\vec{\eta}_i}^{2n}, \overbrace{0^n}^n)_{\mathbb{B}_1^*}$,
return $\text{sk}_{\mathbb{S}} := (\mathbb{S}, \mathbf{k}_0^*, \mathbf{k}_1^*, \dots, \mathbf{k}_\ell^*)$.

$\text{Enc}(\text{pk}, m, \Gamma := \{x_1, \dots, x_{n'} \mid x_j \in \mathbb{F}_q^\times, n' \leq n-1\}) :$

$\omega, \varphi_0, \varphi_1, \zeta \stackrel{\cup}{\leftarrow} \mathbb{F}_q$, $\vec{y} := (y_1, \dots, y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \cdot \prod_{j=1}^{n'} (z - x_j)$,
 $\mathbf{c}_0 := (\omega, 0, \zeta, 0, \varphi_0)_{\mathbb{B}_0}$,
 $C_{1,j} := \omega B_{1,j} + \varphi_1 B_{6,j}$, $C_{2,j} := \sum_{l=1}^n y_l (\omega B'_{1,j,l} + \varphi_1 B'_{6,j,l})$ for $j = 1, \dots, 6$,
 $c_3 := g_T^\zeta m$, $\text{ct}_\Gamma := (\Gamma, \mathbf{c}_0, \{C_{1,j}, C_{2,j}\}_{j=1, \dots, 6}, c_3)$. return ct_Γ .

$\text{Dec}(\text{pk}, \text{sk}_{\mathbb{S}} := (\mathbb{S}, \mathbf{k}_0^*, \mathbf{k}_1^*, \dots, \mathbf{k}_\ell^*), \text{ct}_\Gamma := (\Gamma, \mathbf{c}_0, \{C_{1,j}, C_{2,j}\}_{j=1, \dots, 6}, c_3)) :$

If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{x_1, \dots, x_{n'}\}$, 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
 $I \subseteq \{i \in \{1, \dots, \ell\} \mid [\rho(i) = v_i \wedge v_i \in \Gamma] \vee [\rho(i) = \neg v_i \wedge v_i \notin \Gamma]\}$,
 $\vec{y} := (y_1, \dots, y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \cdot \prod_{j=1}^{n'} (z - x_j)$,
 $(D_1^*, \dots, D_{6n}^*) := \sum_{i \in I \wedge \rho(i) = v_i} \alpha_i \mathbf{k}_i^* + \sum_{i \in I \wedge \rho(i) = \neg v_i} \frac{\alpha_i}{\vec{v}_i \cdot \vec{y}} \mathbf{k}_i^*$,
 $E_j^* := \sum_{l=1}^{n-1} y_{l-1} D_{(j-1)n+l}^*$ for $j = 1, \dots, 6$,
 $K := e(\mathbf{c}_0, \mathbf{k}_0^*) \cdot \prod_{j=1}^6 (e(C_{1,j}, E_j^*) \cdot e(C_{2,j}, D_{jn}^*))$, return $m' := c_3/K$.

Remark A part of the output of $\text{Setup}(1^\lambda, n)$, $\{B_{i,j}, B'_{i,j,l}\}_{i=1,6;j=1, \dots, 6;l=1, \dots, n}$, can be identified with $\widehat{\mathbb{B}}_1 := (\mathbf{b}_{1,1}, \dots, \mathbf{b}_{1,n}, \mathbf{b}_{1,5n+1}, \dots, \mathbf{b}_{1,6n})$ through the form of Eq. (4), while $\mathbb{B}_1 := (\mathbf{b}_{1,1}, \dots, \mathbf{b}_{1,6n})$ is identified with $\{B_{i,j}, B'_{i,j,l}\}_{i,j=1, \dots, 6;l=1, \dots, n}$ by Eq. (4). Decryption Dec can be alternatively described as:

$\text{Dec}'(\text{pk}, \text{sk}_{\mathbb{S}} := (\mathbb{S}, \mathbf{k}_0^*, \mathbf{k}_1^*, \dots, \mathbf{k}_\ell^*), \text{ct}_\Gamma := (\Gamma, \mathbf{c}_0, \{C_{1,j}, C_{2,j}\}_{j=1, \dots, 6}, c_3)) :$

If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{x_1, \dots, x_{n'}\}$, 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
 $I \subseteq \{i \in \{1, \dots, \ell\} \mid [\rho(i) = v_i \wedge v_i \in \Gamma] \vee [\rho(i) = \neg v_i \wedge v_i \notin \Gamma]\}$,
 $\vec{y} := (y_1, \dots, y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \cdot \prod_{j=1}^{n'} (z - x_j)$,

$\mathbf{c}_1 := (\overbrace{y_1 C_{1,1}, \dots, y_{n-1} C_{1,1}, C_{2,1}}^n, \overbrace{y_1 C_{1,2}, \dots, y_{n-1} C_{1,2}, C_{2,2}, \dots}^n, \dots, \overbrace{y_1 C_{1,5}, \dots, y_{n-1} C_{1,5}, C_{2,5}, y_1 C_{1,6}, \dots, y_{n-1} C_{1,6}, C_{2,6}}^n)$,

that is, $\mathbf{c}_1 = (\overbrace{\omega \vec{y}}^n, \overbrace{0^{2n}}^{2n}, \overbrace{0^{2n}}^{2n}, \overbrace{\varphi_1 \vec{y}}^n)_{\mathbb{B}_1}$,

$$K := e(\mathbf{c}_0, \mathbf{k}_0^*) \cdot e\left(\mathbf{c}_1, \sum_{i \in I \wedge \rho(i)=v_i} \alpha_i \mathbf{k}_i^* + \sum_{i \in I \wedge \rho(i)=-v_i} \frac{\alpha_i}{\vec{v}_i \cdot \vec{y}} \mathbf{k}_i^*\right),$$

return $m' := c_3/K$.

[Correctness]

$$\begin{aligned} & e(\mathbf{c}_0, \mathbf{k}_0^*) \prod_{i \in I \wedge \rho(i)=v_i} e(\mathbf{c}_1, \mathbf{k}_i^*)^{\alpha_i} \cdot \prod_{i \in I \wedge \rho(i)=-v_i} e(\mathbf{c}_1, \mathbf{k}_i^*)^{\alpha_i / (\vec{v}_i \cdot \vec{y})} \\ &= g_T^{-\omega s_0 + \zeta} \prod_{i \in I \wedge \rho(i)=v_i} g_T^{\omega \alpha_i s_i} \prod_{i \in I \wedge \rho(i)=-v_i} g_T^{\omega \alpha_i s_i (\vec{v}_i \cdot \vec{y}) / (\vec{v}_i \cdot \vec{y})} = g_T^{\omega(-s_0 + \sum_{i \in I} \alpha_i s_i) + \zeta} = g_T^\zeta. \end{aligned}$$

4.5 Security

The DLIN assumption is given in Appendix A.

Theorem 1. *The proposed KP-ABE scheme is selectively payload-hiding against chosen plaintext attacks under the DLIN assumption.*

For any adversary \mathcal{A} , there is a probabilistic machine \mathcal{F} , whose running time is essentially the same as that of \mathcal{A} , such that for any security parameter λ , $\text{Adv}_{\mathcal{A}}^{\text{KP-ABE,PH}}(\lambda) \leq \sum_{j=0}^n \sum_{\iota=1}^2 \text{Adv}_{\mathcal{F}_{j,\iota}}^{\text{DLIN}}(\lambda) + \epsilon$, where $\mathcal{F}_{j,\iota}(\cdot) := \mathcal{F}(j, \iota, \cdot)$ for $j = 0, \dots, n$; $\iota = 1, 2$, $\epsilon := (\nu\ell + 10n + 12)/q$, and ν is the maximum number of \mathcal{A} 's key queries, ℓ is the maximum number of rows in access matrices M of the key queries.

Proof Outline At the top level strategy of the security proof, the dual system encryption by Waters [30] is employed, where ciphertexts and secret keys have two forms, *normal* and *semi-functional*. The real system uses only normal ciphertexts and normal secret keys, and semi-functional ciphertexts and keys are used only in subsequent security games for the security proof.

To prove this theorem, we employ Game 0 (original selective-security game) through Game 2. In Game 1, the challenge ciphertext and all queried keys are changed to semi-functional form, respectively. In Game 2, the challenge ciphertext is changed to *non-functional* form. In the final game, the advantage of the adversary is zero. As usual, we prove that the advantage gaps between neighboring games are negligible.

A normal secret key (with access structure \mathbb{S}), is the correct form of the secret key of the proposed KP-ABE scheme, and is expressed by Eq. (5). Similarly, a normal ciphertext (with attributes Γ) is expressed by Eq. (6). A semi-functional ciphertext is expressed by Eq. (8). A semi-functional key is expressed by Eq. (7). A non-functional ciphertext is expressed by Eq. (9) (with \mathbf{c}_1 in Eq. (8)).

To prove that the advantage gap between Games 0 and 1 is bounded by the advantage of Problem 1 (to guess $\beta \in \{0, 1\}$), we construct a simulator of the challenger of Game 0 (or 1) (against an adversary \mathcal{A}) by using an instance with $\beta \stackrel{\text{U}}{\leftarrow} \{0, 1\}$ of Problem 1. We then show that the distribution of the secret keys and challenge ciphertext replied by the simulator is equivalent to those of Game 0 when $\beta = 0$ and those of Game 1 when $\beta = 1$. That is, the advantage of Problem 1 is equivalent to the advantage gap between Games 0 and 1 (Lemma 5). The advantage of Problem 1 is proven to be equivalent to $(2n + 2)$ -times of that of the DLIN assumption (Lemma 3).

We then show that Game 1 can be conceptually changed to Game 2 (Lemma 6), by using the fact that parts of bases, $\mathbf{b}_{0,2}$ and $\mathbf{b}_{0,3}^*$, are unknown to the adversary. In the conceptual change, we use the fact that the challenge ciphertext and all queried keys are semi-functional, i.e., respective coefficients of $\mathbf{b}_{0,2}$ and $\mathbf{b}_{0,2}^*$ are random.

Key Lemmas We will show Lemmas 3 and 4 for the proof of Theorem 1.

Definition 8 (Problem 1). *Problem 1 is to guess β , given $(\text{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}_\iota^*\}_{\iota=0,1}, \mathbf{h}_{\beta,0}^*, \mathbf{e}_{\beta,0}, \{\mathbf{h}_{\beta,j,i}^*\}_{j=1,\dots,n; i=1,\dots,n}, \mathbf{e}_{\beta,1}) \xleftarrow{R} \mathcal{G}_\beta^{\text{P1}}(1^\lambda, n, \vec{y})$, where*

$$\begin{aligned}
\mathcal{G}_\beta^{\text{P1}}(1^\lambda, n, \vec{y}) : & \quad (\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \mathbb{B}_1^*) \xleftarrow{R} \mathcal{G}_{\text{ob}}^{\text{KP-ABE}}(1^\lambda, 6, n), \\
\widehat{\mathbb{B}}_0 := & \quad (\mathbf{b}_{0,1}, \mathbf{b}_{0,3}, \dots, \mathbf{b}_{0,5}), \quad \widehat{\mathbb{B}}_0^* := (\mathbf{b}_{0,1}^*, \mathbf{b}_{0,3}^*, \dots, \mathbf{b}_{0,5}^*), \\
\widehat{\mathbb{B}}_1 := & \quad (\mathbf{b}_{1,1}, \dots, \mathbf{b}_{1,n}, \mathbf{b}_{1,3n+1}, \dots, \mathbf{b}_{1,6n}) \text{ is calculated as in Eq. (1) from } \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \\
\widehat{\mathbb{B}}_1^* := & \quad (\mathbf{b}_{1,1}^*, \dots, \mathbf{b}_{1,n}^*, \mathbf{b}_{1,3n+1}^*, \dots, \mathbf{b}_{1,6n}^*), \\
\delta, \delta_0, \omega, \varphi_0, \varphi_1 \xleftarrow{U} & \quad \mathbb{F}_q, \quad \tau, \rho \xleftarrow{U} \mathbb{F}_q^\times, \quad \mathbf{h}_{0,0}^* := (\delta, 0, 0, \delta_0, 0)_{\mathbb{B}_0^*}, \quad \mathbf{h}_{1,0}^* := (\delta, \rho, 0, \delta_0, 0)_{\mathbb{B}_0^*}, \\
\mathbf{e}_{0,0} := & \quad (\omega, 0, 0, 0, \varphi_0)_{\mathbb{B}_0}, \quad \mathbf{e}_{1,0} := (\omega, \tau, 0, 0, \varphi_0)_{\mathbb{B}_0}, \\
\text{for } j = 1, \dots, n; i = 1, \dots, n; & \quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \quad \vec{\delta}_{j,i} \xleftarrow{U} \mathbb{F}_q^{2n}, \\
U_j \xleftarrow{U} & \quad \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q), \quad Z_j := (U_j^{-1})^T, \\
& \quad \begin{array}{cccc}
& \overbrace{\hspace{1.5cm}}^n & \overbrace{\hspace{2.5cm}}^{2n} & \overbrace{\hspace{2.5cm}}^{2n} & \overbrace{\hspace{1.5cm}}^n \\
\mathbf{h}_{0,j,i}^* := & (\delta \vec{e}_i, & 0^{2n}, & \vec{\delta}_{j,i}, & 0^n)_{\mathbb{B}_1^*} \\
\mathbf{h}_{1,j,i}^* := & (\delta \vec{e}_i, & 0^n, \rho \vec{e}_i \cdot Z_j, & \vec{\delta}_{j,i}, & 0^n)_{\mathbb{B}_1^*} \\
\mathbf{e}_{0,1} := & (\omega \vec{y}, & 0^{2n}, & 0^{2n}, & \varphi_1 \vec{y})_{\mathbb{B}_1}, \\
\mathbf{e}_{1,1} := & (\omega \vec{y}, & \tau \vec{y}, \tau \vec{y}, & 0^{2n}, & \varphi_1 \vec{y})_{\mathbb{B}_1},
\end{array} \\
\text{return } & \quad (\text{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}_\iota^*\}_{\iota=0,1}, \mathbf{h}_{\beta,0}^*, \mathbf{e}_{\beta,0}, \{\mathbf{h}_{\beta,j,i}^*\}_{j=1,\dots,n; i=1,\dots,n}, \mathbf{e}_{\beta,1}),
\end{aligned}$$

for $\beta \xleftarrow{U} \{0, 1\}$. For a probabilistic adversary \mathcal{B} , we define the advantage of \mathcal{B} as the quantity $\text{Adv}_{\mathcal{B}}^{\text{P1}}(\lambda) := \left| \Pr \left[\mathcal{B}(1^\lambda, \varrho) \rightarrow 1 \mid \varrho \xleftarrow{R} \mathcal{G}_0^{\text{P1}}(1^\lambda, n) \right] - \Pr \left[\mathcal{B}(1^\lambda, \varrho) \rightarrow 1 \mid \varrho \xleftarrow{R} \mathcal{G}_1^{\text{P1}}(1^\lambda, n) \right] \right|$.

Lemma 3. *Problem 1 is computationally intractable under the DLIN assumption.*

For any adversary \mathcal{B} , there are probabilistic machines $\mathcal{F}_{j,\iota}$ ($j = 0, \dots, n; \iota = 1, 2$), whose running times are essentially the same as that of \mathcal{B} , such that for any security parameter λ , $\text{Adv}_{\mathcal{B}}^{\text{P1}}(\lambda) \leq \sum_{j=0}^n \sum_{\iota=1}^2 \text{Adv}_{\mathcal{F}_{j,\iota}}^{\text{DLIN}}(\lambda) + (10n + 10)/q$.

The proof of Lemma 3 is given in Appendix B. For an outline of the proof, see Section 6.

Next is a key lemma for applying the proof techniques in [23] to our KP-ABE and ABS schemes.

Lemma 4. *For all $\vec{y} \in \mathbb{F}_q^n - \text{span}\langle \vec{e}_n \rangle$ and $\pi \in \mathbb{F}_q$, let $W_{\vec{y},\pi} := \{\vec{w} \in \mathbb{F}_q^n - \text{span}\langle \vec{e}_n \rangle^\perp \mid \vec{y} \cdot \vec{w} = \pi\}$, where $\text{span}\langle \vec{e}_n \rangle^\perp := \{\vec{w} \in \mathbb{F}_q^n \mid \vec{w} \cdot \vec{e}_n = 0\}$.*

For all $(\vec{y}, \vec{v}) \in (\mathbb{F}_q^n - \text{span}\langle \vec{e}_n \rangle) \times (\mathbb{F}_q^n - \text{span}\langle \vec{e}_n \rangle^\perp)$, if Z is generated as $U \xleftarrow{U} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q)$ and $Z := (U^{-1})^T$ where $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ is defined by Eq. (2), then $\vec{v}Z$ is uniformly distributed in $W_{\vec{y},(\vec{y} \cdot \vec{v})}$.

The proof of Lemma 4 is given in Appendix C.

Proof of Theorem 1 : To prove Theorem 1, we consider the following 3 games. In Game 0, a part framed by a box indicates coefficients to be changed in a subsequent game. In the other games, a part framed by a box indicates coefficients which were changed in a game from the previous game.

Game 0 : Original game. That is, the reply to a key query for access structure $\mathbb{S} := (M, \rho)$ is:

$$\left. \begin{aligned} \mathbf{k}_0^* &:= (-s_0, \boxed{0}, 1, \eta_0, 0)_{\mathbb{B}_0^*}, \\ \text{for } i = 1, \dots, \ell; & \quad \underbrace{\hspace{2cm}}_n \quad \underbrace{\hspace{2cm}}_{2n} \quad \underbrace{\hspace{1cm}}_{2n} \quad \underbrace{\hspace{1cm}}_n \\ \text{if } \rho(i) = v_i, \mathbf{k}_i^* &:= (s_i \vec{e}_1 + \theta_i \vec{v}_i, 0^n, \boxed{0^n}, \vec{\eta}_i, 0^n)_{\mathbb{B}_1^*}, \\ \text{if } \rho(i) = \neg v_i, \mathbf{k}_i^* &:= (s_i \vec{v}_i, 0^n, \boxed{0^n}, \vec{\eta}_i, 0^n)_{\mathbb{B}_1^*}, \end{aligned} \right\} \quad (5)$$

where $\vec{f} \xleftarrow{\mathbb{U}} \mathbb{F}_q^r$, $\vec{s}^\top := (s_1, \dots, s_\ell)^\top := M \cdot \vec{f}^\top$, $s_0 := \vec{1} \cdot \vec{f}^\top$, $(s'_1, \dots, s'_\ell) \xleftarrow{\mathbb{U}} \mathbb{F}_q^\ell$, $\theta_i, \eta_0 \xleftarrow{\mathbb{U}} \mathbb{F}_q$, $\vec{\eta}_i \xleftarrow{\mathbb{U}} \mathbb{F}_q^n$, $\vec{e}_1 = (1, 0, \dots, 0) \in \mathbb{F}_q^n$, and $\vec{v}_i := (v_i^{n-1}, \dots, v_i, 1) \in (\mathbb{F}_q^\times)^n$. The challenge ciphertext for challenge plaintexts $(m^{(0)}, m^{(1)})$ and $\Gamma := \{x_1, \dots, x_{n'}\}$ with $n' \leq n - 1$ is:

$$\left. \begin{aligned} \mathbf{c}_0 &:= (\omega, \boxed{0}, \boxed{\zeta}, 0, \varphi_0)_{\mathbb{B}_0}, \quad \mathbf{c}_3 := g_T^\zeta m^{(b)}, \\ & \quad \underbrace{\hspace{2cm}}_n \quad \underbrace{\hspace{2cm}}_{2n} \quad \underbrace{\hspace{1cm}}_{2n} \quad \underbrace{\hspace{1cm}}_n \\ \mathbf{c}_1 &:= (\omega \vec{y}, \boxed{0^{2n}}, 0^{2n}, \varphi_1 \vec{y})_{\mathbb{B}_1}, \end{aligned} \right\} \quad (6)$$

where $b \xleftarrow{\mathbb{U}} \{0, 1\}$; $\omega, \zeta, \varphi_0, \varphi_1 \xleftarrow{\mathbb{U}} \mathbb{F}_q$, and $\vec{y} := (y_1, \dots, y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'}$. $\prod_{j=1}^{n'} (z - x_j)$.

Game 1 : Same as Game 0 except that the reply to a key query for access structure $\mathbb{S} := (M, \rho)$ are:

$$\left. \begin{aligned} \mathbf{k}_0^* &:= (-s_0, \boxed{w_0}, 1, \eta_0, 0)_{\mathbb{B}_0^*}, \\ \text{for } i = 1, \dots, \ell; & \quad \underbrace{\hspace{2cm}}_n \quad \underbrace{\hspace{2cm}}_{2n} \quad \underbrace{\hspace{1cm}}_{2n} \quad \underbrace{\hspace{1cm}}_n \\ \text{if } \rho(i) = v_i, \mathbf{k}_i^* &:= (s_i \vec{e}_1 + \theta_i \vec{v}_i, 0^n, \boxed{\vec{w}_i}, \vec{\eta}_i, 0^n)_{\mathbb{B}_1^*}, \\ \text{if } \rho(i) = \neg v_i, \mathbf{k}_i^* &:= (s_i \vec{v}_i, 0^n, \boxed{\vec{w}_i}, \vec{\eta}_i, 0^n)_{\mathbb{B}_1^*}, \end{aligned} \right\} \quad (7)$$

where $\vec{g} \xleftarrow{\mathbb{U}} \mathbb{F}_q^r$, $\vec{r}^\top := (r_1, \dots, r_\ell)^\top := M \cdot \vec{g}^\top$, $w_0 \xleftarrow{\mathbb{U}} \mathbb{F}_q$, $\psi_i \xleftarrow{\mathbb{U}} \mathbb{F}_q$, $\vec{w}_i \xleftarrow{\mathbb{U}} \{\vec{w}_i \in \mathbb{F}_q^n \mid \vec{w}_i \cdot \vec{y} = (r_i \vec{e}_1 + \psi_i \vec{v}_i) \cdot \vec{y}\}$, $\vec{\bar{w}}_i \xleftarrow{\mathbb{U}} \{\vec{\bar{w}}_i \in \mathbb{F}_q^n \mid \vec{\bar{w}}_i \cdot \vec{y} = r_i \vec{v}_i \cdot \vec{y}\}$, and the challenge ciphertext is:

$$\left. \begin{aligned} \mathbf{c}_0 &:= (\omega, \boxed{\tau}, \zeta, 0, \varphi_0)_{\mathbb{B}_0}, \quad \mathbf{c}_3 := g_T^\zeta m^{(b)}, \\ & \quad \underbrace{\hspace{2cm}}_n \quad \underbrace{\hspace{2cm}}_{2n} \quad \underbrace{\hspace{1cm}}_{2n} \quad \underbrace{\hspace{1cm}}_n \\ \mathbf{c}_1 &:= (\omega \vec{y}, \boxed{\tau \vec{y}, \tau \vec{y}}, 0^{2n}, \varphi_1 \vec{y})_{\mathbb{B}_1}, \end{aligned} \right\} \quad (8)$$

where $\tau \xleftarrow{\mathbb{U}} \mathbb{F}_q$, and all the other variables are generated as in Game 0.

Game 2 : Game 2 is the same as Game 1 except \mathbf{c}_0 (and \mathbf{c}_3) of the challenge ciphertext are

$$\mathbf{c}_0 := (\omega, \tau, \boxed{\zeta'}, 0, \varphi_0)_{\mathbb{B}_0}, \quad \mathbf{c}_3 := g_T^{\zeta'} m^{(b)}, \quad (9)$$

where $\zeta' \stackrel{U}{\leftarrow} \mathbb{F}_q$ (i.e., independent from $\zeta \stackrel{U}{\leftarrow} \mathbb{F}_q$), and all the other variables are generated as in Game 1.

Let $\text{Adv}_{\mathcal{A}}^{(0)}(\lambda)$, $\text{Adv}_{\mathcal{A}}^{(1)}(\lambda)$, and $\text{Adv}_{\mathcal{A}}^{(2)}(\lambda)$ be the advantage of \mathcal{A} in Game 0,1 and 2, respectively. $\text{Adv}_{\mathcal{A}}^{(0)}(\lambda)$ is equivalent to $\text{Adv}_{\mathcal{A}}^{\text{KP-ABE,PH}}(\lambda)$ and it is clear that $\text{Adv}_{\mathcal{A}}^{(2)}(\lambda) = 0$ by Lemma 7.

We will show two lemmas (Lemmas 5 and 6) that evaluate the gaps between pairs of $\text{Adv}_{\mathcal{A}}^{(0)}(\lambda)$, $\text{Adv}_{\mathcal{A}}^{(1)}(\lambda)$, $\text{Adv}_{\mathcal{A}}^{(2)}(\lambda)$. From these lemmas and Lemma 3, we obtain $\text{Adv}_{\mathcal{A}}^{\text{KP-ABE}}(\lambda) = \text{Adv}_{\mathcal{A}}^{(0)}(\lambda) \leq \left| \text{Adv}_{\mathcal{A}}^{(0)}(\lambda) - \text{Adv}_{\mathcal{A}}^{(1)}(\lambda) \right| + \left| \text{Adv}_{\mathcal{A}}^{(1)}(\lambda) - \text{Adv}_{\mathcal{A}}^{(2)}(\lambda) \right| \leq \text{Adv}_{\mathcal{B}}^{\text{P1}}(\lambda) + (\nu\ell + 2)/q \leq \sum_{j=0}^n \sum_{\ell=1}^2 \text{Adv}_{\mathcal{F}_{j,\ell}}^{\text{DLIN}}(\lambda) + (\nu\ell + 10n + 12)/q$. This completes the proof of Theorem 1. \square

Lemma 5. *For any adversary \mathcal{A} , there exists a probabilistic machine \mathcal{B} , whose running time is essentially the same as that of \mathcal{A} , such that for any security parameter λ , $|\text{Adv}_{\mathcal{A}}^{(1)}(\lambda) - \text{Adv}_{\mathcal{A}}^{(0)}(\lambda)| \leq \text{Adv}_{\mathcal{B}}^{\text{P1}}(\lambda) + (\nu\ell + 1)/q$, where ν is the maximum number of \mathcal{A} 's key queries, ℓ is the maximum number of rows in access matrices M of key queries.*

The proof of Lemma 5 is given in Appendix D.

Lemma 6. *For any adversary \mathcal{A} , for any security parameter λ , $|\text{Adv}_{\mathcal{A}}^{(2)}(\lambda) - \text{Adv}_{\mathcal{A}}^{(1)}(\lambda)| \leq 1/q$.*

Lemma 6 is proven in a similar manner to Lemma 7 in the full version of [23]. \square

Lemma 7. *For any adversary \mathcal{A} , for any security parameter λ , $\text{Adv}_{\mathcal{A}}^{(2)}(\lambda) = 0$.*

Proof. The value of b is independent from the adversary's view in Game 2. Hence, $\text{Adv}_{\mathcal{A}}^{(2)}(\lambda) = 0$. \square

5 Proposed Fully Secure Constant-Size Secret-Key ABS Scheme

We propose a *fully secure* (adaptive-predicate unforgeable and private) ABS scheme with constant-size secret-keys in Appendix E.3. Proofs of Theorems 2 and 3 are given in Appendix E.4.

Theorem 2. *The proposed ABS scheme is perfectly private.*

Theorem 3. *The proposed ABS scheme is unforgeable (adaptive-predicate unforgeable) under the DLIN assumption and the existence of collision resistant hash functions.*

6 Proof Outline of Lemma 3 (Iteration of Swapping and Conceptual Change)

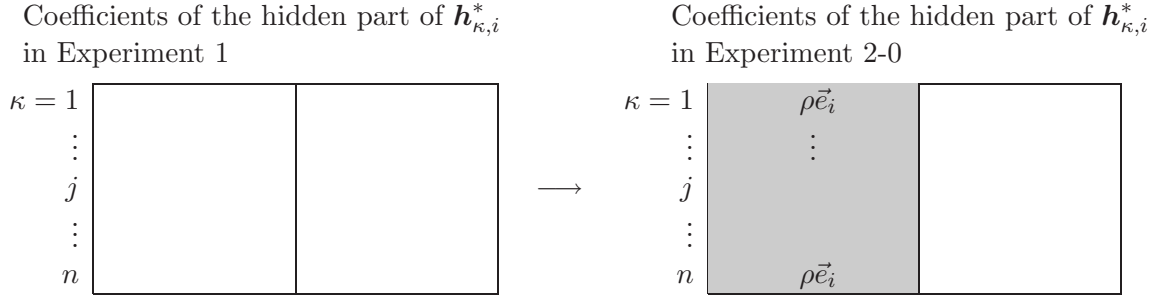
Lemma 3 is proven by the hybrid argument through $2n + 3$ experiments (Appendix B).

Experiment 0 \Rightarrow Experiment 1 \Rightarrow Experiment 2-0 \Rightarrow
for $j = 1, \dots, n$; Experiment 2- j -1 \Rightarrow Experiment 2- j -2

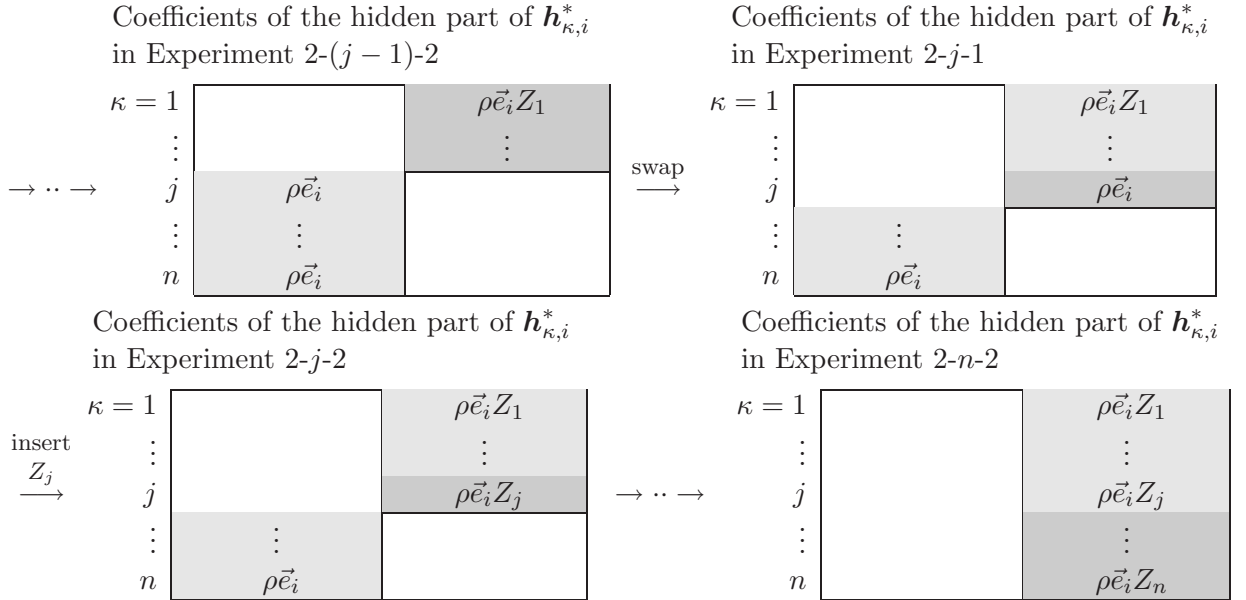
First, in a $\beta = 0$ instance of Problem 1 (Experiment 0), coefficients of the hidden parts of \mathbf{e}_1 and $\mathbf{h}_{\kappa,i}^*$ ($\kappa = 1, \dots, n$) are all zero. Then, in the next Experiment 1, that of \mathbf{e}_1 is filled with $(\tau\vec{y}, \tau\vec{y}) \in \mathbb{F}_q^{2n}$ as: (Hereafter, a blank indicates zero coefficients)

| | | |
|------------------------------------------------------------------------------------------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Coefficients of the hidden part of \mathbf{e}_1 in Experiment 0 | | Coefficients of the hidden part of \mathbf{e}_1 in Experiment 1 |
| <div style="border: 1px solid black; width: 150px; height: 20px; margin: 0 auto;"></div> | \longrightarrow | <div style="display: inline-block; background-color: #cccccc; border: 1px solid black; padding: 2px 10px;">$\tau\vec{y}$</div> <div style="display: inline-block; background-color: #cccccc; border: 1px solid black; padding: 2px 10px;">$\tau\vec{y}$</div> |

Then, in the next Experiment 2-0, the first n -dim. coefficient (block) of the hidden parts of $\mathbf{h}_{\kappa,i}^*$ ($\kappa = 1, \dots, n$) are changed to $\rho\vec{e}_i \in \mathbb{F}_q^n$ as



After that, in turn for $j = 1, \dots, n$, the coefficient vector $\rho\vec{e}_i \in \mathbb{F}_q^n$ is *swapped* to the second block of the hidden parts of $\mathbf{h}_{j,i}^*$ in Experiment 2- j -1 and the coefficient vector is *conceptually (information-theoretically) changed* to $\rho\vec{e}_i Z_j$ in Experiment 2- j -2 by a conceptual basis change. The swapping can be securely executed under the DLIN assumption. At the final Experiment 2- n -2, each $\rho\vec{e}_i Z_j$ ($j = 1, \dots, n$) is embedded in the second block of hidden parts in $\mathbf{h}_{j,i}^*$, i.e., an instance of Experiment 2- n -2 is equivalent to a $\beta = 1$ instance of Problem 1.



7 Why We Use DSE Approach for Selective Security

Previously, the DSE approach was used for achieving adaptive security, not just selective security [30, 16, 23]. From *limited* randomness in a public key of our scheme, we need the DSE approach for (selective) security from DLIN. We will explain the reason below: Okamoto-Takashima [20] obtained an efficient IPE scheme with selective security. We include the scheme description in Appendix F for reference. (A simplified, no message, version of) the IPE scheme for n -dimensional (attribute and predicate) vectors was constructed on $(N := n + 3)$ -dimensional DPVS, and the following intractable problem on the DPVS. Below, a part framed by a box indicates coefficients which are different from each other in Definitions 9 and 10.

Definition 9 (Problem in [20] (for specific \vec{e}_1)). Problem in [20] is to guess β , given $(\text{param}_n, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \mathbf{h}_{\beta,1}^*, \mathbf{e}_\beta, \{\mathbf{h}_i^*\}_{i=2,\dots,n}) \xleftarrow{R} \mathcal{G}_\beta^{\text{POT13}}(1^\lambda, n)$, where

$$\begin{aligned} \mathcal{G}_\beta^{\text{POT13}}(1^\lambda, n) : (\mathbb{B}, \mathbb{B}^*) : N\text{-dimensional random dual bases using random matrix in } GL(N, \mathbb{F}_q), \\ \widehat{\mathbb{B}} := (\mathbf{b}_1, \dots, \mathbf{b}_n, \mathbf{b}_{n+2}, \mathbf{b}_{n+3}), \quad \widehat{\mathbb{B}}^* := (\mathbf{b}_1^*, \dots, \mathbf{b}_n^*, \mathbf{b}_{n+2}^*, \mathbf{b}_{n+3}^*), \\ \delta, \omega, \varphi \xleftarrow{U} \mathbb{F}_q, \quad \tau, \rho \xleftarrow{U} \mathbb{F}_q^\times, \quad \text{for } i = 1, \dots, n; \quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \quad \delta_i \xleftarrow{U} \mathbb{F}_q, \\ \mathbf{h}_{0,1}^* := (\delta \vec{e}_1, 0, \delta_1, 0)_{\mathbb{B}^*}, \quad \mathbf{h}_{1,1}^* := (\delta \vec{e}_1, \boxed{\rho}, \delta_1, 0)_{\mathbb{B}^*}, \\ \text{for } i = 2, \dots, n; \quad \mathbf{h}_i^* := (\delta \vec{e}_i, \boxed{0}, \delta_i, 0)_{\mathbb{B}^*}, \\ \mathbf{e}_0 := (\boxed{\omega \vec{e}_1}, 0, 0, \varphi)_{\mathbb{B}}, \quad \mathbf{e}_1 := (\boxed{\omega \vec{e}_1}, \tau, 0, \varphi)_{\mathbb{B}}, \\ \text{return } (\text{param}_n, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \mathbf{h}_{\beta,1}^*, \{\mathbf{h}_i^*\}_{i=2,\dots,n}, \mathbf{e}_\beta), \end{aligned}$$

for $\beta \xleftarrow{U} \{0, 1\}$.

The intractability of the problem can be easily reduced from that of DLIN [20] since the problem is to distinguish two pairs of vector elements $(\mathbf{h}_{0,1}^*, \mathbf{e}_0)$ and $(\mathbf{h}_{1,1}^*, \mathbf{e}_1)$. For an arbitrary target vector \vec{y} in the selective security game, we consider a generalized problem below using \vec{y} instead of a specific \vec{e}_1 .

Definition 10 (Problem in [20] for general \vec{y}). Problem in [20] for general \vec{y} is to guess β , given $(\text{param}_n, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \mathbf{e}_\beta, \{\mathbf{h}_{\beta,i}^*\}_{i=1,\dots,n}) \xleftarrow{R} \mathcal{G}'_\beta^{\text{POT13}}(1^\lambda, n, \vec{y} := (y_1, \dots, y_n))$, where

$$\begin{aligned} \mathcal{G}'_\beta^{\text{POT13}}(1^\lambda, n, \vec{y} := (y_1, \dots, y_n)) : (\mathbb{B}, \mathbb{B}^*) : N\text{-dim. random dual bases using matrix in } GL(N, \mathbb{F}_q), \\ \widehat{\mathbb{B}} := (\mathbf{b}_1, \dots, \mathbf{b}_n, \mathbf{b}_{n+2}, \mathbf{b}_{n+3}), \quad \widehat{\mathbb{B}}^* := (\mathbf{b}_1^*, \dots, \mathbf{b}_n^*, \mathbf{b}_{n+2}^*, \mathbf{b}_{n+3}^*), \\ \delta, \omega, \varphi \xleftarrow{U} \mathbb{F}_q, \quad \tau, \rho \xleftarrow{U} \mathbb{F}_q^\times, \quad \text{for } i = 1, \dots, n; \quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \quad \delta_i \xleftarrow{U} \mathbb{F}_q, \\ \text{for } i = 1, \dots, n; \quad \mathbf{h}_{0,i}^* := (\delta \vec{e}_i, 0, \delta_i, 0)_{\mathbb{B}^*}, \quad \mathbf{h}_{1,i}^* := (\delta \vec{e}_i, \boxed{\rho y_i}, \delta_i, 0)_{\mathbb{B}^*}, \\ \mathbf{e}_0 := (\boxed{\omega \vec{y}}, 0, 0, \varphi)_{\mathbb{B}}, \quad \mathbf{e}_1 := (\boxed{\omega \vec{y}}, \tau, 0, \varphi)_{\mathbb{B}}, \\ \text{return } (\text{param}_n, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \{\mathbf{h}_{\beta,i}^*\}_{i=1,\dots,n}, \mathbf{e}_\beta), \end{aligned}$$

for $\beta \xleftarrow{U} \{0, 1\}$.

In [20], an instance of the problem P_{OT13} is transformed to that of P'_{OT13} for a target \vec{y} , and the transformed one is used in simulation for the selective security. For our constant-size CT KP-ABE, a sparse matrix X_1 is used for generating dual bases $(\mathbb{B}, \mathbb{B}^*)$. It turns out that the above transformation seems to be difficult in the sparse matrix setting. Also, we have no idea for directly proving the security of P'_{OT13} for arbitrary \vec{y} from that of DLIN. Thus, a straightforward extension of the approach given in [20] is useless for obtaining a constant-size CT KP-ABE scheme from the DLIN assumption.

Therefore, for proving the selective security with no transformation of a target \vec{y} into \vec{e}_1 , we adopt the DSE approach since it is suitable for amplifying randomness by a conceptual change without changing the target \vec{y} into some specific one. Moreover, since Problem 1 must use only one ciphertext component $\mathbf{e}_{\beta,1}$ for a specific target \vec{y} as explained above, two blocks in the semi-functional space are used for *piling up* multiple amplified randomness $\{Z_j\}_{j=1,\dots,n}$ for dealing with

an arbitrary attribute value v_i in a policy (M, ρ) such that $\rho(i) = v_i$ or $\rho(i) = \neg v_i$. See Section 6 for the necessity of the two blocks.

References

1. Attrapadung, N., Libert, B., de Panafieu, E.: Expressive key-policy attribute-based encryption with constant-size ciphertexts. In: Catalano et al. [6], pp. 90–108
2. Beimel, A.: Secure schemes for secret sharing and key distribution. PhD Thesis, Israel Institute of Technology, Technion, Haifa (1996)
3. Boneh, D., Boyen, X., Goh, E.J.: Hierarchical identity based encryption with constant size ciphertext. In: Cramer [8], pp. 440–456
4. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer (2004)
5. Boneh, D., Gentry, C., Waters, B.: Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Shoup, V. (ed.) CRYPTO. Lecture Notes in Computer Science, vol. 3621, pp. 258–275. Springer (2005)
6. Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.): Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings, LNCS, vol. 6571. Springer (2011)
7. Cheon, J.H.: Security analysis of the strong diffie-hellman problem. In: Vaudenay [29], pp. 1–11
8. Cramer, R. (ed.): Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings, LNCS, vol. 3494. Springer (2005)
9. Delerablée, C.: Identity-based broadcast encryption with constant size ciphertexts and private keys. In: Kurosawa, K. (ed.) ASIACRYPT. LNCS, vol. 4833, pp. 200–215. Springer (2007)
10. Emura, K., Miyaji, A., Nomura, A., Omote, K., Soshi, M.: A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. In: Bao, F., Li, H., Wang, G. (eds.) ISPEC 2009. LNCS, vol. 5451, pp. 13–23. Springer (2009)
11. Garg, S., Gentry, C., Halevi, S., Sahai, A., Waters, B.: Attribute-based encryption for circuits from multilinear maps. In: Canetti, R., Garay, J.A. (eds.) CRYPTO (2). Lecture Notes in Computer Science, vol. 8043, pp. 479–499. Springer (2013)
12. Gentry, C.: Practical identity-based encryption without random oracles. In: Vaudenay [29], pp. 445–464
13. Gorbunov, S., Vaikuntanathan, V., Wee, H.: Attribute-based encryption for circuits. In: Boneh, D., Roughgarden, T., Feigenbaum, J. (eds.) STOC. pp. 545–554. ACM (2013)
14. Herranz, J., Laguillaumie, F., Ràfols, C.: Constant size ciphertexts in threshold attribute-based encryption. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 19–34. Springer (2010)
15. Hohenberger, S., Waters, B.: Attribute-based encryption with fast decryption. In: Kurosawa, K., Hanaoka, G. (eds.) Public Key Cryptography. Lecture Notes in Computer Science, vol. 7778, pp. 162–179. Springer (2013)
16. Lewko, A.B., Waters, B.: New techniques for dual system encryption and fully secure hibe with short ciphertexts. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 455–479. Springer (2010)
17. Maji, H.K., Prabhakaran, M., Rosulek, M.: Attribute-based signatures: Achieving attribute-privacy and collusion-resistance. IACR Cryptology ePrint Archive 2008, 328 (2008)
18. Maji, H.K., Prabhakaran, M., Rosulek, M.: Attribute-based signatures. In: Kiayias, A. (ed.) CT-RSA. Lecture Notes in Computer Science, vol. 6558, pp. 376–392. Springer (2011)
19. Mitsunari, S., Sakai, R., Kasahara, M.: A new traitor tracing. IEICE Trans. Fundamentals E85-A(2), 481–484 (2002)
20. Okamoto, T., Takashima, K.: Efficient (hierarchical) inner-product encryption tightly reduced from the decisional linear assumption. IEICE Trans. Fundamentals E96-A(1), 42–52 (2013)
21. Okamoto, T., Takashima, K.: Homomorphic encryption and signatures from vector decomposition. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, vol. 5209, pp. 57–74. Springer (2008)
22. Okamoto, T., Takashima, K.: Hierarchical predicate encryption for inner-products. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 214–231. Springer (2009)
23. 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 (2010), full version is available at <http://eprint.iacr.org/2010/563>

24. Okamoto, T., Takashima, K.: Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. In: Lin, D., Tsudik, G., Wang, X. (eds.) CANS 2011. LNCS, vol. 7092, pp. 138–159. Springer (2011), full version is available at <http://eprint.iacr.org/2011/648>
25. Okamoto, T., Takashima, K.: Efficient attribute-based signatures for non-monotone predicates in the standard model. In: Catalano et al. [6], pp. 35–52, full version is available at <http://eprint.iacr.org/2011/700>
26. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer [8], pp. 457–473
27. Sakemi, Y., Hanaoka, G., Izu, T., Takenaka, M., Yasuda, M.: Solving a discrete logarithm problem with auxiliary input on a 160-bit elliptic curve. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) Public Key Cryptography. Lecture Notes in Computer Science, vol. 7293, pp. 595–608. Springer (2012)
28. Shi, E., Waters, B.: Delegating capabilities in predicate encryption systems. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfssdóttir, A., Walukiewicz, I. (eds.) ICALP (2) 2008. LNCS, vol. 5126, pp. 560–578. Springer (2008)
29. Vaudenay, S. (ed.): Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings, LNCS, vol. 4004. Springer (2006)
30. 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 (2009)

A Decisional Linear (DLIN) Assumption

Definition 11 (DLIN: Decisional Linear Assumption [4]). *The DLIN problem is to guess $\beta \in \{0, 1\}$, given $(\text{param}_{\mathbb{G}}, G, \xi G, \kappa G, \delta \xi G, \sigma \kappa G, Y_\beta) \xleftarrow{R} \mathcal{G}_\beta^{\text{DLIN}}(1^\lambda)$, where $\mathcal{G}_\beta^{\text{DLIN}}(1^\lambda) : \text{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{R} \mathcal{G}_{\text{bpg}}(1^\lambda), \kappa, \delta, \xi, \sigma \xleftarrow{U} \mathbb{F}_q, Y_0 := (\delta + \sigma)G, Y_1 \xleftarrow{U} \mathbb{G}$, return $(\text{param}_{\mathbb{G}}, G, \xi G, \kappa G, \delta \xi G, \sigma \kappa G, Y_\beta)$, for $\beta \xleftarrow{U} \{0, 1\}$. For a probabilistic machine \mathcal{E} , we define the advantage of \mathcal{E} for the DLIN problem as: $\text{Adv}_{\mathcal{E}}^{\text{DLIN}}(\lambda) := \left| \Pr \left[\mathcal{E}(1^\lambda, \varrho) \rightarrow 1 \mid \varrho \xleftarrow{R} \mathcal{G}_0^{\text{DLIN}}(1^\lambda) \right] - \Pr \left[\mathcal{E}(1^\lambda, \varrho) \rightarrow 1 \mid \varrho \xleftarrow{R} \mathcal{G}_1^{\text{DLIN}}(1^\lambda) \right] \right|$. The DLIN assumption is: For any probabilistic polynomial-time adversary \mathcal{E} , the advantage $\text{Adv}_{\mathcal{E}}^{\text{DLIN}}(\lambda)$ is negligible in λ .*

B Proof of Lemma 3 (Security of Problem 1)

B.1 Key Lemmas (on Basic Problems)

We will show Lemmas 8, 9, and 10 for the proof of Lemma 3.

Definition 12 (Basic Problem 1). *Basic Problem 1 is to guess β , given $(\text{param}_n, \{\mathbb{B}_\iota, \widehat{\mathbb{B}}_\iota^*\}_{\iota=0,1}, \{e_{\beta,i}\}_{i=0,\dots,n}) \xleftarrow{R} \mathcal{G}_\beta^{\text{BP1}}(1^\lambda, n)$, where*

$$\begin{aligned}
\mathcal{G}_\beta^{\text{BP1}}(1^\lambda, n) : & \quad (\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \mathbb{B}_1^*) \xleftarrow{R} \mathcal{G}_{\text{ob}}^{\text{KP-ABE}}(1^\lambda, 6, n), \\
\mathbb{B}_1 & := (\mathbf{b}_{1,1}, \dots, \mathbf{b}_{1,6n}) \text{ is calculated as in Eq. (1) from } \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \\
\widehat{\mathbb{B}}_0^* & := (\mathbf{b}_{0,1}^*, \mathbf{b}_{0,3}^*, \dots, \mathbf{b}_{0,5}^*), \quad \widehat{\mathbb{B}}_1^* := (\mathbf{b}_{1,1}^*, \dots, \mathbf{b}_{1,n}^*, \mathbf{b}_{1,3n+1}^*, \dots, \mathbf{b}_{1,6n}^*), \\
\omega, \tau, \varphi_\iota & \xleftarrow{U} \mathbb{F}_q \text{ for } \iota = 0, 1, \quad e_{0,0} := (\omega, 0, 0, 0, \varphi_0)_{\mathbb{B}_0}, \quad e_{1,0} := (\omega, \tau, 0, 0, \varphi_0)_{\mathbb{B}_0}, \\
& \text{for } i = 1, \dots, n; \\
& \quad \begin{array}{cccc}
\overbrace{\phantom{\omega \vec{e}_i}}^n & \overbrace{\phantom{0^{2n}}}^{2n} & \overbrace{\phantom{0^{2n}}}^{2n} & \overbrace{\phantom{\varphi_1 \vec{e}_i}}^n \\
e_{0,i} := & (\omega \vec{e}_i, & 0^{2n}, & 0^{2n}, & \varphi_1 \vec{e}_i)_{\mathbb{B}_1}, \\
e_{1,i} := & (\omega \vec{e}_i, & \tau \vec{e}_i, \tau \vec{e}_i, & 0^{2n}, & \varphi_1 \vec{e}_i)_{\mathbb{B}_1},
\end{array} \\
& \text{return } (\text{param}_n, \{\mathbb{B}_\iota, \widehat{\mathbb{B}}_\iota^*\}_{\iota=0,1}, \{e_{\beta,i}\}_{i=0,\dots,n}),
\end{aligned}$$

for $\beta \stackrel{\text{U}}{\leftarrow} \{0, 1\}$. For a probabilistic adversary \mathcal{C} , the advantage of \mathcal{C} for Basic Problem 1, $\text{Adv}_{\mathcal{C}}^{\text{BP1}}(\lambda)$, is similarly defined as in Definition 8.

Lemma 8. For any adversary \mathcal{C} , there is a probabilistic machine \mathcal{F} , whose running time is essentially the same as that of \mathcal{C} , such that for any security parameter λ , $\text{Adv}_{\mathcal{C}}^{\text{BP1}}(\lambda) \leq \text{Adv}_{\mathcal{F}}^{\text{DLIN}}(\lambda) + 5/q$.

Lemma 8 is proven in a similar manner to Lemma 4 in the full version of [24]. \square

Definition 13 (Basic Problem 2). Problem 2 is to guess β , given $(\text{param}_n, \{\widehat{\mathbb{B}}_\iota, \mathbb{B}_\iota^*\}_{\iota=0,1}, \{\mathbf{h}_{\beta,i}^*, \mathbf{e}_i\}_{i=0,\dots,n}) \stackrel{\text{R}}{\leftarrow} \mathcal{G}_{\beta}^{\text{BP2}}(1^\lambda, n)$, where

$$\begin{aligned} \mathcal{G}_{\beta}^{\text{BP2}}(1^\lambda, n) : & \quad (\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \mathbb{B}_1^*) \stackrel{\text{R}}{\leftarrow} \mathcal{G}_{\text{ob}}^{\text{KP-ABE}}(1^\lambda, 6, n), \\ & \quad \widehat{\mathbb{B}}_0 := (\mathbf{b}_{0,1}, \mathbf{b}_{0,3}, \dots, \mathbf{b}_{0,5}), \\ & \quad \widehat{\mathbb{B}}_1 := (\mathbf{b}_{1,1}, \dots, \mathbf{b}_{1,n}, \mathbf{b}_{1,3n+1}, \dots, \mathbf{b}_{1,6n}) \text{ is calculated as in Eq. (1) from } \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \\ & \quad \delta, \delta_0, \omega \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q, \quad \tau, \rho \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q^\times, \\ & \quad \mathbf{h}_{0,0}^* := (\delta, 0, 0, \delta_0, 0)_{\mathbb{B}_0^*}, \quad \mathbf{h}_{1,0}^* := (\delta, \rho, 0, \delta_0, 0)_{\mathbb{B}_0^*}, \quad \mathbf{e}_0 := (\omega, \tau, 0, 0, 0)_{\mathbb{B}_0}, \\ & \quad \text{for } i = 1, \dots, n; \quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \quad \vec{\delta}_i \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q^{2n}, \\ & \quad \mathbf{h}_{0,i}^* := \left(\underbrace{\delta \vec{e}_i}_n, \underbrace{0^{2n}}_{2n}, \underbrace{\vec{\delta}_i}_{2n}, \underbrace{0^n}_n \right)_{\mathbb{B}_1^*} \\ & \quad \mathbf{h}_{1,i}^* := \left(\delta \vec{e}_i, \rho \vec{e}_i, 0^n, \vec{\delta}_i, 0^n \right)_{\mathbb{B}_1^*} \\ & \quad \mathbf{e}_i := \left(\omega \vec{e}_i, \tau \vec{e}_i, \tau \vec{e}_i, 0^{2n}, 0^n \right)_{\mathbb{B}_1}, \\ & \quad \text{return } (\text{param}_n, \{\widehat{\mathbb{B}}_\iota, \mathbb{B}_\iota^*\}_{\iota=0,1}, \{\mathbf{h}_{\beta,i}^*, \mathbf{e}_i\}_{i=0,\dots,n}), \end{aligned}$$

for $\beta \stackrel{\text{U}}{\leftarrow} \{0, 1\}$. For a probabilistic adversary \mathcal{C} , the advantage of \mathcal{C} for Problem 2, $\text{Adv}_{\mathcal{C}}^{\text{BP2}}(\lambda)$, is similarly defined as in Definition 8.

Lemma 9. For any adversary \mathcal{C} , there is a probabilistic machine \mathcal{F} , whose running time is essentially the same as that of \mathcal{C} , such that for any security parameter λ , $\text{Adv}_{\mathcal{C}}^{\text{BP2}}(\lambda) \leq \text{Adv}_{\mathcal{F}}^{\text{DLIN}}(\lambda) + 5/q$.

Lemma 9 is proven in a similar manner to Lemma 5 in the full version of [24]. \square

Definition 14 (Basic Problem 3). Basic Problem 3 is to guess β , given $(\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbf{f}_0^*, \mathbf{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}_1^*, \{\mathbf{f}_i^*, \widetilde{\mathbf{f}}_i^*, \mathbf{h}_{\beta,i}^*, \mathbf{e}_i\}_{i=1,\dots,n}) \stackrel{\text{R}}{\leftarrow} \mathcal{G}_{\beta}^{\text{BP3}}(1^\lambda, n)$, where

$$\begin{aligned} \mathcal{G}_{\beta}^{\text{BP3}}(1^\lambda, n) : & \quad (\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \mathbb{B}_1^*) \stackrel{\text{R}}{\leftarrow} \mathcal{G}_{\text{ob}}^{\text{KP-ABE}}(1^\lambda, 6, n), \\ & \quad \widehat{\mathbb{B}}_1 := (\mathbf{b}_{1,1}, \dots, \mathbf{b}_{1,n}, \mathbf{b}_{1,3n+1}, \dots, \mathbf{b}_{1,6n}) \text{ is calculated as in Eq. (1) from } \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \\ & \quad \tau, \rho \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q^\times, \quad \mathbf{f}_0^* := \rho \mathbf{b}_{0,2}^*, \quad \mathbf{e}_0 := \tau \mathbf{b}_{0,2}, \\ & \quad \text{for } i = 1, \dots, n; \quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \quad \vec{\delta}_i \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q^{2n}, \quad \mathbf{f}_i^* := \rho \mathbf{b}_{1,n+i}^*, \quad \widetilde{\mathbf{f}}_i^* := \rho \mathbf{b}_{1,2n+i}^*, \\ & \quad \mathbf{h}_{0,i}^* := \left(\underbrace{0^n}_n, \underbrace{\rho \vec{e}_i, 0^n}_{2n}, \underbrace{\vec{\delta}_i}_{2n}, \underbrace{0^n}_n \right)_{\mathbb{B}_1^*} \\ & \quad \mathbf{h}_{1,i}^* := \left(\underbrace{0^n}_n, \underbrace{0^n, \rho \vec{e}_i}_{2n}, \underbrace{\vec{\delta}_i}_{2n}, \underbrace{0^n}_n \right)_{\mathbb{B}_1^*} \\ & \quad \mathbf{e}_i := \left(\underbrace{0^n}_n, \underbrace{\tau \vec{e}_i, \tau \vec{e}_i}_{2n}, \underbrace{0^{2n}}_{2n}, \underbrace{0^n}_n \right)_{\mathbb{B}_1}, \\ & \quad \text{return } (\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbf{f}_0^*, \mathbf{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}_1^*, \{\mathbf{f}_i^*, \widetilde{\mathbf{f}}_i^*, \mathbf{h}_{\beta,i}^*, \mathbf{e}_i\}_{i=1,\dots,n}), \end{aligned}$$

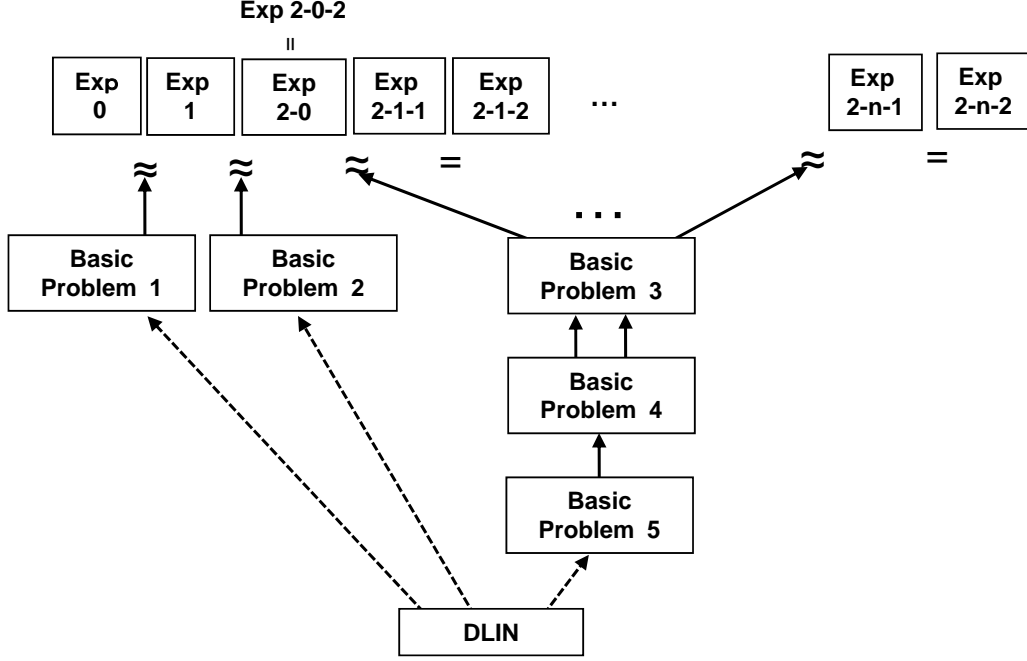


Fig. 1. Structures of Reductions for the Proof of Lemma 3.

for $\beta \xleftarrow{\text{U}} \{0, 1\}$. For a probabilistic adversary \mathcal{C} , the advantage of \mathcal{C} for Basic Problem 3, $\text{Adv}_{\mathcal{C}}^{\text{BP3}}(\lambda)$, is similarly defined as in Definition 8.

Lemma 10. For any adversary \mathcal{C} , there are probabilistic machines $\mathcal{F}_1, \mathcal{F}_2$, whose running times are essentially the same as that of \mathcal{C} , such that for any security parameter λ , $\text{Adv}_{\mathcal{C}}^{\text{BP3}}(\lambda) \leq \text{Adv}_{\mathcal{F}_1}^{\text{DLIN}}(\lambda) + \text{Adv}_{\mathcal{F}_2}^{\text{DLIN}}(\lambda) + 10/q$.

The proof of Lemma 10 is given in Appendix B.3.

B.2 Proof of Lemma 3

To prove Lemma 3, we consider the following $2n + 3$ experiments. For a probabilistic adversary \mathcal{B} , we define Experiment 0, $\text{Exp}_{\mathcal{B}}^0$, using Problem 1 generator $\mathcal{G}_0^{\text{P1}}(1^\lambda, n, \vec{y})$ in Definition 8 as follows:

1. \mathcal{B} is given $\varrho \xleftarrow{\text{R}} \mathcal{G}_0^{\text{P1}}(1^\lambda, n, \vec{y})$.
2. Output $\beta' \xleftarrow{\text{R}} \mathcal{B}(1^\lambda, \varrho)$.

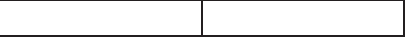
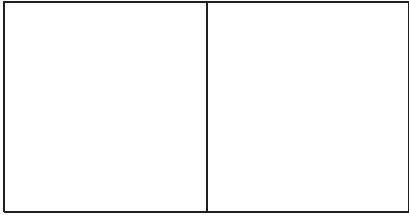
Based on Experiment 0, we define the other experiments below.

In Experiment 0, a part framed by a box indicates coefficients to be changed in a subsequent game. In the other games, a part framed by a box indicates coefficients which were changed in a game from the previous game.

Experiment 0 (Exp_B^0) : Experiment 0 is defined by using $\beta = 0$ instance of Problem 1 as above. That is, $\delta, \delta_0, \omega, \varphi_0, \varphi_1 \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q$, $\tau, \rho \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q^\times$, and

$$\begin{aligned} \mathbf{h}_0^* &:= (\delta, \boxed{0}, 0, \delta_0, 0)_{\mathbb{B}_0^*}, & \mathbf{e}_0 &:= (\omega, \boxed{0}, 0, 0, \varphi_0)_{\mathbb{B}_0}, \\ \text{for } j = 1, \dots, n; i = 1, \dots, n; & \vec{e}_i &:= (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, & \vec{\delta}_{j,i} &\stackrel{\text{U}}{\leftarrow} \mathbb{F}_q^{2n}, \\ \mathbf{h}_{j,i}^* &:= \left(\underbrace{\delta \vec{e}_i}_n, \underbrace{\boxed{0^{2n}}}_{2n}, \underbrace{\vec{\delta}_{j,i}}_{2n}, \underbrace{0^n}_n \right)_{\mathbb{B}_1^*} \\ \mathbf{e}_1 &:= \left(\underbrace{\omega \vec{y}}_n, \underbrace{\boxed{0^{2n}}}_{2n}, \underbrace{0^{2n}}_{2n}, \underbrace{\varphi_1 \vec{y}}_n \right)_{\mathbb{B}_1}, \end{aligned}$$


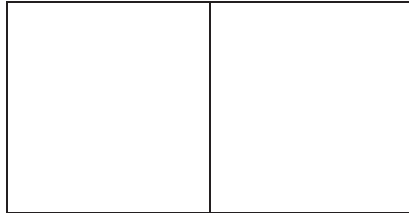
Below, we describe coefficients of the hidden part, i.e., $\text{span}\langle \mathbf{b}_{1,n+1}, \dots, \mathbf{b}_{1,3n} \rangle$ (resp. $\text{span}\langle \mathbf{b}_{1,n+1}^*, \dots, \mathbf{b}_{1,3n}^* \rangle$) of \mathbf{e}_1 (resp. $\mathbf{h}_{\kappa,i}^*$) w.r.t. these bases vectors for $\kappa = 1, \dots, n$. Non-zero coefficients are colored by light gray, and those which were changed from the previous experiment are colored by dark gray.

| | |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Coefficients of the hidden part of \mathbf{e}_1 in Experiment 0 | Coefficients of the hidden part of $\mathbf{h}_{\kappa,i}^*$ in Experiment 0 |
|  | $\kappa = 1$ \vdots j \vdots n  |

Experiment 1 (Exp_B^1) : Same as Experiment 0 except that $\mathbf{e}_0, \mathbf{e}_1$ are:

$$\mathbf{e}_0 := (\omega, \boxed{\tau}, 0, 0, \varphi_0)_{\mathbb{B}_0}, \quad \mathbf{e}_1 := \left(\underbrace{\omega \vec{y}}_n, \underbrace{\boxed{\tau \vec{y}}, \tau \vec{y}}_{2n}, \underbrace{0^{2n}}_{2n}, \underbrace{\varphi_1 \vec{y}}_n \right)_{\mathbb{B}_1},$$

where $\tau \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q$, and all the other variables are generated as in Experiment 0.

| | |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Coefficients of the hidden part of \mathbf{e}_1 in Experiment 1 | Coefficients of the hidden part of $\mathbf{h}_{\kappa,i}^*$ in Experiment 1 |
|  | $\kappa = 1$ \vdots j \vdots n  |

Experiment 2-0 (Exp_B^{2-0}) : Experiment 2-0 is the same as Experiment 1 except that $\mathbf{h}_0^*, \mathbf{h}_{j,i}^*$ are:

$$\begin{aligned} \mathbf{h}_0^* &:= (\delta, \boxed{\rho}, 0, \delta_0, 0)_{\mathbb{B}_0^*}, \\ \text{for } j = 1, \dots, n; i = 1, \dots, n; & \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, & \vec{\delta}_{j,i} &\stackrel{\text{U}}{\leftarrow} \mathbb{F}_q^{2n}, \\ \mathbf{h}_{j,i}^* &:= \left(\underbrace{\delta \vec{e}_i}_n, \underbrace{\boxed{\rho \vec{e}_i}}_{2n}, \underbrace{0^n}_{2n}, \underbrace{\vec{\delta}_{j,i}}_{2n}, \underbrace{0^n}_n \right)_{\mathbb{B}_1^*} \end{aligned}$$

where $\rho \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q$, and all the other variables are generated as in Experiment 1.

Coefficients of the hidden part of \mathbf{e}_1
in Experiment 2-0

| | |
|----------------|----------------|
| $\tau \vec{y}$ | $\tau \vec{y}$ |
|----------------|----------------|

Coefficients of the hidden part of \mathbf{e}_1
in Experiment 2-($j-1$)-2

| | |
|----------------|----------------|
| $\tau \vec{y}$ | $\tau \vec{y}$ |
|----------------|----------------|

Coefficients of the hidden part of $\mathbf{h}_{\kappa,i}^*$
in Experiment 2-0

| | | |
|--------------|------------------|--|
| $\kappa = 1$ | $\rho \vec{e}_i$ | |
| \vdots | \vdots | |
| j | | |
| \vdots | | |
| n | $\rho \vec{e}_i$ | |

Coefficients of the hidden part of $\mathbf{h}_{\kappa,i}^*$
in Experiment 2-($j-1$)-2

| | | |
|--------------|------------------|----------------------|
| $\kappa = 1$ | | $\rho \vec{e}_i Z_1$ |
| \vdots | | \vdots |
| j | $\rho \vec{e}_i$ | |
| \vdots | \vdots | |
| n | $\rho \vec{e}_i$ | |

Experiment 2- j -1 ($\text{Exp}_{\mathcal{B}}^{2-j-1}, j = 1, \dots, n$) : Experiment 2-0-2 is Experiment 2-0. Experiment 2- j -1 is the same as Experiment 2-($j-1$)-2 except the j -th component $\mathbf{h}_{j,i}^*$ are:

$$\text{for } i = 1, \dots, n; \quad \mathbf{h}_{j,i}^* := (\overbrace{\delta \vec{e}_i}^n, \overbrace{0^n, \rho \vec{e}_i}^{2n}, \overbrace{\vec{\delta}_{j,i}}^{2n}, \overbrace{0^n}^n)_{\mathbb{B}_1^*}$$

where all the variables are generated as in Game 2-($j-1$)-2.

Coefficients of the hidden part of \mathbf{e}_1
in Experiment 2- j -1

| | |
|----------------|----------------|
| $\tau \vec{y}$ | $\tau \vec{y}$ |
|----------------|----------------|

Coefficients of the hidden part of $\mathbf{h}_{\kappa,i}^*$
in Experiment 2- j -1

| | | |
|--------------|------------------|----------------------|
| $\kappa = 1$ | | $\rho \vec{e}_i Z_1$ |
| \vdots | | \vdots |
| j | | $\rho \vec{e}_i$ |
| \vdots | \vdots | |
| n | $\rho \vec{e}_i$ | |

Experiment 2- j -2 ($\text{Exp}_{\mathcal{B}}^{2-j-2}, j = 1, \dots, n$) : Experiment 2- j -2 is the same as Experiment 2- j -1 except the j -th component $\mathbf{h}_{j,i}^*$ are:

$$\text{for } i = 1, \dots, n; \quad U_j \stackrel{\text{U}}{\leftarrow} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q), \quad Z_j := (U_j^{-1})^T,$$

$$\mathbf{h}_{j,i}^* := (\overbrace{\delta \vec{e}_i}^n, \overbrace{0^n, \rho \vec{e}_i \cdot Z_j}^{2n}, \overbrace{\vec{\delta}_{j,i}}^{2n}, \overbrace{0^n}^n)_{\mathbb{B}_1^*}$$

where all the other variables are generated as in Game 2- j -1.

| | | | | | | | | | | | | | | | | | | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|--|---------------------|----------|--|----------|-----|--|---------------------|----------|--|--|-----|-----------------|--|
| <p>Coefficients of the hidden part of \mathbf{e}_1 in Experiment 2-j-2</p> <table border="1" style="margin-left: auto; margin-right: auto; border-collapse: collapse;"> <tr> <td style="padding: 5px;">$\tau\vec{y}$</td> <td style="padding: 5px;">$\tau\vec{y}$</td> </tr> </table> | $\tau\vec{y}$ | $\tau\vec{y}$ | <p>Coefficients of the hidden part of $\mathbf{h}_{\kappa,i}^*$ in Experiment 2-j-2</p> <table style="margin-left: auto; margin-right: auto;"> <tr> <td style="padding: 5px;">$\kappa = 1$</td> <td style="border: 1px solid black; padding: 5px;"></td> <td style="border: 1px solid black; padding: 5px;">$\rho\vec{e}_i Z_1$</td> </tr> <tr> <td style="padding: 5px;">\vdots</td> <td style="border: 1px solid black; padding: 5px;"></td> <td style="border: 1px solid black; padding: 5px;">\vdots</td> </tr> <tr> <td style="padding: 5px;">j</td> <td style="border: 1px solid black; padding: 5px;"></td> <td style="border: 1px solid black; padding: 5px;">$\rho\vec{e}_i Z_j$</td> </tr> <tr> <td style="padding: 5px;">\vdots</td> <td style="border: 1px solid black; padding: 5px;"></td> <td style="border: 1px solid black; padding: 5px;"></td> </tr> <tr> <td style="padding: 5px;">n</td> <td style="border: 1px solid black; padding: 5px;">$\rho\vec{e}_i$</td> <td style="border: 1px solid black; padding: 5px;"></td> </tr> </table> | $\kappa = 1$ | | $\rho\vec{e}_i Z_1$ | \vdots | | \vdots | j | | $\rho\vec{e}_i Z_j$ | \vdots | | | n | $\rho\vec{e}_i$ | |
| $\tau\vec{y}$ | $\tau\vec{y}$ | | | | | | | | | | | | | | | | | |
| $\kappa = 1$ | | $\rho\vec{e}_i Z_1$ | | | | | | | | | | | | | | | | |
| \vdots | | \vdots | | | | | | | | | | | | | | | | |
| j | | $\rho\vec{e}_i Z_j$ | | | | | | | | | | | | | | | | |
| \vdots | | | | | | | | | | | | | | | | | | |
| n | $\rho\vec{e}_i$ | | | | | | | | | | | | | | | | | |

We note that an instance of Experiment 2- n -2 is equivalent of a $\beta = 1$ instance of Problem 1.

| | | | | | | | | | | | | | | | | | | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|--|---------------------|----------|--|----------|-----|--|---------------------|----------|--|----------|-----|--|---------------------|
| <p>Coefficients of the hidden part of \mathbf{e}_1 in Experiment 2-n-2</p> <table border="1" style="margin-left: auto; margin-right: auto; border-collapse: collapse;"> <tr> <td style="padding: 5px;">$\tau\vec{y}$</td> <td style="padding: 5px;">$\tau\vec{y}$</td> </tr> </table> | $\tau\vec{y}$ | $\tau\vec{y}$ | <p>Coefficients of the hidden part of $\mathbf{h}_{\kappa,i}^*$ in Experiment 2-n-2</p> <table style="margin-left: auto; margin-right: auto;"> <tr> <td style="padding: 5px;">$\kappa = 1$</td> <td style="border: 1px solid black; padding: 5px;"></td> <td style="border: 1px solid black; padding: 5px;">$\rho\vec{e}_i Z_1$</td> </tr> <tr> <td style="padding: 5px;">\vdots</td> <td style="border: 1px solid black; padding: 5px;"></td> <td style="border: 1px solid black; padding: 5px;">\vdots</td> </tr> <tr> <td style="padding: 5px;">j</td> <td style="border: 1px solid black; padding: 5px;"></td> <td style="border: 1px solid black; padding: 5px;">$\rho\vec{e}_i Z_j$</td> </tr> <tr> <td style="padding: 5px;">\vdots</td> <td style="border: 1px solid black; padding: 5px;"></td> <td style="border: 1px solid black; padding: 5px;">\vdots</td> </tr> <tr> <td style="padding: 5px;">n</td> <td style="border: 1px solid black; padding: 5px;"></td> <td style="border: 1px solid black; padding: 5px;">$\rho\vec{e}_i Z_n$</td> </tr> </table> | $\kappa = 1$ | | $\rho\vec{e}_i Z_1$ | \vdots | | \vdots | j | | $\rho\vec{e}_i Z_j$ | \vdots | | \vdots | n | | $\rho\vec{e}_i Z_n$ |
| $\tau\vec{y}$ | $\tau\vec{y}$ | | | | | | | | | | | | | | | | | |
| $\kappa = 1$ | | $\rho\vec{e}_i Z_1$ | | | | | | | | | | | | | | | | |
| \vdots | | \vdots | | | | | | | | | | | | | | | | |
| j | | $\rho\vec{e}_i Z_j$ | | | | | | | | | | | | | | | | |
| \vdots | | \vdots | | | | | | | | | | | | | | | | |
| n | | $\rho\vec{e}_i Z_n$ | | | | | | | | | | | | | | | | |

We will show four lemmas (Lemmas 11-14) that evaluate the gaps between pairs of $\Pr[\text{Exp}_{\mathcal{B}}^0(\lambda) \rightarrow 1]$, $\Pr[\text{Exp}_{\mathcal{B}}^1(\lambda) \rightarrow 1]$, $\Pr[\text{Exp}_{\mathcal{B}}^{2-0}(\lambda) \rightarrow 1]$ and $\Pr[\text{Exp}_{\mathcal{B}}^{2-j-\iota}(\lambda) \rightarrow 1]$ for $j = 1, \dots, n$; $\iota = 1, 2$. From these lemmas and Lemmas 8–10, we obtain $\text{Adv}_{\mathcal{B}}^{\text{BP1}}(\lambda) = |\Pr[\text{Exp}_{\mathcal{B}}^0(\lambda) \rightarrow 1] - \Pr[\text{Exp}_{\mathcal{B}}^{2-n-2}(\lambda) \rightarrow 1]| \leq \text{Adv}_{\mathcal{C}_{0-1}}^{\text{BP1}}(\lambda) + \text{Adv}_{\mathcal{C}_{0-2}}^{\text{BP2}}(\lambda) + \sum_{j=1}^n \sum_{\iota=1}^2 \text{Adv}_{\mathcal{C}_{j-\iota}}^{\text{BP2}}(\lambda) \leq \sum_{j=0}^n \sum_{\iota=1}^2 \text{Adv}_{\mathcal{F}_{j,\iota}}^{\text{DLIN}}(\lambda) + (10n + 10)/q$. This completes the proof of Lemma 3. \square

Lemma 11. *For any adversary \mathcal{B} , there exists a probabilistic machine \mathcal{C}_{0-1} , whose running time is essentially the same as that of \mathcal{B} , such that for any security parameter λ , $|\Pr[\text{Exp}_{\mathcal{B}}^1(\lambda) \rightarrow 1] - \Pr[\text{Exp}_{\mathcal{B}}^0(\lambda) \rightarrow 1]| \leq \text{Adv}_{\mathcal{C}_{0-1}}^{\text{BP1}}(\lambda)$.*

Proof. \mathcal{C}_{0-1} is given a BP1 instance $(\text{param}_n, \{\mathbb{B}_\iota, \widehat{\mathbb{B}}_\iota^*\}_{\iota=0,1}, \{\mathbf{e}_{\beta,i}\}_{i=0,\dots,n})$ and a target vector \vec{y} . \mathcal{C}_{0-1} then calculates $(\text{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}_\iota^*\}_{\iota=0,1}, \mathbf{h}_0^*, \{\mathbf{h}_{j,i}^*\}_{j=1,\dots,n; i=1,\dots,n})$ in Experiment 0, and calculates $\mathbf{e}'_0 := \mathbf{e}_{\beta,0}$, $\mathbf{e}'_1 := \sum_{\iota=1}^n y_\iota \mathbf{e}_{\beta,\iota}$, sends $\varrho := (\text{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}_\iota^*\}_{\iota=0,1}, \mathbf{h}_0^*, \mathbf{e}'_0, \{\mathbf{h}_{j,i}^*\}_{j=1,\dots,n; i=1,\dots,n}, \mathbf{e}'_1)$ to \mathcal{B} . \mathcal{C}_{0-1} outputs $\beta' \in \{0, 1\}$ if \mathcal{B} outputs β' . The distribution of ϱ is equivalent to that in Experiment 0 (resp. 1) when β is 0 (resp. 1). This completes the proof of Lemma 11. \square

Lemma 12. *For any adversary \mathcal{B} , there exists a probabilistic machine \mathcal{C}_{0-2} , whose running time is essentially the same as that of \mathcal{B} , such that for any security parameter λ , $|\Pr[\text{Exp}_{\mathcal{B}}^{2-0}(\lambda) \rightarrow 1] - \Pr[\text{Exp}_{\mathcal{B}}^1(\lambda) \rightarrow 1]| \leq \text{Adv}_{\mathcal{C}_{0-2}}^{\text{BP2}}(\lambda)$.*

Proof. \mathcal{C}_{0-2} is given a BP2 instance $(\text{param}_n, \{\widehat{\mathbb{B}}_\iota, \mathbb{B}_\iota^*\}_{\iota=0,1}, \{\mathbf{h}_{\beta,i}^*, \mathbf{e}_i\}_{i=0,\dots,n})$ and a target vector \vec{y} . \mathcal{C}_{0-2} then calculates $(\text{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}_\iota^*\}_{\iota=0,1}, \mathbf{e}_0, \mathbf{e}'_1 := \sum_{\iota=1}^n y_\iota \mathbf{e}_\iota)$ in Experiment 1, and calculates $\mathbf{h}_0'^* := \mathbf{h}_{\beta,0}^*$, $\{\mathbf{h}_{j,i}^* := \mathbf{h}_{\beta,i}^* + \sum_{\iota=1}^n \delta_{j,\iota} \mathbf{b}_{1,3n+\iota}\}_{j=1,\dots,n; i=1,\dots,n}$ with $\delta_{j,\iota} \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q$, sends $\varrho := (\text{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}_\iota^*\}_{\iota=0,1}, \mathbf{h}_0'^*, \mathbf{e}_0, \{\mathbf{h}_{j,i}^*\}_{j=1,\dots,n; i=1,\dots,n}, \mathbf{e}'_1)$ to \mathcal{B} . \mathcal{C}_{0-2} outputs $\beta' \in \{0, 1\}$ if \mathcal{B} outputs β' . The distribution of ϱ is equivalent to that in Experiment 1 (resp. 2-0) when β is 0 (resp. 1). This completes the proof of Lemma 12. \square

Lemma 13. For any adversary \mathcal{B} , there exists a probabilistic machine \mathcal{C} , whose running time is essentially the same as that of \mathcal{B} , such that for any security parameter λ , $|\Pr[\text{Exp}_{\mathcal{B}}^{2-(j-1)-2}(\lambda) \rightarrow 1] - \Pr[\text{Exp}_{\mathcal{B}}^{2-j-1}(\lambda) \rightarrow 1]| \leq \text{Adv}_{\mathcal{C}_j}^{\text{BP3}}(\lambda)$, where $\mathcal{C}_j(\cdot) := \mathcal{C}(j, \cdot)$ ($j \geq 1$).

Proof. \mathcal{C} is given a BP3 instance $(\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbf{f}_0^*, \mathbf{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}_1^*, \{\mathbf{f}_i^*, \widetilde{\mathbf{f}}_i^*, \mathbf{h}_{\beta,i}^*, \mathbf{e}_i\}_{i=1,\dots,n})$, a target vector \vec{y} and an index j . \mathcal{C} then calculates $(\text{param}_n, \{\widehat{\mathbb{B}}_\ell, \widehat{\mathbb{B}}_\ell^*\}_{\ell=0,1}, \mathbf{h}_0'^* := \delta \mathbf{b}_{0,1}^* + \mathbf{f}_0^* + \delta_0 \mathbf{b}_{0,5}^*, \mathbf{e}'_0 := \omega \mathbf{b}_{0,1} + \mathbf{e}_0 + \varphi_0 \mathbf{b}_{0,5}, \mathbf{e}'_1 := \sum_{\ell=1}^n y_\ell (\omega \mathbf{b}_{1,\ell} + \mathbf{e}_\ell + \varphi_1 \mathbf{b}_{1,5n+\ell}))$ in Experiment 2-($j-1$)-2 with $\delta, \delta_0, \omega, \varphi_0, \varphi_1 \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q$, and calculates

$$\begin{aligned} & \text{if } \kappa < j; \text{ for } i = 1, \dots, n, \mathbf{h}'_{\kappa,i} := \delta \mathbf{b}_{1,i}^* + \sum_{\ell=1}^n (z_{\kappa,i,\ell} \widetilde{\mathbf{f}}_\ell^* + \delta_{\kappa,\ell} \mathbf{b}_{1,3n+\ell}^*) \\ & \quad \text{where } Z_\kappa \stackrel{\text{U}}{\leftarrow} (\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q))^{\text{T}}, (z_{\kappa,i,1}, \dots, z_{\kappa,i,n}) := \vec{e}_i \cdot Z_\kappa, \delta_{\kappa,\ell} \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q, \\ & \text{if } \kappa = j; \text{ for } i = 1, \dots, n, \mathbf{h}'_{j,i} := \delta \mathbf{b}_{1,i}^* + \mathbf{h}_{\beta,i}^* + \sum_{\ell=1}^n \delta_{j,\ell} \mathbf{b}_{1,3n+\ell}^* \text{ where } \delta_{j,\ell} \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q, \\ & \text{if } \kappa > j; \text{ for } i = 1, \dots, n, \mathbf{h}'_{\kappa,i} := \delta \mathbf{b}_{1,i}^* + \mathbf{f}_i^* + \sum_{\ell=1}^n \delta_{\kappa,\ell} \mathbf{b}_{1,3n+\ell}^* \text{ where } \delta_{\kappa,\ell} \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q, \end{aligned}$$

and sends $\varrho := (\text{param}_n, \{\widehat{\mathbb{B}}_\ell, \widehat{\mathbb{B}}_\ell^*\}_{\ell=0,1}, \mathbf{h}_0'^*, \mathbf{e}'_0, \{\mathbf{h}'_{j,i}\}_{j=1,\dots,n; i=1,\dots,n}, \mathbf{e}'_1)$ to \mathcal{B} . \mathcal{C} outputs $\beta' \in \{0, 1\}$ if \mathcal{B} outputs β' . The distribution of ϱ is equivalent to that in Experiment 2-($j-1$)-2 (resp. 2- $j-1$) when β is 0 (resp. 1). This completes the proof of Lemma 13. \square

Lemma 14. For any adversary \mathcal{B} , for any security parameter λ , $\Pr[\text{Exp}_{\mathcal{B}}^{2-j-1}(\lambda) \rightarrow 1] = \Pr[\text{Exp}_{\mathcal{B}}^{2-j-2}(\lambda) \rightarrow 1]$.

Proof. To prove Lemma 14, we will show distribution $(\text{param}_n, \{\widehat{\mathbb{B}}_\ell, \widehat{\mathbb{B}}_\ell^*\}_{\ell=0,1}, \mathbf{h}_0^*, \mathbf{e}_0, \{\mathbf{h}_{j,i}^*\}_{j=1,\dots,n; i=1,\dots,n}, \mathbf{e}_1)$ in Experiments 2- $j-1$ and 2- $j-2$ are equivalent. For that purpose, we define new subbases $\mathbf{d}_{1,2n+1}, \dots, \mathbf{d}_{1,3n}$ and $\mathbf{d}_{1,2n+1}^*, \dots, \mathbf{d}_{1,3n}^*$ of \mathbb{V}_1 as follows:

For the target vector $\vec{y} := (y_1, \dots, y_n)$, we generate $U \stackrel{\text{U}}{\leftarrow} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q)$ and $Z := (U^{-1})^{\text{T}}$. We note that $\vec{y} \cdot U = \vec{y}$. Then we set $(\mathbf{d}_{1,2n+1}, \dots, \mathbf{d}_{1,3n})^{\text{T}} := Z \cdot (\mathbf{b}_{1,2n+1}, \dots, \mathbf{b}_{1,3n})^{\text{T}}$ and $(\mathbf{d}_{1,2n+1}^*, \dots, \mathbf{d}_{1,3n}^*)^{\text{T}} := U \cdot (\mathbf{b}_{1,2n+1}^*, \dots, \mathbf{b}_{1,3n}^*)^{\text{T}}$ and

$$\begin{aligned} \mathbb{D}_1 &:= (\mathbf{b}_{1,1}, \dots, \mathbf{b}_{1,2n}, \mathbf{d}_{1,2n+1}, \dots, \mathbf{d}_{1,3n}, \mathbf{b}_{1,3n+1}, \dots, \mathbf{b}_{1,6n}), \\ \mathbb{D}_1^* &:= (\mathbf{b}_{1,1}^*, \dots, \mathbf{b}_{1,2n}^*, \mathbf{d}_{1,2n+1}^*, \dots, \mathbf{d}_{1,3n}^*, \mathbf{b}_{1,3n+1}^*, \dots, \mathbf{b}_{1,6n}^*). \end{aligned}$$

We then easily verify that \mathbb{D}_1 and \mathbb{D}_1^* are dual orthonormal, and are distributed the same as the original bases, \mathbb{B}_1 and \mathbb{B}_1^* . Keys $\{\mathbf{h}_{j,i}^*\}$ in Experiment 2- $j-1$ are expressed over bases \mathbb{B}_1^* and \mathbb{D}_1^* as follows.

$$\begin{array}{l} \text{if } \kappa < j; \text{ for } i = 1, \dots, n; \quad \mathbf{h}_{\kappa,i}^* = \left(\begin{array}{cccc} \overbrace{\delta \vec{e}_i}^n & \overbrace{0^n}^{2n} & \overbrace{\rho \vec{e}_i \cdot Z_\kappa}^{2n} & \overbrace{\vec{\delta}_{\kappa,i}}^n & \overbrace{0^n}^n \end{array} \right)_{\mathbb{B}_1^*} \\ & = \left(\begin{array}{cccc} \delta \vec{e}_i & 0^n & \rho \vec{e}_i \cdot Z_\kappa \cdot Z & \vec{\delta}_{\kappa,i} & 0^n \end{array} \right)_{\mathbb{D}_1^*}, \\ \text{if } \kappa = j; \text{ for } i = 1, \dots, n; \quad \mathbf{h}_{j,i}^* = \left(\begin{array}{cccc} \delta \vec{e}_i & 0^n & \rho \vec{e}_i & \vec{\delta}_{j,i} & 0^n \end{array} \right)_{\mathbb{B}_1^*} \\ & = \left(\begin{array}{cccc} \delta \vec{e}_i & 0^n & \rho \vec{e}_i \cdot Z & \vec{\delta}_{j,i} & 0^n \end{array} \right)_{\mathbb{D}_1^*}, \\ \text{if } \kappa > j; \text{ for } i = 1, \dots, n; \quad \mathbf{h}_{\kappa,i}^* = \left(\begin{array}{cccc} \delta \vec{e}_i & \rho \vec{e}_i & 0^n & \vec{\delta}_{\kappa,i} & 0^n \end{array} \right)_{\mathbb{B}_1^*} \\ & = \left(\begin{array}{cccc} \delta \vec{e}_i & \rho \vec{e}_i & 0^n & \vec{\delta}_{\kappa,i} & 0^n \end{array} \right)_{\mathbb{D}_1^*}, \end{array}$$

where $Z_j := Z$ and $\{Z'_\kappa := Z_\kappa \cdot Z\}_{\kappa < j}$ are independently and uniformly distributed in $(\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q))^\top$ since $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q)$ is a subgroup of $GL(n, \mathbb{F}_q)$ (Lemma 1). Since $\vec{y} \cdot U = \vec{y}$, \mathbf{e}_1 has the same representations over both \mathbb{B}_1 and \mathbb{D}_1 .

Therefore, the distribution of $(\text{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}_\iota^*\}_{\iota=0,1}, \mathbf{h}_0^*, \mathbf{e}_0, \{\mathbf{h}_{j,i}^*\}_{j=1,\dots,n; i=1,\dots,n}, \mathbf{e}_1)$ in Experiments 2- j -1 and 2- j -2 are equivalent. This completes the proof of Lemma 14. \square

B.3 Proof of Lemma 10 (Security of Basic Problem 3)

To prove Lemma 10, we use an intermediate problem, Basic Problems 4, as indicated below.

Definition 15 (Basic Problem 4). *Basic Problem 4 is to guess β , given $(\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbf{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}_1^*, \{\mathbf{h}_{\beta,i}^*, \mathbf{e}_i\}_{i=1,\dots,n}) \xleftarrow{\text{R}} \mathcal{G}_\beta^{\text{BP4}}(1^\lambda, n)$, where*

$$\begin{aligned} \mathcal{G}_\beta^{\text{BP4}}(1^\lambda, n) : & \quad (\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \mathbb{B}_1^*) \xleftarrow{\text{R}} \mathcal{G}_{\text{ob}}^{\text{KP-ABE}}(1^\lambda, 6, n), \\ & \quad \widehat{\mathbb{B}}_1 := (\mathbf{b}_{1,1}, \dots, \mathbf{b}_{1,n}, \mathbf{b}_{1,3n+1}, \dots, \mathbf{b}_{1,6n}) \text{ is calculated as in Eq. (1) from } \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \\ & \quad \tau \xleftarrow{\text{U}} \mathbb{F}_q^\times, \theta, \psi \xleftarrow{\text{U}} \mathbb{F}_q, \quad \mathbf{e}_0 := \tau \mathbf{b}_{0,2}, \\ & \quad \text{for } i = 1, \dots, n; \quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \quad \vec{\delta}_i \xleftarrow{\text{U}} \mathbb{F}_q^n, \\ & \quad \begin{array}{ccccccc} & \underbrace{\hspace{2cm}} & \underbrace{\hspace{2cm}} & \underbrace{\hspace{2cm}} & \underbrace{\hspace{2cm}} & & \\ & n & 2n & 2n & n & & \\ \mathbf{h}_{0,i}^* := & (& 0^n, & 0^{2n}, & \psi \vec{e}_i, & \vec{\delta}_i, & 0^n &)_{\mathbb{B}_1^*} \\ \mathbf{h}_{1,i}^* := & (& 0^n, & \theta \vec{e}_i, & -\theta \vec{e}_i, & \psi \vec{e}_i, & \vec{\delta}_i, & 0^n &)_{\mathbb{B}_1^*} \\ \mathbf{e}_i := & (& 0^n, & \tau \vec{e}_i, & \tau \vec{e}_i, & 0^{2n}, & 0^n &)_{\mathbb{B}_1}, \end{array} \\ & \quad \text{return } (\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbf{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}_1^*, \{\mathbf{h}_{\beta,i}^*, \mathbf{e}_i\}_{i=1,\dots,n}), \end{aligned}$$

for $\beta \xleftarrow{\text{U}} \{0, 1\}$. For a probabilistic adversary \mathcal{D} , the advantage of \mathcal{D} for Basic Problem 4, $\text{Adv}_{\mathcal{D}}^{\text{BP4}}(\lambda)$, is similarly defined as in Definition 8.

Lemma 15. *For any adversary \mathcal{C} , there are probabilistic machine \mathcal{D}_1 and \mathcal{D}_2 , whose running times are essentially the same as that of \mathcal{C} , such that for any security parameter λ , $\text{Adv}_{\mathcal{C}}^{\text{BP3}}(\lambda) \leq \text{Adv}_{\mathcal{D}_1}^{\text{BP4}}(\lambda) + \text{Adv}_{\mathcal{D}_2}^{\text{BP4}}(\lambda)$.*

Lemma 16. *For any adversary \mathcal{D} , there is a probabilistic machine \mathcal{F} , whose running time is essentially the same as that of \mathcal{D} , such that for any security parameter λ , $\text{Adv}_{\mathcal{D}}^{\text{BP4}}(\lambda) \leq \text{Adv}_{\mathcal{F}}^{\text{DLIN}}(\lambda) + 5/q$.*

From Lemmas 15 and 16, we obtain Lemma 10. \square

Below, we give proofs of Lemmas 15 and 16 in turn.

Proof of Lemma 15 To prove Lemma 15, we consider the following experiments. Problem 3 is the hybrid of the following Experiments 0, \dots , 3, i.e., $\text{Adv}_{\mathcal{C}}^{\text{BP3}}(\lambda) = |\Pr[\text{Exp}_{\mathcal{C}}^0(\lambda) \rightarrow 1] - \Pr[\text{Exp}_{\mathcal{C}}^3(\lambda) \rightarrow 1]|$.

For a probabilistic adversary \mathcal{C} , we define Experiment 0, $\text{Exp}_{\mathcal{C}}^0$, using Problem BP3 generator $\mathcal{G}_0^{\text{BP3}}(1^\lambda, n)$ in Definition 14 as follows:

1. \mathcal{C} is given $\varrho \xleftarrow{\text{R}} \mathcal{G}_0^{\text{BP3}}(1^\lambda, n)$.

2. Output $\beta' \stackrel{R}{\leftarrow} \mathcal{C}(1^\lambda, \varrho)$.

Based on Experiment 0, we define Experiments 0–3 below.

Experiment 0 (Exp_C^0): $\beta = 0$ case of Basic Problem 3. That is,

$$\text{for } i = 1, \dots, n, \quad \mathbf{h}_i^* := \left(\overbrace{0^n}^n, \overbrace{\rho \vec{e}_i, 0^n}^{2n}, \overbrace{\vec{\delta}_i}^{2n}, \overbrace{0^n}^n \right)_{\mathbb{B}_1^*}$$

where all variables are generated as in Basic Problem 3.

Experiment 1 (Exp_C^1): Same as Experiment 0 except that

$$\text{for } i = 1, \dots, n, \quad \mathbf{h}_i^* := \left(\overbrace{0^n}^n, \overbrace{(\rho + \theta) \vec{e}_i, -\theta \vec{e}_i}^{2n}, \overbrace{\vec{\delta}_i}^{2n}, \overbrace{0^n}^n \right)_{\mathbb{B}_1^*},$$

where $\theta \stackrel{U}{\leftarrow} \mathbb{F}_q$, and all the other variables are generated as in Experiment 0.

Experiment 2 (Exp_C^2): Same as Experiment 1 except that

$$\text{for } i = 1, \dots, n, \quad \mathbf{h}_i^* := \left(\overbrace{0^n}^n, \overbrace{\theta \vec{e}_i, (\rho - \theta) \vec{e}_i}^{2n}, \overbrace{\vec{\delta}_i}^{2n}, \overbrace{0^n}^n \right)_{\mathbb{B}_1^*},$$

where $\theta \stackrel{U}{\leftarrow} \mathbb{F}_q$, and all the other variables are generated as in Experiment 1.

Experiment 3 (Exp_C^3): Same as Experiment 2 except that

$$\text{for } i = 1, \dots, n, \quad \mathbf{h}_i^* := \left(\overbrace{0^n}^n, \overbrace{0^n, \rho \vec{e}_i}^{2n}, \overbrace{\vec{\delta}_i}^{2n}, \overbrace{0^n}^n \right)_{\mathbb{B}_1^*},$$

where all variables are generated as in Experiment 2.

Lemma 17. *For any adversary \mathcal{C} , there exists a probabilistic machine \mathcal{D}_1 , whose running time is essentially the same as that of \mathcal{C} , such that for any security parameter λ , $|\Pr[\text{Exp}_C^1(\lambda) \rightarrow 1] - \Pr[\text{Exp}_C^0(\lambda) \rightarrow 1]| \leq \text{Adv}_{\mathcal{D}_1}^{\text{BP4}}(\lambda)$.*

Proof. Given a BP4 instance $(\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbf{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}_1^*, \{\mathbf{h}_{\beta,i}^*, \mathbf{e}_i\}_{i=1,\dots,n})$, \mathcal{D}_1 calculates $\rho \stackrel{U}{\leftarrow} \mathbb{F}_q$, $\mathbf{f}_0^* := \rho \mathbf{b}_{0,2}^*$, for $i = 1, \dots, n$, $\mathbf{f}_i^* := \rho \mathbf{b}_{1,n+i}^*$, $\tilde{\mathbf{f}}_i^* := \rho \mathbf{b}_{1,2n+i}^*$, $\tilde{\mathbf{h}}_i^* := \mathbf{h}_{\beta,i}^* + \rho \mathbf{b}_{1,n+i}^* + \mathbf{r}^*$ where $\mathbf{r}^* \stackrel{U}{\leftarrow} \text{span}(\mathbf{b}_{1,3n+1}^*, \dots, \mathbf{b}_{1,5n}^*)$. \mathcal{D}_1 then gives $\varrho := (\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbf{f}_0^*, \mathbf{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}_1^*, \{\mathbf{f}_i^*, \tilde{\mathbf{f}}_i^*, \tilde{\mathbf{h}}_{\beta,i}^*, \mathbf{e}_i\}_{i=1,\dots,n})$ to \mathcal{C} , and outputs $\beta' \in \{0, 1\}$ if \mathcal{C} outputs β' . When $\beta = 0$ (resp. $\beta = 1$), the distribution of ϱ is exactly same as that of instances in Experiment 0 (resp. Experiment 1). This completes the proof of Lemma 17. \square

Lemma 18. *For any adversary \mathcal{C} , for any security parameter λ , $\Pr[\text{Exp}_C^2(\lambda) \rightarrow 1] = \Pr[\text{Exp}_C^1(\lambda) \rightarrow 1]$.*

Proof. Because the distributions $(\rho, \rho + \theta, -\theta)$ and $(\rho, \theta, \rho - \theta)$ with $\rho, \theta \stackrel{U}{\leftarrow} \mathbb{F}_q$ are equivalent. \square

Lemma 19. For any adversary \mathcal{C} , there exists a probabilistic machine \mathcal{D}_2 , whose running time is essentially the same as that of \mathcal{C} , such that for any security parameter λ , $|\Pr[\text{Exp}_{\mathcal{C}}^3(\lambda) \rightarrow 1] - \Pr[\text{Exp}_{\mathcal{D}_2}^2(\lambda) \rightarrow 1]| \leq \text{Adv}_{\mathcal{D}_2}^{\text{BP}^4}(\lambda)$.

Proof. Lemma 19 is proven in a similar manner to Lemma 17. \square

Proof of Lemma 16 To prove Lemma 16, we use an intermediate problem, Basic Problems 5, as indicated below.

Definition 16 (Basic Problem 5). Basic Problem 5 is to guess β , given $(\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}_1, \mathbb{B}_1^*, \{\mathbf{h}_{\beta,i}^*\}_{i=1,\dots,n}) \leftarrow^{\text{R}} \mathcal{G}_{\beta}^{\text{BP}^5}(1^\lambda, n)$, where

$$\begin{aligned} \mathcal{G}_{\beta}^{\text{BP}^5}(1^\lambda, n) : & \quad (\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \mathbb{B}_1^*) \leftarrow^{\text{R}} \mathcal{G}_{\text{ob}}^{\text{KP-ABE}}(1^\lambda, 6, n), \\ & \quad \widehat{\mathbb{B}}_1 := (\mathbf{b}_{1,1}, \dots, \mathbf{b}_{1,n}, \mathbf{b}_{1,3n+1}, \dots, \mathbf{b}_{1,6n}) \text{ is calculated as in Eq. (1) from } \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \\ & \quad \theta, \psi \leftarrow^{\text{U}} \mathbb{F}_q, \\ & \quad \text{for } i = 1, \dots, n; \quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \quad \vec{\delta}_i \leftarrow^{\text{U}} \mathbb{F}_q^n, \\ & \quad \mathbf{h}_{0,i}^* := \left(\underbrace{0^n}_n, \underbrace{0^{2n}}_{2n}, \underbrace{\psi \vec{e}_i, \vec{\delta}_i}_{2n}, \underbrace{0^n}_n \right)_{\mathbb{B}_1^*} \\ & \quad \mathbf{h}_{1,i}^* := \left(\underbrace{0^n}_n, \underbrace{\theta \vec{e}_i, 0^n}_{2n}, \underbrace{\psi \vec{e}_i, \vec{\delta}_i}_{2n}, \underbrace{0^n}_n \right)_{\mathbb{B}_1^*} \\ & \quad \text{return } (\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}_1, \mathbb{B}_1^*, \{\mathbf{h}_{\beta,i}^*\}_{i=1,\dots,n}), \end{aligned}$$

for $\beta \leftarrow^{\text{U}} \{0, 1\}$. For a probabilistic adversary \mathcal{E} , the advantage of \mathcal{E} for Basic Problem 5, $\text{Adv}_{\mathcal{E}}^{\text{BP}^5}(\lambda)$, is similarly defined as in Definition 8.

Lemma 20. For any adversary \mathcal{D} , there is a probabilistic machine \mathcal{E} , whose running time is essentially the same as that of \mathcal{D} , such that for any security parameter λ , $\text{Adv}_{\mathcal{D}}^{\text{BP}^4}(\lambda) \leq \text{Adv}_{\mathcal{E}}^{\text{BP}^5}(\lambda)$.

Proof. Given a BP5 instance $(\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}_1, \mathbb{B}_1^*, \{\mathbf{h}_{\beta,i}^*\}_{i=1,\dots,n})$, \mathcal{E} calculates $\tau \leftarrow^{\text{U}} \mathbb{F}_q$, $\mathbf{e}_0 := \tau \mathbf{b}_{0,2}$, $\mathbf{e}_i := \tau \mathbf{b}_{1,2n+i}$ for $i = 1, \dots, n$ and $\widehat{\mathbb{B}}'_1 := (\mathbf{b}_{1,1}, \dots, \mathbf{b}_{1,n}, \mathbf{b}_{1,3n+1}, \dots, \mathbf{b}_{1,6n})$.

\mathcal{E} defines new dual orthonormal bases $\mathbb{D}_1 := (\mathbf{b}_{1,1}, \dots, \mathbf{b}_{1,2n}, \mathbf{d}_{1,2n+1}, \dots, \mathbf{d}_{1,3n}, \mathbf{b}_{1,3n+1}, \dots, \mathbf{b}_{1,6n})$ and $\mathbb{D}_1^* := (\mathbf{b}_{1,1}^*, \dots, \mathbf{b}_{1,n}^*, \mathbf{d}_{1,n+1}^*, \dots, \mathbf{d}_{1,2n}^*, \mathbf{b}_{1,2n+1}^*, \dots, \mathbf{b}_{1,6n}^*)$, where $\mathbf{d}_{1,2n+i} := \mathbf{b}_{1,2n+i} - \mathbf{b}_{1,n+i}$ and $\mathbf{d}_{1,n+i}^* := \mathbf{b}_{1,n+i}^* + \mathbf{b}_{1,2n+i}^*$ for $i = 1, \dots, n$. We note that \mathbb{D}_1 is compatible with subspace $\widehat{\mathbb{B}}'_1$.

\mathcal{E} then gives $\varrho := (\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbf{e}_0, \widehat{\mathbb{B}}'_1, \mathbb{D}_1^*, \{\mathbf{h}_{\beta,i}^*, \mathbf{e}_i\}_{i=1,\dots,n})$ to \mathcal{D} , and outputs $\beta' \in \{0, 1\}$ if \mathcal{D} outputs β' .

Claim 1 When $\beta = 0$ (resp. $\beta = 1$), the distribution of ϱ is exactly same as that of instances from $\mathcal{G}_0^{\text{BP}^4}$ (resp. $\mathcal{G}_1^{\text{BP}^4}$).

Proof. $(\mathbf{h}_{0,i}^*, \mathbf{h}_{1,i}^*, \mathbf{e}_i)$ are expressed over bases $(\mathbb{B}_1, \mathbb{B}_1^*)$ and $(\mathbb{D}_1, \mathbb{D}_1^*)$ as

$$\begin{aligned} \mathbf{h}_{0,i}^* &= \left(\begin{array}{cccc} 0^n & 0^{2n} & \psi \vec{e}_i, \vec{\delta}_i & 0^n \end{array} \right)_{\mathbb{B}_1^*} = \left(\begin{array}{cccc} 0^n & 0^{2n} & \psi \vec{e}_i, \vec{\delta}_i & 0^n \end{array} \right)_{\mathbb{D}_1^*} \\ \mathbf{h}_{1,i}^* &= \left(\begin{array}{cccc} 0^n & \theta \vec{e}_i, 0^n & \psi \vec{e}_i, \vec{\delta}_i & 0^n \end{array} \right)_{\mathbb{B}_1^*} = \left(\begin{array}{cccc} 0^n & \theta \vec{e}_i, -\theta \vec{e}_i & \psi \vec{e}_i, \vec{\delta}_i & 0^n \end{array} \right)_{\mathbb{D}_1^*} \\ \mathbf{e}_i &= \left(\begin{array}{cccc} 0^n & 0^n, \tau \vec{e}_i & 0^{2n} & 0^n \end{array} \right)_{\mathbb{B}_1} = \left(\begin{array}{cccc} 0^n & \tau \vec{e}_i, \tau \vec{e}_i & 0^{2n} & 0^n \end{array} \right)_{\mathbb{D}_1}. \end{aligned}$$

This completes the proof of Claim 1. \square

2. When \mathcal{B} (or challenger) obtains challenge attributes Γ where $\Gamma := \{x_1, \dots, x_{n'}\}$ with $n' \leq n - 1$ in the first step of the game, \mathcal{B} selects (challenge) bit $b \xleftarrow{\text{U}} \{0, 1\}$. \mathcal{B} calculates $\vec{y} := (y_1, \dots, y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \cdot \prod_{j=1}^{n'} (z - x_j)$, and \mathcal{B} is given a Problem 1 instance, $(\text{param}_n, \{\widehat{\mathbb{B}}_\ell, \widehat{\mathbb{B}}_\ell^*\}_{\ell=0,1}, \mathbf{h}_{\beta,0}^*, \mathbf{e}_{\beta,0}, \{\mathbf{h}_{\beta,j,i}^*\}_{j=1,\dots,n; i=1,\dots,n}, \mathbf{e}_{\beta,1}) \xleftarrow{\text{R}} \mathcal{G}_\beta^{\text{P1}}(1^\lambda, n, \vec{y})$. \mathcal{B} provides \mathcal{A} a public key $\text{pk} := (1^\lambda, \text{param}_n, \{\widehat{\mathbb{B}}_\ell^*\}_{\ell=0,1})$ of Game 0 (and 1), where $\widehat{\mathbb{B}}_0 := (\mathbf{b}_{0,1}, \mathbf{b}_{0,3}, \mathbf{b}_{0,5})$ and $\widehat{\mathbb{B}}_1 := (\mathbf{b}_{1,1}, \dots, \mathbf{b}_{1,n}, \mathbf{b}_{1,5n+1}, \dots, \mathbf{b}_{1,6n})$, that are obtained from the Problem 1 instance.
3. When the h -th key query is issued for access structure $\mathbb{S} := (M, \rho)$, \mathcal{B} answers as follows ($h = 1, \dots, \nu$): \mathcal{B} generates $\vec{f}, \vec{g} \xleftarrow{\text{U}} \mathbb{F}_q^r, (s_1, \dots, s_\ell)^\text{T} := M \cdot \vec{f}^\text{T}, (r_1, \dots, r_\ell)^\text{T} := M \cdot \vec{g}^\text{T}, s_0 := \vec{1} \cdot \vec{f}^\text{T}, r_0 := \vec{1} \cdot \vec{g}^\text{T}, (\xi_i)_{i=1,\dots,n} \xleftarrow{\text{U}} \{(\xi_i)_{i=1,\dots,n} \in \mathbb{F}_q^n \mid \sum_{i=1}^n \xi_i = 1\}$, and calculates $\mathbf{k}_0^* := -s_0 \mathbf{b}_{0,0}^* - r_0 \mathbf{h}_{\beta,0}^*, \mathbf{k}_i^* := \sum_{\ell=1,\dots,n} (v'_{i,\ell} \mathbf{b}_{1,\ell}^* + v'_{i,\ell} (\sum_{j=1}^n \xi_j \mathbf{h}_{\beta,j,\ell}^*))$ where $\vec{v}_i := (v_i^{n-1}, \dots, v_i, 1), \vec{v}'_i := (v'_{i,\ell})_{\ell=1,\dots,n} := s_i \vec{e}_1 + \theta_i \vec{v}_i$ if $\rho(i) = v_i$ and $\vec{v}'_i := (v'_{i,\ell})_{\ell=1,\dots,n} := s_i \vec{v}_i$ if $\rho(i) = \neg v_i$, and $\vec{v}''_i := (v''_{i,\ell})_{\ell=1,\dots,n} := r_i \vec{e}_1 + \psi_i \vec{v}_i$ if $\rho(i) = v_i$ and $\vec{v}''_i := (v''_{i,\ell})_{\ell=1,\dots,n} := r_i \vec{v}_i$ if $\rho(i) = \neg v_i$. \mathcal{B} send the generated key $\text{sk}_\mathbb{S} := (\mathbb{S}, \mathbf{k}_0^*, \mathbf{k}_1^*, \dots, \mathbf{k}_\ell^*)$ to \mathcal{A} .
4. When \mathcal{B} receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ from \mathcal{A} , \mathcal{B} computes the challenge ciphertext $\text{ct}_\Gamma := (\Gamma, \mathbf{c}_0 := \mathbf{e}_{\beta,0} + \zeta \mathbf{b}_{0,3}, \mathbf{c}_1 := \mathbf{e}_{\beta,0}, \mathbf{c}_3 := \mathbf{g}_T^\zeta m^{(b)})$ where $\zeta \xleftarrow{\text{U}} \mathbb{F}_q$, and $\{\mathbf{e}_{\beta,\ell}\}_{\ell=0,1}, \mathbf{b}_{0,3}$ is a part of the Problem 1 instance.
5. When a key query is issued by \mathcal{A} after the encryption query, \mathcal{B} executes the same procedure as that of step 3.
6. \mathcal{A} finally outputs bit b' . If $b = b'$, \mathcal{B} outputs $\beta' := 1$. Otherwise, \mathcal{B} outputs $\beta' := 0$.

Claim 2 *If $\beta = 0$ (resp. $\beta = 1$), the distribution of ct_Γ and $\text{sk}_\mathbb{S}$ generated in steps 4 and 3, 5 is the same as that in Game 0 (resp. Game 1 except with probability $(\nu\ell + 1)/q$).*

Proof of Claim 2. When $\beta = 0$, it is clear that the distribution of ct_Γ and $\text{sk}_\mathbb{S}$ generated in steps 4 and 3, 5 is the same as that in Game 0.

When $\beta = 1$, let $\tilde{\mathbf{h}}_{1,\ell}^{*(h)} := \sum_{j=1}^n \xi_j \mathbf{h}_{1,j,\ell}^*$ for the h -th key query in step 3. We remark that since $\{\xi_j\}$ are freshly random for each key query and $\sum_{j=1}^n \xi_j = 1$, $\{\tilde{\mathbf{h}}_{1,\ell}^{*(h)}\}$ have a freshly random sparse matrix $Z^{(h)} := \sum_{j=1}^n \xi_j Z_j$ in the hidden subspace. We note that $\{Z_j\}_{j=1,\dots,n}$ (given by $\{\vec{u}'_j := (u'_{j,1}, \dots, u'_{j,n})\}_{j=1,\dots,n}$) forms a basis of $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^\text{T}$ except that the determinant of $(u'_{j,2}, \dots, u'_{j,n})_{j=1,\dots,n-1}$ are nonzero, i.e., except for probability $1/q$. At that time, $Z^{(h)}$ is in $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^\text{T} \cap GL(n, \mathbb{F}_q)$ except for probability $1/q$ for each $h = 1, \dots, \nu\ell$.

Let $\vec{v}_i^{''(h)} := r_i^{(h)} \vec{e}_1 + \psi_i^{(h)} \vec{v}_i^{(h)}$ if $\rho(i) = v_i$ and $\vec{v}_i^{''(h)} := r_i^{(h)} \vec{v}_i^{(h)}$ if $\rho(i) = \neg v_i$ for $h = 1, \dots, \nu; i = 1, \dots, \ell$. From Lemma 4, $\{\vec{v}_i^{''(h)} Z^{(h)}\}_{h=1,\dots,\nu; i=1,\dots,\ell}$ are uniformly and independently distributed in $W_{\vec{y}, \vec{y} \cdot \vec{v}_i^{''(h)}}$.

Claim 2 is proven in a similar manner to Claim 1 in [23]. In the above simulation, coefficients in semi-functional part of a queried key $\{\mathbf{k}_i^*\}_{i=1,\dots,\ell}$ are given as $\vec{w}_i \xleftarrow{\text{U}} \{\vec{w}_i | \vec{w}_i \cdot \vec{y} = (r_i \vec{e}_1 + \tilde{\psi}_i \vec{v}_i) \cdot \vec{y}\}$ if $\rho(i) = v_i$, $\vec{w}_i \xleftarrow{\text{U}} \{\vec{w}_i | \vec{w}_i \cdot \vec{y} = r_i \vec{v}_i \cdot \vec{y}\}$ if $\rho(i) = \neg v_i$. Therefore, if $\rho(i) = v_i \wedge \vec{y} \cdot \vec{v}_i \neq 0$, \vec{w}_i is uniformly distributed in \mathbb{F}_q^n , and if $\rho(i) = \neg v_i \wedge \vec{y} \cdot \vec{v}_i = 0$, $\vec{w}_i \xleftarrow{\text{U}} \{\vec{w}_i | \vec{w}_i \cdot \vec{y} = 0\}$. Then, r_i obtained from the other indexes i are independent from a central secret r_0 . From this independence, the above distribution with $\beta = 0$ (resp. $\beta = 1$) is the same as that in Game 0 (resp. Game 1). This completes the proof of Claim 2. \square

From Claim 2, when $\beta = 0$ (resp. $\beta = 1$), the view of \mathcal{A} is equivalent to that in Game 0 (resp. 1). This completes the proof of Lemma 5. \square

E Proposed Fully Secure Constant-Size Secret-Key ABS Scheme

E.1 Attribute-Based Signatures

Definition 17 (Attribute-Based Signatures : ABS). *An attribute-based signature scheme consists of four algorithms.*

Setup *This is a randomized algorithm that takes as input security parameter and a bound on the number of attributes per ciphertext n . It outputs public parameters pk and master key sk .*

KeyGen *This is a randomized algorithm that takes as input a set of attributes, $\Gamma := \{x_j\}_{1 \leq j \leq n'}$, pk and sk . It outputs signature generation key sk_Γ .*

Sig *This is a randomized algorithm that takes as input message m , access structure $\mathbb{S} := (M, \rho)$, signature generation key sk_Γ , and public parameters pk such that \mathbb{S} accepts Γ . It outputs signature σ .*

Ver *This takes as input message m , access structure \mathbb{S} , signature σ and public parameters pk . It outputs boolean value $\text{accept} := 1$ or $\text{reject} := 0$.*

An ABS scheme should have the following correctness property: for all $(\text{sk}, \text{pk}) \xleftarrow{\text{R}} \text{Setup}(1^\lambda, n)$, all messages m , all attribute sets Γ , all signing keys $\text{sk}_\Gamma \xleftarrow{\text{R}} \text{KeyGen}(\text{pk}, \text{sk}, \Gamma)$, all access structures \mathbb{S} such that \mathbb{S} accepts Γ , and all signatures $\sigma \xleftarrow{\text{R}} \text{Sig}(\text{pk}, \text{sk}_\Gamma, m, \mathbb{S})$, it holds that $\text{Ver}(\text{pk}, m, \mathbb{S}, \sigma) = 1$ with probability 1.

Definition 18 (Perfect Privacy). *An ABS scheme is perfectly private, if, for all $(\text{sk}, \text{pk}) \xleftarrow{\text{R}} \text{Setup}(1^\lambda, n)$, all messages m , all attribute sets Γ_1 and Γ_2 , all signing keys $\text{sk}_{\Gamma_1} \xleftarrow{\text{R}} \text{KeyGen}(\text{pk}, \text{sk}, \Gamma_1)$ and $\text{sk}_{\Gamma_2} \xleftarrow{\text{R}} \text{KeyGen}(\text{pk}, \text{sk}, \Gamma_2)$, all access structures \mathbb{S} such that \mathbb{S} accepts Γ_1 and \mathbb{S} accepts Γ_2 , distributions $\text{Sig}(\text{pk}, \text{sk}_{\Gamma_1}, m, \mathbb{S})$ and $\text{Sig}(\text{pk}, \text{sk}_{\Gamma_2}, m, \mathbb{S})$ are equal.*

For an ABS scheme with perfect privacy, we define algorithm $\text{AltSig}(\text{pk}, \text{sk}, m, \mathbb{S})$ with \mathbb{S} and master key sk instead of Γ and sk_Γ : First, generate $\text{sk}_\Gamma \xleftarrow{\text{R}} \text{KeyGen}(\text{pk}, \text{sk}, \Gamma)$ for arbitrary Γ which satisfies \mathbb{S} , then $\sigma \xleftarrow{\text{R}} \text{Sig}(\text{pk}, \text{sk}_\Gamma, m, \mathbb{S})$. return σ .

Since the correct distribution on signatures can be perfectly simulated without taking any private information as input, signatures must not leak any such private information of the signer.

Definition 19 (Unforgeability). *For an adversary, \mathcal{A} , we define $\text{Adv}_{\mathcal{A}}^{\text{ABS}, \text{UF}}(\lambda)$ to be the success probability in the following experiment for any security parameter λ . An ABS scheme is existentially unforgeable if the success probability of any polynomial-time adversary is negligible:*

1. Run $(\text{sk}, \text{pk}) \xleftarrow{\text{R}} \text{Setup}(1^\lambda, n)$ and give pk to the adversary.
2. \mathcal{A} may adaptively makes a polynomial number of queries of the following type:
 - [Create key] \mathcal{A} asks the challenger to create a signing key for an attribute set Γ . The challenger creates a key for Γ without giving it to \mathcal{A} .
 - [Create signature] \mathcal{A} specifies a key for predicate Γ that has already been created, and asks the challenger to perform a signing operation to create a signature for a message m and an access structure \mathbb{S} that accepts Γ . The challenger computes the signature without giving it to the adversary.
 - [Reveal key or signature] \mathcal{A} asks the challenger to reveal an already-created key for an attribute set Γ , or an already-created signature for an access structure \mathbb{S} .

Note that when key or signature creation requests are made, \mathcal{A} does not automatically see the created key or signature. \mathcal{A} sees it only when it makes a reveal query.

3. At the end, the adversary outputs $(m', \mathbb{S}', \sigma')$.

We say the adversary succeeds if a correctly-created signature for (m', \mathbb{S}') was never revealed to the adversary, \mathbb{S}' does not accept any Γ queried to the create key and reveal (key) oracles, and $\text{Ver}(\text{pk}, m', \mathbb{S}', \sigma') = 1$.

Remark 2 Since a signing query in the unforgeability definition in [18, 25] is made only with an access structure \mathbb{S} , the challenger should *find* an attribute set Γ that satisfies \mathbb{S} , and generate a key sk_Γ with Γ and a signature with \mathbb{S} using $(\Gamma, \text{sk}_\Gamma)$. In general, however, the challenger may not always find a suitable Γ from \mathbb{S} in a polynomial time since it includes the problem of solving the satisfiability for any DNF and CNF formulas with polynomial sizes. In this sense, the definition of unforgeability in [18, 25] is problematic.

To address this issue, our definition of unforgeability introduces four types of queries, create and reveal queries for keys and signatures, in a manner similar to the security definition for key-delegation by Shi and Waters [28]. Here, to obtain a signature for \mathbb{S} from the challenger, the adversary is required to give an attribute set Γ that satisfies \mathbb{S} to the challenger in advance (i.e., the challenger has no need to find a suitable Γ by itself.)

E.2 Building Blocks for the Proposed ABS

Dual Orthonormal Basis Generator We describe random dual orthonormal basis generator $\mathcal{G}_{\text{ob}}^{\text{ABS}}$ below, which is used as a subroutine in the proposed ABS scheme.

$$\begin{aligned}
\mathcal{G}_{\text{ob}}^{\text{ABS}}(1^\lambda, 6, n) : \quad & \text{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathbb{R}} \mathcal{G}_{\text{bpg}}(1^\lambda), \quad N_0 := 4, \quad N_1 := 6n, \quad N_2 := 7, \\
& \text{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\text{dpvs}}(1^\lambda, N_t, \text{param}_{\mathbb{G}}) \quad \text{for } t = 0, 1, 2, \\
& \psi \xleftarrow{\mathbb{U}} \mathbb{F}_q^\times, \quad g_T := e(G, G)^\psi, \quad \text{param}_n := (\{\text{param}_{\mathbb{V}_t}\}_{t=0,1}, g_T), \\
& X_t := (\chi_{t,i,j})_{i,j=1,\dots,N_t} \xleftarrow{\mathbb{U}} GL(N_t, \mathbb{F}_q) \quad \text{for } t = 0, 2, \quad X_1 \xleftarrow{\mathbb{U}} \mathcal{L}(6, n, \mathbb{F}_q), \quad \text{hereafter,} \\
& \{\mu_{i,j}, \mu'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n} \text{ denotes non-zero entries of } X_1 \text{ as in Eq. (3),} \\
& \mathbf{b}_{t,i}^* := (\chi_{t,i,1}, \dots, \chi_{t,i,N_t})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \chi_{t,i,j} \mathbf{a}_j \quad \text{for } i = 1, \dots, N_t, \quad \mathbb{B}_t^* := (\mathbf{b}_{t,1}^*, \dots, \mathbf{b}_{t,N_t}^*) \quad \text{for } t = 0, 2, \\
& B_{i,j}^* := \mu_{i,j} G, \quad B'_{i,j,l} := \mu'_{i,j,l} G \quad \text{for } i, j = 1, \dots, 6; l = 1, \dots, n, \\
& \text{for } t = 0, 1, 2, \quad (\vartheta_{t,i,j})_{i,j=1,\dots,N_t} := \psi \cdot (X_t^T)^{-1}, \\
& \mathbf{b}_{t,i} := (\vartheta_{t,i,1}, \dots, \vartheta_{t,i,N_t})_{\mathbb{A}} = \sum_{j=1}^{N_t} \vartheta_{t,i,j} \mathbf{a}_j \quad \text{for } i = 1, \dots, N_t, \quad \mathbb{B}_t := (\mathbf{b}_{t,1}, \dots, \mathbf{b}_{t,N_t}), \\
& \text{return } (\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1, \{B_{i,j}^*, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \mathbb{B}_2, \mathbb{B}_2^*).
\end{aligned}$$

Remark 3 From Remark 1, $\{B_{i,j}^*, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}$ is identified with basis $\mathbb{B}_1^* := (\mathbf{b}_{1,1}^*, \dots, \mathbf{b}_{1,6n}^*)$ dual to \mathbb{B}_1 .

Collision Resistant (CR) Hash Functions Let $\lambda \in \mathbb{N}$ be a security parameter. A collision resistant (CR) hash function family, \mathbb{H} , associated with \mathcal{G}_{bpg} and a polynomial, $\text{poly}(\cdot)$, specifies two items:

- A family of key spaces indexed by λ . Each such key space is a probability space on bit strings denoted by KH_λ . There must exist a probabilistic polynomial-time algorithm whose output distribution on input 1^λ is equal to KH_λ .
- A family of hash functions indexed by λ , $\text{hk} \stackrel{\text{R}}{\leftarrow} \text{KH}_\lambda$ and $\text{D} := \{0, 1\}^{\text{poly}(\lambda)}$. Each such hash function $\text{H}_{\text{hk}}^{\lambda, \text{D}}$ maps an element of D to an element of \mathbb{F}_q^\times with q that is the first element of output $\text{param}_{\mathbb{G}}$ of $\mathcal{G}_{\text{bpg}}(1^\lambda)$. There must exist a deterministic polynomial-time algorithm that on input 1^λ , hk and $\varrho \in \text{D}$, outputs $\text{H}_{\text{hk}}^{\lambda, \text{D}}(\varrho)$.

Let \mathcal{F} be a probabilistic polynomial-time machine. For all λ , we define $\text{Adv}_{\mathcal{F}}^{\text{H}, \text{CR}}(\lambda) := \Pr[(\varrho_1, \varrho_2) \in \text{D}^2 \wedge \varrho_1 \neq \varrho_2 \wedge \text{H}_{\text{hk}}^{\lambda, \text{D}}(\varrho_1) = \text{H}_{\text{hk}}^{\lambda, \text{D}}(\varrho_2)]$, where $\text{D} := \{0, 1\}^{\text{poly}(\lambda)}$, $\text{hk} \stackrel{\text{R}}{\leftarrow} \text{KH}_\lambda$, and $(\varrho_1, \varrho_2) \stackrel{\text{R}}{\leftarrow} \mathcal{F}(1^\lambda, \text{hk}, \text{D})$. H is a collision resistant (CR) hash function family if for any probabilistic polynomial-time adversary \mathcal{F} , $\text{Adv}_{\mathcal{F}}^{\text{H}, \text{CR}}(\lambda)$ is negligible in λ .

E.3 Construction

Setup($1^\lambda, n$): $\text{hk} \stackrel{\text{R}}{\leftarrow} \text{KH}_\lambda$,

$(\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1, \{B_{i,j}^*, B_{i,j,l}^*\}_{i,j=1,\dots,6;l=1,\dots,n}, \mathbb{B}_2, \mathbb{B}_2^*) \stackrel{\text{R}}{\leftarrow} \mathcal{G}_{\text{ob}}^{\text{ABS}}(1^\lambda, 6, n)$,

$\widehat{\mathbb{B}}_0 := (\mathbf{b}_{0,1}, \mathbf{b}_{0,4})$, $\widehat{\mathbb{B}}_1 := (\mathbf{b}_{1,1}, \dots, \mathbf{b}_{1,n}, \mathbf{b}_{1,4n+1}, \dots, \mathbf{b}_{1,6n})$, $\widehat{\mathbb{B}}_2 := (\mathbf{b}_{2,1}, \mathbf{b}_{2,2}, \mathbf{b}_{2,7})$,

$\widehat{\mathbb{B}}_1^* := (\mathbf{b}_{1,1}^*, \dots, \mathbf{b}_{1,n}^*, \mathbf{b}_{1,3n+1}^*, \dots, \mathbf{b}_{1,4n}^*) = \{B_{i,j}^*, B_{i,j,l}^*\}_{i=1,4;j=1,\dots,6;l=1,\dots,n}$,

$\widehat{\mathbb{B}}_2^* := (\mathbf{b}_{2,1}^*, \mathbf{b}_{2,2}^*, \mathbf{b}_{2,5}^*, \mathbf{b}_{2,6}^*)$,

return $\text{sk} := \mathbf{b}_{0,1}^*$, $\text{pk} := (1^\lambda, \text{hk}, \text{param}_n, \{\widehat{\mathbb{B}}_t\}_{t=0,1,2}, \{\widehat{\mathbb{B}}_t^*\}_{t=1,2}, \mathbf{b}_{0,3}^*)$.

KeyGen($\text{pk}, \text{sk}, \Gamma := \{x_1, \dots, x_{n'} \mid x_j \in \mathbb{F}_q^\times\}$):

$\omega, \varphi_0, \varphi_1 \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q$, $\vec{y} := (y_1, \dots, y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \cdot \prod_{j=1}^{n'} (z - x_j)$,

$\mathbf{k}_0^* := (\omega, 0, \varphi_0, 0)_{\mathbb{B}_0^*}$,

$L_{1,j}^* := \omega B_{1,j}^* + \varphi_1 B_{4,j}^*$, $L_{2,j}^* := \sum_{l=1}^n y_l (\omega B_{1,j,l}^* + \varphi_1 B_{4,j,l}^*)$ for $j = 1, \dots, 6$,

$\mathbf{k}_{2,1}^* := (\omega(1, 0), 0, 0, \varphi_{2,1,1}, \varphi_{2,1,2}, 0)_{\mathbb{B}_2^*}$, $\mathbf{k}_{2,2}^* := (\omega(0, 1), 0, 0, \varphi_{2,2,1}, \varphi_{2,2,2}, 0)_{\mathbb{B}_2^*}$,

return $\text{sk}_\Gamma := (\Gamma, \mathbf{k}_0^*, \{L_{1,j}^*, L_{2,j}^*\}_{j=1,\dots,6}, \{\mathbf{k}_{2,t}^*\}_{t=1,2})$.

Remark From $\{L_{1,j}^*, L_{2,j}^*\}_{j=1,\dots,6}$ and \vec{y} , \mathbf{k}_1^* is defined as

$$\mathbf{k}_1^* := (\overbrace{y_1 L_{1,1}^*, \dots, y_{n-1} L_{1,1}^*, L_{2,1}^*}^n, \overbrace{y_1 L_{1,2}^*, \dots, y_{n-1} L_{1,2}^*, L_{2,2}^*, \dots}^n, \dots, \underbrace{y_1 L_{1,5}^*, \dots, y_{n-1} L_{1,5}^*, L_{2,5}^*}_n, \underbrace{y_1 L_{1,6}^*, \dots, y_{n-1} L_{1,6}^*, L_{2,6}^*}_n)$$

$$\text{that is, } \mathbf{k}_1^* = (\underbrace{\omega \vec{y}}_n, \underbrace{0^{2n}}_{2n}, \underbrace{\varphi_1 \vec{y}}_n, \underbrace{0^{2n}}_{2n})_{\mathbb{B}_1^*},$$

Sig($\text{pk}, \text{sk}_\Gamma, m, \mathbb{S} := (M, \rho)$): If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{x_j\}_{j=1,\dots,n'}$,

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

I and $\{\alpha_i\}_{i \in I}$ such that $\sum_{i \in I} \alpha_i M_i = \vec{1}$, and

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

$\xi \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q^\times$, $(\beta_i) \stackrel{\text{U}}{\leftarrow} \{(\beta_1, \dots, \beta_\ell) \mid \sum_{i=1}^\ell \beta_i M_i = \vec{0}\}$,

$\mathbf{s}_0^* := \xi \mathbf{k}_0^* + \mathbf{r}_0^*$, where $\mathbf{r}_0^* \leftarrow^{\text{U}} \text{span}\langle \mathbf{b}_{0,3}^* \rangle$,
 $\mathbf{s}_i^* := \gamma_i \cdot \xi \mathbf{k}_1^* + \sum_{\iota=1}^n w_{i,\iota} \cdot \mathbf{b}_{i,\iota}^* + \mathbf{r}_i^*$, $\vec{v}_i := (v_i^{n-1}, \dots, v_i, 1)$ for $i = 1, \dots, \ell$,
 where $\mathbf{r}_i^* \leftarrow^{\text{U}} \text{span}\langle \mathbf{b}_{1,3n+1}^*, \dots, \mathbf{b}_{1,4n}^* \rangle$, and $\gamma_i, \vec{u}_i := (u_{i,1}, \dots, u_{i,n})$ are defined as
 if $i \in I \wedge \rho(i) = v_i$, $\gamma_i := \alpha_i$, $\vec{u}_i \leftarrow^{\text{U}} \{\vec{u}_i \mid \vec{u}_i \cdot \vec{v}_i = 0 \wedge u_{i,1} = \beta_i\}$,
 if $i \in I \wedge \rho(i) = \neg v_i$, $\gamma_i := \alpha_i / (\vec{v}_i \cdot \vec{y})$, $\vec{u}_i \leftarrow^{\text{U}} \{\vec{u}_i \mid \vec{u}_i \cdot \vec{v}_i = \beta_i\}$,
 if $i \notin I \wedge \rho(i) = v_i$, $\gamma_i := 0$, $\vec{u}_i \leftarrow^{\text{U}} \{\vec{u}_i \mid \vec{u}_i \cdot \vec{v}_i = 0 \wedge u_{i,1} = \beta_i\}$,
 if $i \notin I \wedge \rho(i) = \neg v_i$, $\gamma_i := 0$, $\vec{u}_i \leftarrow^{\text{U}} \{\vec{u}_i \mid \vec{u}_i \cdot \vec{v}_i = \beta_i\}$,
 $\mathbf{s}_{\ell+1}^* := \xi(\mathbf{k}_{2,1}^* + \mathbf{H}_{\text{hk}}^{\lambda, \text{D}}(m \parallel \mathbb{S}) \cdot \mathbf{k}_{2,2}^*) + \mathbf{r}_{\ell+1}^*$, where $\mathbf{r}_{\ell+1}^* \leftarrow^{\text{U}} \text{span}\langle \mathbf{b}_{2,5}^*, \mathbf{b}_{2,6}^* \rangle$,
 return $\vec{\mathbf{s}}^* := (\mathbf{s}_0^*, \dots, \mathbf{s}_{\ell+1}^*)$.

$\text{Ver}(\text{pk}, m, \mathbb{S} := (M, \rho), \vec{\mathbf{s}}^*) : \vec{f} \leftarrow^{\text{R}} \mathbb{F}_q^r$, $\vec{s}^{\text{T}} := (s_1, \dots, s_\ell)^{\text{T}} := M \cdot \vec{f}^{\text{T}}$,
 $s_0 := \vec{1} \cdot \vec{f}^{\text{T}}$, $\eta_0, \eta_{\ell+1}, \theta_{\ell+1}, s_{\ell+1} \leftarrow^{\text{U}} \mathbb{F}_q$, $\mathbf{c}_0 := (-s_0 - s_{\ell+1}, 0, 0, \eta_0)_{\mathbb{B}_0}$,
 for $1 \leq i \leq \ell$, $\vec{v}_i := (v_i^{n-1}, \dots, v_i, 1)$, $\vec{e}_1 := (1, 0, \dots, 0)$,
 if $\rho(i) = v_i$, return 0 if $\mathbf{s}_i^* \notin \mathbb{V}_1$, else $\theta_i \leftarrow^{\text{U}} \mathbb{F}_q$, $\vec{\eta}_i \leftarrow^{\text{U}} \mathbb{F}_q^{2n}$,
 $\mathbf{c}_i := (\underbrace{\hspace{1.5cm}}_n s_i \vec{e}_1 + \theta_i \vec{v}_i, \underbrace{\hspace{1.5cm}}_{2n} 0^{2n}, \underbrace{\hspace{1.5cm}}_n 0^n, \underbrace{\hspace{1.5cm}}_{2n} \vec{\eta}_i)_{\mathbb{B}_1}$,

if $\rho(i) = \neg v_i$, return 0 if $\mathbf{s}_i^* \notin \mathbb{V}_t$, else $\vec{\eta}_i \leftarrow^{\text{U}} \mathbb{F}_q^{2n}$,
 $\mathbf{c}_i := (\underbrace{\hspace{1.5cm}}_n s_i \vec{v}_i, \underbrace{\hspace{1.5cm}}_{2n} 0^{2n}, \underbrace{\hspace{1.5cm}}_n 0^n, \underbrace{\hspace{1.5cm}}_{2n} \vec{\eta}_i)_{\mathbb{B}_1}$,

$\mathbf{c}_{\ell+1} := (s_{\ell+1} - \theta_{\ell+1} \cdot \mathbf{H}_{\text{hk}}^{\lambda, \text{D}}(m \parallel \mathbb{S}), \theta_{\ell+1}, 0, 0, 0, 0, \eta_{\ell+1})_{\mathbb{B}_2}$,

return 0 if $e(\mathbf{b}_{0,1}, \mathbf{s}_0^*) = 1$,

return 1 if $\prod_{i=0}^{\ell+1} e(\mathbf{c}_i, \mathbf{s}_i^*) = 1$, return 0 otherwise.

E.4 Security

Theorem 2. The proposed ABS scheme is perfectly private.

Theorem 2 is proven in a similar manner to Theorem 1 in the full version of [25] (privacy of ABS scheme in [25]).

Theorem 3. The proposed ABS scheme is unforgeable (adaptive-predicate unforgeable) under the DLIN assumption and the existence of collision resistant hash functions.

For any adversary \mathcal{A} , there exist probabilistic machines $\mathcal{F}_0, \dots, \mathcal{F}_4$, whose running times are essentially the same as that of \mathcal{A} , such that for any security parameter λ ,

$$\begin{aligned}
 \text{Adv}_{\mathcal{A}}^{\text{ABS,UF}}(\lambda) &\leq \text{Adv}_{\mathcal{F}_0}^{\text{DLIN}}(\lambda) + \sum_{l=1}^2 \sum_{h=1}^{\nu_1} (\text{Adv}_{\mathcal{F}_{l,h,0}}^{\text{DLIN}}(\lambda) + \sum_{j=1}^n \sum_{\iota=1}^2 \text{Adv}_{\mathcal{F}_{l,h,j,\iota}}^{\text{DLIN}}(\lambda)) \\
 &\quad + \sum_{h=1}^{\nu_2} (\text{Adv}_{\mathcal{F}_{3,h}}^{\text{DLIN}}(\lambda) + \text{Adv}_{\mathcal{F}_{4,h}}^{\text{H,CR}}(\lambda)) + \epsilon,
 \end{aligned}$$

where $\mathcal{F}_{l,h,0}(\cdot) := \mathcal{F}_l(h, 0, \cdot)$, $\mathcal{F}_{l,h,j,\iota}(\cdot) := \mathcal{F}_l(h, j, \iota, \cdot)$ for $l = 1, 2$, $\mathcal{F}_{l,h}(\cdot) := \mathcal{F}_l(h, \cdot)$ for $l = 3, 4$, ν_1 (resp. ν_2) is the maximum number of \mathcal{A} 's reveal key (resp. signature) queries, ℓ is the maximum number of rows in access matrices M of key queries, and $\epsilon := (2\nu_1\ell + 20\nu_1n + 12\nu_1 + 5\nu_2 + 10)/q$.

Key Lemmas We will show Lemmas 3 and 4 for the proof of Theorem 1.

Definition 20 (Problem 2). *Problem 2 is to guess β , given $(\text{param}_n, \{\mathbb{B}_\iota, \widehat{\mathbb{B}}_\iota^*\}_{\iota=0,1,2}, \{e_{\beta,i}\}_{i=0,\dots,n+1}, \mathbf{f}) \xleftarrow{\text{R}} \mathcal{G}_\beta^{\text{P2}}(1^\lambda, n)$, where*

$$\begin{aligned} \mathcal{G}_\beta^{\text{P2}}(1^\lambda, n) : & \quad (\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1, \{B_{i,j}^*, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \mathbb{B}_2, \mathbb{B}_2^*) \xleftarrow{\text{R}} \mathcal{G}_{\text{ob}}^{\text{ABS}}(1^\lambda, 6, n), \\ & \quad \widehat{\mathbb{B}}_0^* := (\mathbf{b}_{0,1}^*, \mathbf{b}_{0,3}^*, \mathbf{b}_{0,4}^*), \\ & \quad \widehat{\mathbb{B}}_1^* := (\mathbf{b}_{1,1}^*, \dots, \mathbf{b}_{1,n}^*, \mathbf{b}_{1,3n+1}^*, \dots, \mathbf{b}_{1,6n}^*) \text{ is calculated as in Eq. (1) from } \{B_{i,j}^*, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \\ & \quad \widehat{\mathbb{B}}_2^* := (\mathbf{b}_{2,1}^*, \mathbf{b}_{2,2}^*, \mathbf{b}_{2,5}^*, \dots, \mathbf{b}_{2,7}^*), \quad \delta, \delta_0 \xleftarrow{\text{U}} \mathbb{F}_q, \quad \rho \xleftarrow{\text{U}} \mathbb{F}_q^\times, \quad \vec{z} \xleftarrow{\text{U}} \mathbb{F}_q^2, \\ & \quad \mathbf{e}_{0,0} := (\delta, 0, 0, \delta_0)_{\mathbb{B}_0}, \quad \mathbf{e}_{1,0} := (\delta, \rho, 0, \delta_0)_{\mathbb{B}_0}, \\ & \quad \text{for } i = 1, \dots, n; \quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \quad \vec{\delta}_{j,i} \xleftarrow{\text{U}} \mathbb{F}_q^{2n}, \\ & \quad \mathbf{e}_{0,i} := \left(\underbrace{\delta \vec{e}_i}_n, \underbrace{0^{2n}}_{2n}, \underbrace{0^n}_n, \underbrace{\vec{\delta}_{j,i}}_{2n} \right)_{\mathbb{B}_1}, \\ & \quad \mathbf{e}_{1,i} := \left(\delta \vec{e}_i, \rho \vec{e}_i, 0^n, 0^n, \vec{\delta}_{j,i} \right)_{\mathbb{B}_1}, \\ & \quad \mathbf{e}_{0,n+1} := (\delta, 0, 0^2, 0^2, \delta_0)_{\mathbb{B}_2}, \quad \mathbf{e}_{1,n+1} := (\delta, 0, \vec{z}, 0^2, \delta_0)_{\mathbb{B}_2}, \quad \mathbf{f} := \delta \mathbf{b}_{2,2}, \\ & \quad \text{return } (\text{param}_n, \{\mathbb{B}_\iota, \widehat{\mathbb{B}}_\iota^*\}_{\iota=0,1,2}, \{e_{\beta,i}\}_{i=0,\dots,n+1}, \mathbf{f}), \end{aligned}$$

for $\beta \xleftarrow{\text{U}} \{0, 1\}$. For a probabilistic machine \mathcal{B} , the advantage of \mathcal{B} for Problem 2, $\text{Adv}_{\mathcal{B}}^{\text{P2}}(\lambda)$, is similarly defined as in Definition 8.

Lemma 22. *For any adversary \mathcal{B} , there is a probabilistic machine \mathcal{F} , whose running time is essentially the same as that of \mathcal{B} , such that for any security parameter λ , $\text{Adv}_{\mathcal{B}}^{\text{P2}}(\lambda) \leq \text{Adv}_{\mathcal{F}}^{\text{DLIN}}(\lambda) + 5/q$.*

Lemma 22 is proven similarly to Lemma 1 in [23]. □

Definition 21 (Problem 3). *Problem 3 is to guess β , after running the following 2-step game:*

1. *The challenger generates*

$$\begin{aligned} & \quad (\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1, \{B_{i,j}^*, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \mathbb{B}_2, \mathbb{B}_2^*) \xleftarrow{\text{R}} \mathcal{G}_{\text{ob}}^{\text{ABS}}(1^\lambda, 6, n), \\ & \quad \widehat{\mathbb{B}}_0 := (\mathbf{b}_{0,1}, \mathbf{b}_{0,3}, \mathbf{b}_{0,4}), \quad \widehat{\mathbb{B}}_1 := (\mathbf{b}_{1,1}, \dots, \mathbf{b}_{1,n}, \mathbf{b}_{1,3n+1}, \dots, \mathbf{b}_{1,6n}), \\ & \quad \widehat{\mathbb{B}}_1^* := (\mathbf{b}_{1,1}^*, \dots, \mathbf{b}_{1,n}^*, \mathbf{b}_{1,3n+1}^*, \dots, \mathbf{b}_{1,6n}^*) \text{ is calculated as in Eq. (1) from } \{B_{i,j}^*, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \end{aligned}$$

and gives $(\text{param}_n, \widehat{\mathbb{B}}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}_1, \widehat{\mathbb{B}}_1^*, \mathbb{B}_2, \mathbb{B}_2^*)$ to the adversary.

2. The adversary gives the target vector \vec{y} to the challenger. The challenger then generates

$$\begin{aligned} \delta, \delta_0, \omega, \varphi_0, \varphi_1 &\stackrel{\text{U}}{\leftarrow} \mathbb{F}_q, \quad \tau, \rho \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q^\times, \\ \mathbf{h}_{0,0}^* &:= (\omega, 0, 0, \varphi_0, 0)_{\mathbb{B}_0^*}, \quad \mathbf{h}_{1,0}^* := (\omega, \tau, 0, \varphi_0, 0)_{\mathbb{B}_0^*}, \quad \mathbf{e}_0 := (\delta, \rho, 0, 0, \delta_0)_{\mathbb{B}_0}, \\ \text{for } j = 1, \dots, n; \quad i = 1, \dots, n; \quad \vec{e}_i &:= (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \quad \vec{\delta}_{j,i} \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q^{2n}, \\ U_j &\stackrel{\text{U}}{\leftarrow} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q), \quad Z_j := (U_j^{-1})^T, \\ \mathbf{h}_{0,1}^* &:= \left(\begin{array}{cccc} \omega \vec{y}, & 0^{2n}, & \varphi_1 \vec{y}, & 0^{2n} \end{array} \right)_{\mathbb{B}_1^*}, \\ \mathbf{h}_{1,1}^* &:= \left(\begin{array}{cccc} \omega \vec{y}, & \tau \vec{y}, & \tau \vec{y}, & \varphi_1 \vec{y}, & 0^{2n} \end{array} \right)_{\mathbb{B}_1^*}, \\ \mathbf{e}_{0,j,i} &:= \left(\begin{array}{cccc} \delta \vec{e}_i, & \rho \vec{e}_i, & 0^n, & 0^n, & \vec{\delta}_{j,i} \end{array} \right)_{\mathbb{B}_1}, \\ \mathbf{e}_{1,j,i} &:= \left(\begin{array}{cccc} \delta \vec{e}_i, & 0^n, & \rho \vec{e}_i \cdot Z_j, & 0^n, & \vec{\delta}_{j,i} \end{array} \right)_{\mathbb{B}_1}, \end{aligned}$$

for $\beta \stackrel{\text{U}}{\leftarrow} \{0, 1\}$, and returns $\varrho := (\mathbf{h}_{\beta,0}^*, \mathbf{e}_0, \mathbf{h}_{\beta,1}^*, \{\mathbf{e}_{\beta,j,i}\}_{j=1,\dots,\ell; i=1,\dots,n})$ to the adversary.

For a probabilistic adversary \mathcal{B} , we define the advantage of \mathcal{B} as the quantity $\text{Adv}_{\mathcal{B}}^{\text{P3}}(\lambda) := |\Pr[\mathcal{B} \text{ outputs } 1 \mid \varrho \text{ with } \beta = 0 \text{ is given to } \mathcal{B}] - \Pr[\mathcal{B} \text{ outputs } 1 \mid \varrho \text{ with } \beta = 1 \text{ is given to } \mathcal{B}]|$.

Lemma 23. For any adversary \mathcal{B} , there are probabilistic machines $\mathcal{F}_0, \mathcal{F}_{j,\iota}$ ($j = 1, \dots, n; \iota = 1, 2$), whose running times are essentially the same as that of \mathcal{B} , such that for any security parameter λ , $\text{Adv}_{\mathcal{B}}^{\text{P3}}(\lambda) \leq \text{Adv}_{\mathcal{F}_0}^{\text{DLIN}}(\lambda) + \sum_{j=1}^n \sum_{\iota=1}^2 \text{Adv}_{\mathcal{F}_{j,\iota}}^{\text{DLIN}}(\lambda) + (10n + 5)/q$.

Lemma 23 is proven in a similar manner to Lemma 3.

Definition 22 (Problem 4). Problem 4 is to guess $\beta \in \{0, 1\}$, given $(\text{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}_t^*\}_{t=0,d+1}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=1,\dots,d}, \mathbf{h}_{\beta,0}^*, \mathbf{e}_0, \{\mathbf{h}_{t,i}^*\}_{t=1,\dots,d; i=1,\dots,n_t}, \{\mathbf{h}_{\beta,d+1,i}^*, \mathbf{e}_{d+1,i}\}_{i=1,2}) \stackrel{\text{R}}{\leftarrow} \mathcal{G}_{\beta}^{\text{P4}}(1^\lambda, n)$, where

$$\begin{aligned} \mathcal{G}_{\beta}^{\text{P4}}(1^\lambda, n) &: (\text{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1, \{B_{i,j}^*, B'_{i,j,l}\}_{i,j=1,\dots,6; l=1,\dots,n}, \mathbb{B}_2, \mathbb{B}_2^*) \stackrel{\text{R}}{\leftarrow} \mathcal{G}_{\text{ob}}^{\text{ABS}}(1^\lambda, 6, n), \\ \widehat{\mathbb{B}}_0 &:= (\mathbf{b}_{0,1}, \mathbf{b}_{0,3}, \mathbf{b}_{0,4}), \quad \widehat{\mathbb{B}}_2 := (\mathbf{b}_{2,1}, \mathbf{b}_{2,2}, \mathbf{b}_{2,5}, \dots, \mathbf{b}_{2,7}), \\ \mathbb{B}_1^* &:= (\mathbf{b}_{1,1}^*, \dots, \mathbf{b}_{1,6n}^*) \text{ is calculated as in Eq. (1) from } \{B_{i,j}^*, B'_{i,j,l}\}_{i,j=1,\dots,6; l=1,\dots,n}, \\ \sigma, \tau &\stackrel{\text{U}}{\leftarrow} \mathbb{F}_q^\times, \quad \omega, \delta, \delta_0 \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q, \quad \mathbf{h}_{0,0}^* := (\delta, 0, \delta_0, 0)_{\mathbb{B}_0^*}, \quad \mathbf{h}_{1,0}^* := (\delta, \sigma, \delta_0, 0)_{\mathbb{B}_0^*}, \quad \mathbf{e}_0 := (\omega, \tau, 0, 0)_{\mathbb{B}_0}, \\ \mathbf{h}_{1,i}^* &:= \delta \mathbf{b}_{1,i}^* \text{ for } i = 1, \dots, n, \quad U \stackrel{\text{U}}{\leftarrow} GL(2, \mathbb{F}_q), \quad Z := (U^{-1})^T, \\ \text{for } i = 1, 2; \quad \vec{e}_i &:= (0^{i-1}, 1, 0^{2-i}), \quad \vec{\delta}_i \stackrel{\text{U}}{\leftarrow} \mathbb{F}_q^2, \\ \mathbf{h}_{0,2,i}^* &:= \left(\begin{array}{cccc} \delta \vec{e}_i, & 0^2, & \vec{\delta}_i, & 0 \end{array} \right)_{\mathbb{B}_2^*}, \\ \mathbf{h}_{1,2,i}^* &:= \left(\begin{array}{cccc} \delta \vec{e}_i, & \sigma \vec{e}_i U, & \vec{\delta}_i, & 0 \end{array} \right)_{\mathbb{B}_2^*}, \\ \mathbf{e}_{2,i} &:= \left(\begin{array}{cccc} \omega \vec{e}_i, & \tau \vec{e}_i Z, & 0^2, & 0 \end{array} \right)_{\mathbb{B}_2}, \\ \text{return } &(\text{param}_n, \{\widehat{\mathbb{B}}_t, \mathbb{B}_t^*\}_{t=0,2}, \mathbb{B}_1, \mathbb{B}_1^*, \mathbf{h}_{\beta,0}^*, \mathbf{e}_0, \{\mathbf{h}_{1,i}^*\}_{i=1,\dots,n}, \{\mathbf{h}_{\beta,2,i}^*, \mathbf{e}_{2,i}\}_{i=1,2}), \end{aligned}$$

for $\beta \stackrel{\text{U}}{\leftarrow} \{0, 1\}$. For a probabilistic machine \mathcal{B} , the advantage of \mathcal{B} for Problem 4, $\text{Adv}_{\mathcal{B}}^{\text{P4}}(\lambda)$, is similarly defined as in Definition 8.

Lemma 24. For any adversary \mathcal{B} , there is a probabilistic machine \mathcal{F} , whose running time is essentially the same as that of \mathcal{B} , such that for any security parameter λ , $\text{Adv}_{\mathcal{B}}^{\text{P4}}(\lambda) \leq \text{Adv}_{\mathcal{F}}^{\text{DLIN}}(\lambda) + 5/q$.

Lemma 24 is proven similarly to Lemma 2 in [23]. \square

Proof of Theorem 3 : To prove Theorem 3, we consider the following $(2\nu_1 + \nu_2 + 3)$ games. In Game 0, a part framed by a box indicates coefficients to be changed in a subsequent game. In the other games, a part framed by a box indicates coefficients which were changed in a game from the previous game.

Game 0 : Original game. That is, the reply to a reveal key query for $\Gamma := \{x_j\}_{j=1,\dots,n'}$ is:

$$\mathbf{k}_0^* := (\omega, \boxed{0}, \varphi_0, 0)_{\mathbb{B}_0^*}, \quad (11)$$

$$\mathbf{k}_1^* := (\underbrace{\omega \vec{y}}_n, \underbrace{\boxed{0^{2n}}}_{2n}, \underbrace{\varphi_1 \vec{y}}_n, \underbrace{0^{2n}}_{2n})_{\mathbb{B}_1^*}, \quad (12)$$

where $b \stackrel{\cup}{\leftarrow} \{0, 1\}; \omega, \varphi_0, \varphi_1 \stackrel{\cup}{\leftarrow} \mathbb{F}_q$, and $\vec{y} := (y_1, \dots, y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \cdot \prod_{j=1}^{n'} (z - x_j)$. The reply to a reveal signature query for (m, \mathbb{S}) with $\mathbb{S} := (M, \rho)$ are:

$$\mathbf{s}_0^* := (\tilde{\delta}, \boxed{0}, \sigma_0, 0)_{\mathbb{B}_0^*}, \quad (13)$$

$$\mathbf{s}_i^* := (\vec{z}_i, 0^{2n_i}, \vec{\sigma}_i, 0^{2n})_{\mathbb{B}_1^*} \text{ for } i = 1, \dots, \ell, \quad (14)$$

$$\mathbf{s}_{\ell+1}^* := (\tilde{\delta}(1, H_{\text{hk}}^{\lambda, \text{D}}(m \| \mathbb{S})), \boxed{0^2}, \vec{\sigma}_{\ell+1}, 0)_{\mathbb{B}_2^*}, \quad (15)$$

where, $\tilde{\delta} \stackrel{\cup}{\leftarrow} \mathbb{F}_q^\times$, $\sigma_0 \stackrel{\cup}{\leftarrow} \mathbb{F}_q$, $\vec{\sigma}_i \stackrel{\cup}{\leftarrow} \mathbb{F}_q^n$, $\vec{\sigma}_{\ell+1} \stackrel{\cup}{\leftarrow} \mathbb{F}_q^2$, $(\zeta_i) \stackrel{\cup}{\leftarrow} \{(\zeta_i) \mid \sum_{i=1}^{\ell} \zeta_i M_i = \vec{1}\}$, and for $i = 1, \dots, \ell$, if $\rho(i) = v_i$, then $\vec{z}_i \stackrel{\cup}{\leftarrow} \{\vec{z}_i \mid \vec{z}_i \cdot \vec{v}_i = 0, z_{i,1} = \tilde{\delta} \zeta_i\}$, if $\rho(i) = -v_i$, then $\vec{z}_i \stackrel{\cup}{\leftarrow} \{\vec{z}_i \mid \vec{z}_i \cdot \vec{v}_i = \tilde{\delta} \zeta_i\}$ with $\vec{v}_i := (v_i^{n-1}, \dots, v_i, 1) \in \mathbb{F}_q^n$. The verification text for (m', \mathbb{S}') with $\mathbb{S}' := (M, \rho)$ is:

$$\left. \begin{aligned} \mathbf{c}_0 &:= (\boxed{-s_0 - s_{\ell+1}}, \boxed{0}, 0, \eta_0)_{\mathbb{B}_0}, \\ \text{for } i = 1, \dots, \ell, & \left. \begin{aligned} \text{if } \rho(i) = v_i, \mathbf{c}_i &:= (\underbrace{s_i \vec{e}_1 + \theta_i \vec{v}_i}_n, \underbrace{\boxed{0^{2n}}}_{2n}, \underbrace{0^n}_n, \underbrace{\vec{\eta}_i}_{2n})_{\mathbb{B}_1}, \\ \text{if } \rho(i) = -v_i, \mathbf{c}_i &:= (\underbrace{s_i \vec{v}_i}_n, \underbrace{\boxed{0^{2n}}}_{2n}, \underbrace{0^n}_n, \underbrace{\vec{\eta}_i}_{2n})_{\mathbb{B}_1}, \end{aligned} \right\} \\ \mathbf{c}_{\ell+1} &:= (s_{\ell+1} \vec{e}_1 + \theta_{\ell+1} (-H_{\text{hk}}^{\lambda, \text{D}}(m' \| \mathbb{S}')), \boxed{0^2}, 0^2, \eta_{\ell+1})_{\mathbb{B}_2}, \end{aligned} \right\} \quad (16)$$

where $\vec{f} \stackrel{\cup}{\leftarrow} \mathbb{F}_q^r$, $\vec{s}^\top := (s_1, \dots, s_\ell)^\top := M \cdot \vec{f}^\top$, $s_0 := \vec{1} \cdot \vec{f}^\top$, $\theta_i, s_{\ell+1}, \eta_0, \eta_{\ell+1} \stackrel{\cup}{\leftarrow} \mathbb{F}_q$, $\vec{\eta}_i \stackrel{\cup}{\leftarrow} \mathbb{F}_q^{2n}$, $\vec{e}_1 = (1, 0, \dots, 0) \in \mathbb{F}_q^n$, and $\vec{v}_i := (v_i^{n-1}, \dots, v_i, 1) \in \mathbb{F}_q^n$.

Game 1 : Same as Game 0 except that the verification text for (m', \mathbb{S}') with $\mathbb{S}' := (M, \rho)$ is:

$$\mathbf{c}_0 := (-s_0 - s_{\ell+1}, \boxed{-r_0 - r_{\ell+1}}, 0, \eta_0)_{\mathbb{B}_0}, \quad (17)$$

$$\left. \begin{aligned} \text{for } i = 1, \dots, \ell, & \left. \begin{aligned} \text{if } \rho(i) = v_i, \mathbf{c}_i &:= (\underbrace{s_i \vec{e}_1 + \theta_i \vec{v}_i}_n, \underbrace{\boxed{r_i \vec{e}_1 + \psi_i \vec{v}_i}}_{2n}, \underbrace{0^n}_n, \underbrace{\vec{\eta}_i}_{2n})_{\mathbb{B}_1}, \\ \text{if } \rho(i) = -v_i, \mathbf{c}_i &:= (\underbrace{s_i \vec{v}_i}_n, \underbrace{\boxed{r_i \vec{v}_i}}_{2n}, \underbrace{0^n}_n, \underbrace{\vec{\eta}_i}_{2n})_{\mathbb{B}_1}, \end{aligned} \right\} \\ \mathbf{c}_{\ell+1} &:= (s_{\ell+1} \vec{e}_1 + \theta_{\ell+1} (-H_{\text{hk}}^{\lambda, \text{D}}(m' \| \mathbb{S}')), 1), \end{aligned} \right\} \quad (18)$$

$$\left. \begin{aligned} \mathbf{c}_{\ell+1} &:= (s_{\ell+1} \vec{e}_1 + \theta_{\ell+1} (-H_{\text{hk}}^{\lambda, \text{D}}(m' \| \mathbb{S}')), 1), \\ & \boxed{r_{\ell+1} \vec{e}_1 + \psi_{\ell+1} (-H_{\text{hk}}^{\lambda, \text{D}}(m' \| \mathbb{S}')), 0^2, \eta_{\ell+1})_{\mathbb{B}_2}, \end{aligned} \right\} \quad (19)$$

where $\vec{g} \stackrel{\cup}{\leftarrow} \mathbb{F}_q^r$, $\vec{r}^\top := (r_1, \dots, r_\ell)^\top := M \cdot \vec{g}^\top$, $r_0 := \vec{1} \cdot \vec{g}^\top$, $r_{\ell+1}, \psi_i \stackrel{\cup}{\leftarrow} \mathbb{F}_q$, and all the other variables are generated as in Game 0.

Game 2- h -1 ($h = 1, \dots, \nu_1$) : Game 2-0-2 is Game 1. Game 2- h -1 is the same as Game 2- $(h-1)$ -2 except the reply to the h -th key query for Γ are:

$$\begin{aligned} \mathbf{k}_0^* &:= (\omega, \boxed{\tau'}, \varphi_0, 0)_{\mathbb{B}_0^*}, \\ \mathbf{k}_1^* &:= (\underbrace{\omega \vec{y}}_n, \underbrace{\boxed{\tau \vec{y}, \tau \vec{y}'}}_{2n}, \underbrace{\varphi_1 \vec{y}}_n, \underbrace{0^{2n}}_{2n})_{\mathbb{B}_1^*}, \end{aligned} \quad (20)$$

where $\tau, \tau' \xleftarrow{\text{U}} \mathbb{F}_q$, and the i -th component ($i = 1, \dots, \ell$) of the verification text for (m', \mathbb{S}') with $\mathbb{S}' := (M, \rho)$ is:

$$\left. \begin{aligned} &\text{for } i = 1, \dots, \ell, \\ &\text{if } \rho(i) = v_i, \quad \mathbf{c}_i := (\underbrace{s_i \vec{e}_1 + \theta_i \vec{v}_i}_n, \underbrace{0^n, \boxed{\vec{w}_i}}_{2n}, \underbrace{0^n}_n, \underbrace{\vec{\eta}_i}_{2n})_{\mathbb{B}_1}, \\ &\text{if } \rho(i) = \neg v_i, \quad \mathbf{c}_i := (\underbrace{s_i \vec{v}_i}_n, \underbrace{0^n, \boxed{\vec{w}_i}}_{2n}, \underbrace{0^n}_n, \underbrace{\vec{\eta}_i}_{2n})_{\mathbb{B}_1}, \end{aligned} \right\} \quad (21)$$

where $\vec{w}_i \xleftarrow{\text{U}} \{\vec{w}_i \in \mathbb{F}_q^n \mid \vec{w}_i \cdot \vec{y} = (r_i \vec{e}_1 + \psi_i \vec{v}_i) \cdot \vec{y}\}$, $\vec{w}_i \xleftarrow{\text{U}} \{\vec{w}_i \in \mathbb{F}_q^n \mid \vec{w}_i \cdot \vec{y} = r_i \vec{v}_i \cdot \vec{y}\}$, all the other variables are generated as in Game 2- $(h-1)$ -2.

Game 2- h -2 ($h = 1, \dots, \nu_1$) : Game 2- h -2 is the same as Game 2- h -1 except the i -th component \mathbf{c}_i of the verification text for (m', \mathbb{S}') with $\mathbb{S}' := (M, \rho)$ are given by Eq. (18), and the component \mathbf{k}_1^* of the reply to the h -th key query for Γ is given by Eq. (12) (and \mathbf{k}_0^* is given by Eq. (20)). all the other variables are generated as in Game 2- h -1.

Game 3- h ($h = 1, \dots, \nu_2$) : Game 3-0 is Game 2- ν_1 -2. Game 3- h is the same as Game 3- $(h-1)$ except that $\mathbf{s}_0^*, \mathbf{s}_{\ell+1}^*$ of the reply to the h -th AltSig query for (m, \mathbb{S}) are:

$$\left. \begin{aligned} \mathbf{s}_0^* &:= (\tilde{\delta}, \boxed{\pi_0}, \sigma_0, 0)_{\mathbb{B}_0^*}, \\ \mathbf{s}_{\ell+1}^* &:= (\tilde{\delta}(1, \text{H}_{\text{hk}}^{\lambda, \text{D}}(m \parallel \mathbb{S})), \boxed{\vec{\pi}_{\ell+1}}, \vec{\sigma}_{\ell+1}, 0)_{\mathbb{B}_2^*}, \end{aligned} \right\} \quad (22)$$

where $\pi_0 \xleftarrow{\text{U}} \mathbb{F}_q$, $\vec{\pi}_{\ell+1} \xleftarrow{\text{U}} \mathbb{F}_q^2$, and all the other variables are generated as in Game 3- $(h-1)$.

Game 4 : Same as Game 3- ν_2 except that \mathbf{c}_0 generated in Ver for verifying the output of the adversary is:

$$\mathbf{c}_0 := (\boxed{\tilde{s}_0}, -r_0 - r_{\ell+1}, 0, \eta_0)_{\mathbb{B}_0}, \quad (23)$$

where $\tilde{s}_0 \xleftarrow{\text{U}} \mathbb{F}_q$ (i.e., independent from all the other variables) and all the other variables are generated as in Game 3- ν_2 .

Let $\text{Adv}_{\mathcal{A}}^{(0)}(\lambda), \text{Adv}_{\mathcal{A}}^{(1)}(\lambda), \text{Adv}_{\mathcal{A}}^{(2-h-\ell)}(\lambda), \text{Adv}_{\mathcal{A}}^{(3-h)}(\lambda)$, and $\text{Adv}_{\mathcal{A}}^{(4)}(\lambda)$ be the advantage of \mathcal{A} in Game 0, 1, 2- $h-\ell$, 3- h and 4, respectively. $\text{Adv}_{\mathcal{A}}^{(0)}(\lambda)$ is equivalent to $\text{Adv}_{\mathcal{A}}^{\text{ABS}, \text{UF}}(\lambda)$ and it is obtained that $\text{Adv}_{\mathcal{A}}^{(4)}(\lambda) = 1/q$ by Lemma 30.

We will show five lemmas (Lemmas 25–29) that evaluate the gaps between pairs of subsequent games. From these lemmas and Lemmas 22–24, we obtain $\text{Adv}_{\mathcal{A}}^{\text{ABS}, \text{UF}}(\lambda) = \text{Adv}_{\mathcal{A}}^{(0)}(\lambda) \leq \left| \text{Adv}_{\mathcal{A}}^{(0)}(\lambda) - \text{Adv}_{\mathcal{A}}^{(1)}(\lambda) \right| + \sum_{h=1}^{\nu_1} \left(\left| \text{Adv}_{\mathcal{A}}^{(2-(h-1)-2)}(\lambda) - \text{Adv}_{\mathcal{A}}^{(2-h-1)}(\lambda) \right| + \left| \text{Adv}_{\mathcal{A}}^{(2-h-1)}(\lambda) - \text{Adv}_{\mathcal{A}}^{(2-h-2)}(\lambda) \right| \right) + \sum_{h=1}^{\nu_2} \left| \text{Adv}_{\mathcal{A}}^{(3-(h-1))}(\lambda) - \text{Adv}_{\mathcal{A}}^{(3-h)}(\lambda) \right| + \left| \text{Adv}_{\mathcal{A}}^{(3-\nu_2)}(\lambda) - \text{Adv}_{\mathcal{A}}^{(4)}(\lambda) \right| + \text{Adv}_{\mathcal{A}}^{(4)}(\lambda) \leq \text{Adv}_{\mathcal{F}_0}^{\text{DLIN}}(\lambda) + \sum_{l=1}^2 \sum_{h=1}^{\nu_1} (\text{Adv}_{\mathcal{F}_{l,h,0}}^{\text{DLIN}}(\lambda) + \sum_{j=1}^{\ell} \sum_{\iota=1}^2 \text{Adv}_{\mathcal{F}_{l,h,j,\iota}}^{\text{DLIN}}(\lambda)) + \sum_{h=1}^{\nu_2} (\text{Adv}_{\mathcal{F}_{3,h}}^{\text{DLIN}}(\lambda) + \text{Adv}_{\mathcal{F}_{4,h}}^{\text{H,CR}}(\lambda)) + (2\nu_1 \ell + 20\nu_1 n + 12\nu_1 + 5\nu_2 + 10)/q$. This completes the proof of Theorem 3. \square

Lemma 25. For any adversary \mathcal{A} , there exists a probabilistic machine \mathcal{B}_0 , whose running time is essentially the same as that of \mathcal{A} , such that for any security parameter λ , $|\text{Adv}_{\mathcal{A}}^{(1)}(\lambda) - \text{Adv}_{\mathcal{A}}^{(0)}(\lambda)| \leq \text{Adv}_{\mathcal{B}_0}^{\text{P2}}(\lambda)$.

Lemma 25 is proven in a similar manner to Lemma 6 in the full version of [25]. \square

Lemma 26. For any adversary \mathcal{A} , there exists a probabilistic machine \mathcal{B}_1 , whose running time is essentially the same as that of \mathcal{A} , such that for any security parameter λ , $|\text{Adv}_{\mathcal{A}}^{(2-h-1)}(\lambda) - \text{Adv}_{\mathcal{A}}^{(2-(h-1)-2)}(\lambda)| \leq \text{Adv}_{\mathcal{B}_{1,h}}^{\text{P3}}(\lambda) + (\ell + 1)/q$, where $\mathcal{B}_{1,h}(\cdot) := \mathcal{B}_1(h, \cdot)$ and ℓ is the maximum number of rows in access matrices M of key queries.

Lemma 26 is proven in a similar manner to Lemma 5. \square

Lemma 27. For any adversary \mathcal{A} , there exists a probabilistic machine \mathcal{B}_2 , whose running time is essentially the same as that of \mathcal{A} , such that for any security parameter λ , $|\text{Adv}_{\mathcal{A}}^{(2-h-2)}(\lambda) - \text{Adv}_{\mathcal{A}}^{(2-h-1)}(\lambda)| \leq \text{Adv}_{\mathcal{B}_{2,h}}^{\text{P3}}(\lambda) + (\ell + 1)/q$, where $\mathcal{B}_{2,h}(\cdot) := \mathcal{B}_2(h, \cdot)$ and ℓ is the maximum number of rows in access matrices M of key queries.

Lemma 27 is proven in a similar manner to Lemma 5. \square

Lemma 28. For any adversary \mathcal{A} , there exist probabilistic machines \mathcal{B}_3 and \mathcal{F}_4 , whose running times are essentially the same as that of \mathcal{A} , such that for any security parameter λ , $|\text{Adv}_{\mathcal{A}}^{(3-h)}(\lambda) - \text{Adv}_{\mathcal{A}}^{(3-(h-1))}(\lambda)| \leq \text{Adv}_{\mathcal{B}_{3,h}}^{\text{P4}}(\lambda) + \text{Adv}_{\mathcal{F}_{4,h}}^{\text{H,CR}}(\lambda) + 3/q$, where $\mathcal{B}_{3,h}(\cdot) := \mathcal{B}_3(h, \cdot)$ and $\mathcal{F}_{4,h}(\cdot) := \mathcal{F}_4(h, \cdot)$.

Lemma 29 is proven in a similar manner to Lemma 16 in the full version of [25]. \square

Lemma 29. For any adversary \mathcal{A} , for any security parameter λ , $|\text{Adv}_{\mathcal{A}}^{(4)}(\lambda) - \text{Adv}_{\mathcal{A}}^{(3-\nu_2)}(\lambda)| \leq 1/q$.

Lemma 29 is proven in a similar manner to Lemma 17 in the full version of [25]. \square

Lemma 30. For any adversary \mathcal{A} , for any security parameter λ , $\text{Adv}_{\mathcal{A}}^{(4)}(\lambda) = 1/q$.

Lemma 30 is proven in a similar manner to Lemma 18 in the full version of [25]. \square

F Selectively Secure Efficient IPE Scheme in [20]

We describe random dual orthonormal basis generator $\mathcal{G}_{\text{ob}}^{\text{IPE}}$ below, which is used as a subroutine in the proposed IPE scheme [20].

$$\begin{aligned} \mathcal{G}_{\text{ob}}^{\text{IPE}}(1^\lambda, N) : \text{param}'_{\mathbb{V}} &:= (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e) \xleftarrow{\text{R}} \mathcal{G}_{\text{dpts}}(1^\lambda, N), \\ \psi &\xleftarrow{\text{U}} \mathbb{F}_q^\times, g_T := e(G, G)^\psi, \quad \text{param}_{\mathbb{V}} := (\text{param}'_{\mathbb{V}}, g_T), \\ X &:= (\chi_{i,j}) \xleftarrow{\text{U}} \text{GL}(N, \mathbb{F}_q), \quad (\vartheta_{i,j}) := \psi \cdot (X^{\text{T}})^{-1}, \\ \mathbf{b}_i &:= \sum_{j=0}^{N-1} \chi_{i,j} \mathbf{a}_j, \mathbb{B} := (\mathbf{b}_0, \dots, \mathbf{b}_{N-1}), \quad \mathbf{b}_i^* := \sum_{j=0}^{N-1} \vartheta_{i,j} \mathbf{a}_j, \mathbb{B}^* := (\mathbf{b}_0^*, \dots, \mathbf{b}_{N-1}^*), \\ &\text{return } (\text{param}_{\mathbb{V}}, \mathbb{B}, \mathbb{B}^*). \end{aligned}$$

Construction

Setup($1^\lambda, n$) :

$$(\text{param}_{\mathbb{V}}, \mathbb{B} := (\mathbf{b}_0, \dots, \mathbf{b}_{n+3}), \mathbb{B}^* := (\mathbf{b}_0^*, \dots, \mathbf{b}_{n+3}^*)) \xleftarrow{\text{R}} \mathcal{G}_{\text{ob}}^{\text{IPE}}(1^\lambda, n+4),$$

$$\widehat{\mathbb{B}} := (\mathbf{b}_0, \dots, \mathbf{b}_n, \mathbf{b}_{n+3}), \widehat{\mathbb{B}}^* := (\mathbf{b}_0^*, \dots, \mathbf{b}_n^*, \mathbf{b}_{n+2}^*), \text{ return } \text{pk} := (1^\lambda, \text{param}_{\mathbb{V}}, \widehat{\mathbb{B}}), \text{ sk} := \widehat{\mathbb{B}}^*.$$

KeyGen(pk, sk, $\vec{v} \in \mathbb{F}_q^n \setminus \{\vec{0}\}$) : $\sigma, \eta \xleftarrow{\text{U}} \mathbb{F}_q$,

$$\mathbf{k}^* := (1, \overbrace{\sigma \vec{v}}^n, 0, \eta, 0)_{\mathbb{B}^*}, \text{ return } \text{sk}_{\vec{v}} := \mathbf{k}^*.$$

Enc(pk, $m, \vec{x} \in \mathbb{F}_q^n \setminus \{\vec{0}\}$) : $\omega, \varphi, \zeta \xleftarrow{\text{U}} \mathbb{F}_q$,

$$\mathbf{c}_1 := (\zeta, \overbrace{\omega \vec{x}}^n, 0, 0, \varphi)_{\mathbb{B}}, \mathbf{c}_2 := g_T^\zeta m, \text{ return } \text{ct}_{\vec{x}} := (\mathbf{c}_1, \mathbf{c}_2).$$

Dec(pk, $\text{sk}_{\vec{v}} := \mathbf{k}^*$, $\text{ct}_{\vec{x}} := (\mathbf{c}_1, \mathbf{c}_2)$) : $m' := \mathbf{c}_2 / e(\mathbf{c}_1, \mathbf{k}^*)$, return m' .

[Correctness] If $\vec{v} \cdot \vec{x} = 0$, then $e(\mathbf{c}_1, \mathbf{k}^*) = g_T^{\zeta + \omega \sigma \vec{v} \cdot \vec{x}} = g_T^\zeta$.

Theorem 4. *The proposed IPE scheme is selectively fully-attribute-hiding against chosen plaintext attacks under the DLIN assumption.*

For any adversary \mathcal{A} , there exist probabilistic machines \mathcal{D}_1 and \mathcal{D}_2 , whose running times are essentially the same as that of \mathcal{A} , such that for any security parameter λ , $\text{Adv}_{\mathcal{A}}^{\text{IPE, AH}}(\lambda) \leq \text{Adv}_{\mathcal{D}_1}^{\text{DLIN}}(\lambda) + \text{Adv}_{\mathcal{D}_2}^{\text{DLIN}}(\lambda) + \epsilon$, where $\epsilon := 12/q$.

The proof of Theorem 4 is given in [20].