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

Katsuyuki Takashima
Mitsubishi Electric
Takashima.Katsuyuki@aj.MitsubishiElectric.co.jp

August 29, 2014

Abstract

We propose a key-policy attribute-based encryption (KP-ABE) scheme with *constant-size ciphertexts*, whose semi-adaptive 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) keys from the DLIN. For achieving the above results, we extend the sparse matrix technique on dual pairing vector spaces. In particular, several algebraic properties of an elaborately chosen sparse matrix group are applied to the security proofs.

*An extended abstract of a preliminary version of this paper was presented at SCN 2014, the 9th Conference on Security and Cryptography for Networks. This is the full version, and provides significant technical contributions over the preliminary version, e.g., semi-adaptive security from DLIN with reduction factor $O(n)$, where n is the maximum number of attributes per ciphertext. Refer to Table 1 in Section 1.2 and Theorem 1 in Section 6.1.

Contents

1 Introduction

1.1 Backgrounds

The notion of *attribute-based encryption* (ABE) introduced by Sahai and Waters [28] 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 [16, 18] 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. [15], Herranz et al. [19], and Chen et al. [10] constructed ABE schemes with constant-size ciphertexts, but their access structures are very limited. Attrapadung, Libert and Panafieu [3] first constructed a KP-ABE scheme for span programs with constant-size ciphertexts and fast decryption which needs only a constant-number of pairing operations.

While Attrapadung et al.'s KP-ABE scheme (and subsequent works [33, 2]) show an interesting approach to achieving constant-size ciphertexts with expressive access structures, the security are proven only based on q-type assumptions (n-DBDHE assumption with n the maximum number of attributes per ciphertext and more complex EDHE assumptions). Previously, since the introduction by Mitsunari et al. [21] and Boneh et al. [6], various kinds of q-type assumptions have been widely used in order to achieve efficient cryptographic primitives [5, 7, 17, 14, 19]. However, the assumptions (and also the associated schemes) suffered a special attack which was presented by Cheon [12] at Eurocrypt 2006. More recently, Sakemi et al. [29] 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 concurrent and independent work, Chen and Wee [11] introduced the notion of semi-adaptive security for ABE, where the adversary specifies the challenge attribute set after it sees the public parameters but before it makes any secret key queries, and they also constructed a small-universe KP-ABE scheme with constant-size ciphertexts on *composite-order groups*.

Hence, to construct an expressive KP-ABE scheme with constant-size ciphertexts *from a static assumption on the prime-order groups* remains an interesting open problem in terms of practical and theoretical aspects on ABE. Also, since there exist no attribute-based signatures (ABS) [20, 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 semi-adaptive security is proven from the DLIN assumption in the standard model (Section 5). 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 of the sizes of the used attribute set and access structure. For

Table 1: Comparison of our scheme with KP-ABE *for span programs with constant-size ciphertexts* in [3, 2, 11], where $|\mathbb{G}|$, $|\mathbb{G}_T|$, n, ℓ, r, and ν_1 represent size of an element of a bilinear source group $\mathbb{G}$, that of a target group $\mathbb{G}_T$, the maximum number of attributes per ciphertext, and the number of rows and columns in access structure matrix for the secret key, and the maximum number of the adversary's pre-challenge key queries, respectively. PK, SK, and CT stand for public key, secret key, and ciphertext, respectively.

	ALP11 [3]	A14 [2]	CW14 [11]	Proposed
Universe	large	large	small	large
Security	selective	adaptive	semi-adaptive	semi-adaptive
Reduction factor	$O(n)$	$O(\nu_1)$	$O(n)$	$O(n)$
Order of $\mathbb{G}$	prime	composite	composite	prime
Assumption	n-DBDHE	EDHE3 & 4 parametrized by n, ℓ, r	Static assump. on composite order $\mathbb{G}$	DLIN
Access structures	Non-monotone span program	Monotone span program	Monotone span program	Non-monotone span program
PK size	$O(n)\,\lvert\mathbb{G}\rvert$	$O(n)\,\lvert\mathbb{G}\rvert$	$O(n)\,\lvert\mathbb{G}\rvert$	$O(n)\,\lvert\mathbb{G}\rvert$
SK size	$O(\ell n)\,\lvert\mathbb{G}\rvert$	$O(\ell n)\,\lvert\mathbb{G}\rvert$	$O(\ell n)\,\lvert\mathbb{G}\rvert$	$O(\ell n)\,\lvert\mathbb{G}\rvert$
CT size	$3\,\lvert\mathbb{G}\rvert + 1\,\lvert\mathbb{G}_T\rvert$*	$6\,\lvert\mathbb{G}\rvert + 1\,\lvert\mathbb{G}_T\rvert$	$2\,\lvert\mathbb{G}\rvert + 1\,\lvert\mathbb{G}_T\rvert$	$17\,\lvert\mathbb{G}\rvert + 1\,\lvert\mathbb{G}_T\rvert$

* In a subsequent work [33], CT size is reduced to $2\,|\mathbb{G}| + 1\,|\mathbb{G}_T|$.

comparison of our scheme with previous KP-ABE for span programs with constant-size ciphertexts, 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 7).
- For achieving the above results, we extend the sparse matrix technique on dual pairing vector spaces (DPVS) [22, 23] developed in [24]. In particular, several algebraic properties of an elaborately chosen sparse matrix group $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ are applied to the security proofs. For the details, see Sections 1.3, 4 and 6.3.

1.3 Key Techniques

We extend the sparse matrix technique on DPVS developed in [24], in which constant-size ciphertext zero/non-zero inner-product encryption are constructed from DLIN on a sparse matrix master key pair. Using the basic construction [24], to achieve short ciphertexts in our KP-ABE, attributes $\Gamma := \{x_j\}_{j=1,\ldots,n'}$ are encoded in an n-dimensional (with $n \geq n'+1$) vector $\vec{y} := (y_1, \ldots, y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \prod_{j=1}^{n'} (z - x_j)$. Each (non-zero) attribute value v_i (for $i = 1, \ldots, \ell$) associated with a row of access structure matrix M (in $\mathbb{S}$) is encoded as $\vec{v}_i := (v_i^{n-1}, \ldots, v_i, 1)$, so $\vec{y} \cdot \vec{v}_i = v_i^{n-1-n'} \prod_{j=1}^{n'} (v_i - x_j)$, and the value of inner product is equal to zero if and only if $v_i = x_j$ for some j, i.e., $v_i \in \Gamma$. Here, the relation between $\mathbb{S}$ and Γ is determined by the multiple inner product values $\vec{y} \cdot \vec{v}_i$ for one vector $\vec{y}$ which is equivalent to Γ. Hence, a ciphertext vector element $\boldsymbol{c}_1$ 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 $\boldsymbol{k}_i^*$ are encoded with $\vec{v}_i$ and shares s_i ($i = 1, \ldots, \ell$) for a central secret s_0, respectively (see Section 5.1 for the key idea). A standard dual system encryption (DSE) approach considers each pair of vectors

in the semi-functional space, $(\tau\vec{y}, r_i\vec{e}_1 + \psi_i\vec{v}_i)$ or $(\tau\vec{y}, r_i\vec{v}_i)$ with secret shares r_i of a secret r_0 and random τ, ψ_i, and then the vector pair is randomized with *preserving* the inner product values based on a *pairwise* independence argument. Since we must deal with a *common* $\tau\vec{y}$ in all the above pairs, we should modify the original argument for our scheme, which is based on a modified form of pairwise independence lemma (Lemma 3) for a specific matrix group $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ of size $n \times n$.

The security of our scheme is reduced to that of DLIN through multiple reduction steps (Theorem 1). A technical challenge for the security is to insert random (sparse) matrices $\{Z_{h,i}\}_{h=1,\ldots,\nu;\, i=1,\ldots,\ell}$ in $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}$ to key components $\{\boldsymbol{k}^*_{h,i}\}_{h=1,\ldots,\nu;\, i=1,\ldots,\ell}$ for each key query $h = 1, \ldots, \nu$ even when the underlying matrix for the basis $\mathbb{B}_1$ is *sparse*. For the purpose, first, only n randomness $\{Z_\kappa\}_{\kappa=1,\ldots,n}$ are sequentially inserted in a consistent manner with the security condition on the challenge $\vec{y}$ and key queries, and then, they are amplified to any polynomial number of random matrices, $\{Z_{h,i}\}_{h=1,\ldots,\nu;\, i=1,\ldots,\ell}$, by making linear combinations of $\{Z_\kappa\}_{\kappa=1,\ldots,n}$. The above steps are accomplished by applying computational (*swap*) game changes and information-theoretical (or conceptual) changes alternatingly, and by applying four nice algebraic properties of elaborately chosen sparse matrix group $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ to the security proof. The two key techniques are described in detail in Sections 6.3.1 and 6.3.2, respectively.

1.4 Notations

When A is a random variable or distribution, $y \xleftarrow{\mathsf{R}} A$ denotes that y is randomly selected from A according to its distribution. When A is a set, $y \xleftarrow{\mathsf{U}} A$ denotes that y is uniformly selected from A. We denote the finite field of order q by $\mathbb{F}_q$, and $\mathbb{F}_q \setminus \{0\}$ by $\mathbb{F}_q^\times$. A vector symbol denotes a vector representation over $\mathbb{F}_q$, e.g., $\vec{x}$ denotes $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$. For two vectors $\vec{x} = (x_1, \ldots, x_n)$ and $\vec{v} = (v_1, \ldots, v_n)$, $\vec{x} \cdot \vec{v}$ 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., $\boldsymbol{x} \in \mathbb{V}$. When $\boldsymbol{b}_i \in \mathbb{V}$ $(i = 1, \ldots, n)$, $\mathsf{span}\langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \rangle \subseteq \mathbb{V}$ (resp. $\mathsf{span}\langle \vec{x}_1, \ldots, \vec{x}_n \rangle$) denotes the subspace generated by $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ (resp. $\vec{x}_1, \ldots, \vec{x}_n$). For bases $\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N)$ and $\mathbb{B}^* := (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_N)$, $(x_1, \ldots, x_N)_{\mathbb{B}} := \sum_{i=1}^N x_i \boldsymbol{b}_i$ and $(y_1, \ldots, y_N)_{\mathbb{B}^*} := \sum_{i=1}^N y_i \boldsymbol{b}^*_i$. $\vec{e}_j$ denotes the canonical basis vector $(\overbrace{0 \cdots 0}^{j-1}, 1, \overbrace{0 \cdots 0}^{n-j}) \in \mathbb{F}_q^n$. $GL(n, \mathbb{F}_q)$ denotes the general linear group of degree n over $\mathbb{F}_q$.

2 Dual Pairing Vector Spaces and Decisional Linear (DLIN) Assumption

For simplicity of description, we will present the proposed schemes on the symmetric version of dual pairing vector spaces (DPVS) [22] constructed using symmetric bilinear pairing groups. For the asymmetric version of DPVS, see Appendix A.2 of the full version of [23].

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

"Dual pairing vector spaces (DPVS)" of dimension N *by a direct product of symmetric pairing groups* $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ *are given by prime* q*,* N*-dimensional vector space* $\mathbb{V} := \overbrace{\mathbb{G} \times \cdots \times \mathbb{G}}^{N}$ *over* $\mathbb{F}_q$*, cyclic group* $\mathbb{G}_T$ *of order* q*, and pairing* $e : \mathbb{V} \times \mathbb{V} \to \mathbb{G}_T$*. The pairing is defined by*

$e(\boldsymbol{x},\boldsymbol{y}) := \prod_{i=1}^{N} e(G_i,H_i) \in \mathbb{G}_T$ *where* $\boldsymbol{x} := (G_1,\ldots,G_N) \in \mathbb{V}$ *and* $\boldsymbol{y} := (H_1,\ldots,H_N) \in \mathbb{V}$. *This is nondegenerate bilinear i.e.,* $e(s\boldsymbol{x},t\boldsymbol{y}) = e(\boldsymbol{x},\boldsymbol{y})^{st}$ *and if* $e(\boldsymbol{x},\boldsymbol{y}) = 1$ *for all* $\boldsymbol{y} \in \mathbb{V}$, *then* $\boldsymbol{x} = \boldsymbol{0}$.

Definition 2 (DLIN: Decisional Linear Assumption [6]) *The DLIN problem is to guess* $\beta \in \{0,1\}$, *given* $(\mathsf{param}_{\mathbb{G}},\ G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda)$, *where* $\mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda) : \mathsf{param}_{\mathbb{G}} := (q,\mathbb{G},\mathbb{G}_T,G,e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda), \kappa,\delta,\xi,\sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q, Y_0 := (\delta+\sigma)G, Y_1 \xleftarrow{\mathsf{U}} \mathbb{G}, \mathrm{return}\ (\mathsf{param}_{\mathbb{G}}, G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta)$, *for* $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. *For a probabilistic machine* $\mathcal{E}$, *we define the advantage of* $\mathcal{E}$ *for the DLIN problem as:* $\mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) := \left|\mathsf{Pr}\left[\mathcal{E}(1^\lambda,\varrho)\to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{DLIN}}(1^\lambda)\right] - \mathsf{Pr}\left[\mathcal{E}(1^\lambda,\varrho)\to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{DLIN}}(1^\lambda)\right]\right|$. *The DLIN assumption is: For any probabilistic polynomial-time adversary* $\mathcal{E}$, *the advantage* $\mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda)$ *is negligible in* λ.

3 Definitions of Key-Policy Attribute-Based Encryption and Attribute-Based Signatures

3.1 Span Programs and Non-Monotone Access Structures

Definition 3 (Span Programs [4]) $\mathcal{U}$ $(\subset \{0,1\}^*)$ *is a universe, a set of attributes, which is expressed by a value of attribute, i.e.,* $v \in \mathbb{F}_q^\times (:= \mathbb{F}_q \setminus \{0\})$. *A span program over* $\mathbb{F}_q$ *is a labeled matrix* $\mathbb{S} := (M,\rho)$ *where* M *is a* $(\ell \times r)$ *matrix over* $\mathbb{F}_q$ *and* ρ *is a labeling of the rows of* M *by literals from* $\{v, v', \ldots, \neg v, \neg v', \ldots\}$ *(every row is labeled by one literal), i.e.,* $\rho : \{1,\ldots,\ell\} \to \{v, v', \ldots, \neg v, \neg v', \ldots\}$.

A span program accepts or rejects an input by the following criterion. Let Γ *be a set of attributes, i.e.,* $\Gamma := \{x_j\}_{1\le j\le n'}$. *When* Γ *is given to access structure* $\mathbb{S}$, *map* $\gamma : \{1,\ldots,\ell\} \to \{0,1\}$ *for span program* $\mathbb{S} := (M,\rho)$ *is defined as follows: For* $i = 1,\ldots,\ell$, *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.*

The span program $\mathbb{S}$ *accepts* Γ *if and only if* $\vec{1} \in \mathsf{span}\langle (M_i)_{\gamma(i)=1}\rangle$, *i.e., some linear combination of the rows* $(M_i)_{\gamma(i)=1}$ *gives the all one vector* $\vec{1}$. *(The row vector has the value 1 in eciphertextsach coordinate.)*

A span program is called monotone if the labels of the rows are only the positive literals $\{v, v', \ldots\}$. *Monotone span programs compute monotone functions. (So, a span program in general is "non"-monotone.)*

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

Definition 4 *A secret-sharing scheme for span program* $\mathbb{S} := (M,\rho)$ *is:*

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

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

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

Definition 5 (Key-Policy Attribute-Based Encryption: KP-ABE) *A key-policy attribute-based encryption scheme consists of probabilistic polynomial-time algorithms* $\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}$ *and* Dec. *They are given as follows:*

Setup *takes as input security parameter* 1^λ *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* $\mathsf{sk}_{\mathbb{S}}$.

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

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

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

Definition 6 (Semi-Adaptive Security) *The model for defining the semi-adaptively payload-hiding security of KP-ABE under chosen plaintext attack is given by the following game:*

Setup *In the semi-adaptive security, the challenger runs the setup,* $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda, n)$, *and gives public parameters* pk *to the adversary, then the adversary output a challenge attribute set,* Γ.

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* $\mathsf{sk}_{\mathbb{S}} \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \mathbb{S})$ *to the adversary.*

Challenge *The adversary submits two messages* $m^{(0)}, m^{(1)}$. *The challenger flips a coin* $b \xleftarrow{\mathsf{U}} \{0, 1\}$, *and computes* $\mathsf{ct}_\Gamma^{(b)} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, m^{(b)}, \Gamma)$. *It gives* $\mathsf{ct}_\Gamma^{(b)}$ *to the adversary.*

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

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

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

3.3 Attribute-Based Signatures (ABS)

Definition 7 (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* $\mathsf{accept} := 1$ *or* $\mathsf{reject} := 0$.

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

Definition 8 (Perfect Privacy) *An ABS scheme is perfectly private, if, for all* $(\mathsf{sk}, \mathsf{pk}) \xleftarrow{R} \mathsf{Setup}(1^\lambda, n)$, *all messages m, all attribute sets* Γ_1 *and* Γ_2, *all signing keys* $\mathsf{sk}_{\Gamma_1} \xleftarrow{R} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \Gamma_1)$ *and* $\mathsf{sk}_{\Gamma_2} \xleftarrow{R} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \Gamma_2)$, *all access structures* $\mathbb{S}$ *such that* $\mathbb{S}$ *accepts* Γ_1 *and* $\mathbb{S}$ *accepts* Γ_2, *distributions* $\mathsf{Sig}(\mathsf{pk}, \mathsf{sk}_{\Gamma_1}, m, \mathbb{S})$ *and* $\mathsf{Sig}(\mathsf{pk}, \mathsf{sk}_{\Gamma_2}, m, \mathbb{S})$ *are equal.*

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 9 (Unforgeability) *For an adversary, $\mathcal{A}$, we define* $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{ABS,UF}}(\lambda)$ *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* $(\mathsf{sk}, \mathsf{pk}) \xleftarrow{R} \mathsf{Setup}(1^\lambda, n)$ *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* $\mathsf{Ver}(\mathsf{pk}, m', \mathbb{S}', \sigma') = 1$.

Remark 1 Since a signing query in the unforgeability definition in [20, 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 $(\Gamma, \mathsf{sk}_\Gamma)$. 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 [20, 25] is problematic.

To address this issue, as in [27], 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 [30]. 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.)

4 Special Matrix Subgroups

Lemmas 1 and 4 are key lemmas for the security proof for our KP-ABE and ABS schemes. For positive integers w, n and $\vec{y} := (y_1, .., y_n) \in \mathbb{F}_q^n \setminus \mathsf{span}\langle \vec{e}_n \rangle$, let

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

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

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* $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ *are subgroups of* $GL(n, \mathbb{F}_q)$. *More specifically,* $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ *is the isotropy group of* $\vec{y}$ *in* $\mathcal{H}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q)$, *that is,* $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q) = \{U \in \mathcal{H}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q) \,|\, \vec{y}U = \vec{y}\}$.

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

Lemma 2 $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ *has a linear structure as* $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q) \cong A_{n-1} \setminus H_{n-2}$, *where* $A_{n-1} := \{\vec{u}' \in \mathbb{F}_q^n \,|\, \vec{y} \cdot \vec{u}' = y_n\}$ *is an* $(n-1)$*-dimensional affine space and* $H_{n-2} := A_{n-1} \cap \{u'_n = 0\}$ *is a hyperplane section of* A_{n-1}.

For all $(Z_\kappa \in \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}})_{\kappa=1,\ldots,n}$ *such that* $(\widetilde{Z}_\kappa := Z_\kappa - Z_1)_{\kappa=2,\ldots,n}$ *is a basis of linear subspace* $V_{n-1} := \{\vec{u}' \in \mathbb{F}_q^n \,|\, \vec{y} \cdot \vec{u}' = 0\}$ *over* $\mathbb{F}_q$, *the distribution of* $Z := \sum_{\kappa=1}^n \xi_\kappa Z_\kappa$ *with* $(\xi_\kappa) \xleftarrow{\mathsf{U}} \{(\xi_\kappa)_{\kappa=1,\ldots,n} \,|\, \sum_{\kappa=1}^n \xi_\kappa = 1\}$ *is equivalent to uniform one, i.e.,* $Z \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}$ *except with negligible probability* $1/q$.

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

Lemma 3 *For all* $\vec{y} \in \mathbb{F}_q^n - \mathsf{span}\langle \vec{e}_n \rangle$ *and* $\pi \in \mathbb{F}_q$, *let* $W_{\vec{y},\pi} := \{\vec{w} \in \mathbb{F}_q^n - \mathsf{span}\langle \vec{e}_n \rangle^{\perp} \mid \vec{y} \cdot \vec{w} = \pi\}$, *where* $\mathsf{span}\langle \vec{e}_n \rangle^{\perp} := \{\vec{w} \in \mathbb{F}_q^n \mid \vec{w} \cdot \vec{e}_n = 0\}$.

For all $(\vec{y}, \vec{v}) \in \left(\mathbb{F}_q^n - \mathsf{span}\langle \vec{e}_n \rangle\right) \times \left(\mathbb{F}_q^n - \mathsf{span}\langle \vec{e}_n \rangle^{\perp}\right)$, *if* U *and* Z *are generated as* $U \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q), Z := (U^{-1})^{\mathrm{T}}$, *then* $\vec{v}Z$ *is uniformly distributed in* $W_{\vec{y},(\vec{y}\cdot\vec{v})}$.

Let

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

Lemma 4 $\mathcal{L}(w, n, \mathbb{F}_q)$ *is a subgroup of* $GL(wn, \mathbb{F}_q)$.

The proof of Lemma 4 is given in Appendix A in the full version of [24].

5 Proposed KP-ABE Scheme with Constant Size Ciphertexts

5.1 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, $(\boldsymbol{c}_0, \boldsymbol{c}_1) \in \mathbb{G}^5 \times \mathbb{G}^n$, and $c_T \in \mathbb{G}_T$. A secret key consists of $\ell+1$ vector elements, $(\boldsymbol{k}_0^*, \boldsymbol{k}_1^*, \ldots, \boldsymbol{k}_\ell^*) \in \mathbb{G}^5 \times (\mathbb{G}^n)^\ell$ for access structure $\mathbb{S} := (M, \rho)$, where the number of rows of M is ℓ and $\boldsymbol{k}_i^*$ with $i \geq 1$ corresponds to the i-th row. Therefore, to achieve constant-size ciphertexts, we have to compress $\boldsymbol{c}_1 \in \mathbb{G}^n$ to a constant size in n. We now employ a special form of basis generation matrix, $X := \begin{pmatrix} \mu & & & \mu'_1 \\ & \ddots & & \vdots \\ & & \mu & \mu'_{n-1} \\ & & & \mu'_n \end{pmatrix} \in \mathcal{H}(n, \mathbb{F}_q)$ of Eq. (1) in Section 4, where $\mu, \mu'_1, \ldots, \mu'_n \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and a blank in the matrix denotes $0 \in \mathbb{F}_q$. The public key (DPVS basis) is $\mathbb{B} := \begin{pmatrix} \boldsymbol{b}_1 \\ \vdots \\ \boldsymbol{b}_n \end{pmatrix} := \begin{pmatrix} \mu G & & & \mu'_1 G \\ & \ddots & & \vdots \\ & & \mu G & \mu'_{n-1} G \\ & & & \mu'_n G \end{pmatrix}$. Let a ciphertext associated with $\Gamma := \{x_1, \ldots, x_{n'}\}$ be $\boldsymbol{c}_1 := (\omega \vec{y})_{\mathbb{B}} = \omega(y_1 \boldsymbol{b}_1 + \cdots + y_n \boldsymbol{b}_n) = (y_1 \omega \mu G, \ldots, y_{n-1} \omega \mu G,\ \omega(\sum_{i=1}^n y_i \mu'_i) G)$, where $\omega \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and $\vec{y} := (y_1, \ldots, y_n)$ 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, $\boldsymbol{c}_1$ 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 $\boldsymbol{c}_1$ can be obtained by $(y_1C_1, \ldots, y_{n-1}C_1, C_2)$ (note that $y_iC_1 = y_i\omega\mu G$ for $i = 1, \ldots, n-1$). That is, a ciphertext (excluding $\vec{y}$) can be just two group elements, or the size is constant in n.

Let $\mathbb{B}^* := (\boldsymbol{b}^*_i)$ be the dual orthonormal basis of $\mathbb{B} := (\boldsymbol{b}_i)$, and $\mathbb{B}^*$ be the master secret key in the simplified KP-ABE scheme. We specify $(\boldsymbol{c}_0, \boldsymbol{k}^*_0, c_T)$ such that $e(\boldsymbol{c}_0, \boldsymbol{k}^*_0) = g_T^{\zeta-\omega s_0}$ and $c_T := g_T^{\zeta} m \in \mathbb{G}_T$ with s_0 is a center secret of shares $\{s_i\}_{i=1,\ldots,\ell}$ associated with access structure $\mathbb{S}$. Using $\{s_i\}_{i=1,\ldots,\ell}$, we also set a secret key for $\mathbb{S}$ as $\boldsymbol{k}^*_i := (s_i\vec{e}_1 + \theta_i\vec{v}_i)_{\mathbb{B}^*}$ if $\rho(i) = v_i$ and $\boldsymbol{k}^*_i := (s_i\vec{v}_i)_{\mathbb{B}^*}$ if $\rho(i) = \neg v_i$ where $\vec{v}_i := (v_i^{n-1}, \ldots, v_i, 1)$ and $\theta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$. From the dual orthonormality of $\mathbb{B}$ and $\mathbb{B}^*$, if $\mathbb{S}$ accepts Γ, there exist a system of coefficients $\{\alpha_i\}_{i\in I}$ such that $e(\boldsymbol{c}_1, \widetilde{\boldsymbol{k}}^*) = g_T^{\omega s_0}$, where $\widetilde{\boldsymbol{k}}^* := \sum_{i\in I \wedge \rho(i)=v_i} \alpha_i \boldsymbol{k}^*_i + \sum_{i\in I \wedge \rho(i)=\neg v_i} \alpha_i(\vec{y}\cdot\vec{v}_i)^{-1}\boldsymbol{k}^*_i$. 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 $\boldsymbol{c}_1$ is expressed as $(y_1C_1, \ldots, y_{n-1}C_1, C_2) \in \mathbb{G}^n$ and $\widetilde{\boldsymbol{k}}^*$ is parsed as a n-tuple $(D^*_1, \ldots, D^*_n) \in \mathbb{G}^n$, the value of $e(\boldsymbol{c}_1, \widetilde{\boldsymbol{k}}^*)$ 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 $e(\boldsymbol{c}_1, \widetilde{\boldsymbol{k}}^*)$. 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 (resp. semi-adaptive) 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, $\boldsymbol{k}^*_i := (\ s_i\vec{e}_1 + \theta_i\vec{v}_i,\ 0^{2n},\ \vec{\eta}_i,\ 0^n\ )_{\mathbb{B}^*_1}$ if $\rho(i) = v_i$, $\boldsymbol{k}^*_i := (\ s_i\vec{v}_i,\ 0^{2n},\ \vec{\eta}_i,\ 0^n\ )_{\mathbb{B}^*_1}$ if $\rho(i) = \neg v_i$, $\boldsymbol{c}_1 = (\ \omega\vec{y}, 0^{2n}, 0^{2n}, \varphi_1\vec{y}\ )_{\mathbb{B}_1}$, 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 4, 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 4), which enables a *random-self-reducibility* argument for reducing the intractability of Problem 1 in Definition 10 to the DLIN assumption. For the reduction, see [24]. The property that $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ is a *subgroup* of $GL(n, \mathbb{F}_q)$ is also crucial for a special form of pairwise independence lemma in this paper (Lemma 3), where a super-group $\mathcal{H}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q) (\supset \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q))$ is specified in $\mathcal{L}(6, n, \mathbb{F}_q)$ or X. Our Problem 1 employs the special form matrices $\{U_j \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)\}$ and $\{Z_j := (U_j^{-1})^{\mathrm{T}}\}$, and makes Lemma 3 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 $\mathbb{F}_q^n \setminus \mathsf{span}\langle\vec{e}_n\rangle^{\perp}$ with preserving the inner-product value, $\vec{y}\cdot\vec{v}$, i.e., $\vec{v}Z$ reveal no information but ($\vec{y}$ and) $\vec{y}\cdot\vec{v}$.

5.2 Dual Orthonormal Basis Generator

We describe random dual orthonormal basis generator $\mathcal{G}_{\mathsf{ob}}^{\mathsf{KP\text{-}ABE}}$ using a sparse matrix given by Eq. (3), which is used in the proposed KP-ABE scheme.

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

Remark 2 Let

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

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., $e(\boldsymbol{b}_{1,i}, \boldsymbol{b}^*_{1,i}) = g_T$ and $e(\boldsymbol{b}_{1,i}, \boldsymbol{b}^*_{1,j}) = 1$ for $1 \le i \ne j \le 6n$.

5.3 Construction

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

$$
\begin{aligned}
&\mathsf{Setup}(1^\lambda, \ n):\\
&(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n}, \mathbb{B}^*_1) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}^{\mathsf{KP\text{-}ABE}}(1^\lambda, \ 6, \ n)),\\
&\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}),\\
&\widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, \ldots, \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,5n+1}, \ldots, \boldsymbol{b}_{1,6n}) = \{B_{i,j}, B'_{i,j,l}\}_{i=1,6;j=1,\ldots,6;l=1,\ldots,n},\\
&\widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,3}, \boldsymbol{b}^*_{0,4}), \ \ \widehat{\mathbb{B}}^*_1 := (\boldsymbol{b}^*_{1,1}, \ldots, \boldsymbol{b}^*_{1,n}, \boldsymbol{b}^*_{1,3n+1}, \ldots, \boldsymbol{b}^*_{1,5n}),\\
&\mathsf{pk} := (1^\lambda, \mathsf{param}_n, \{\widehat{\mathbb{B}}_t\}_{t=0,1}), \ \ \mathsf{sk} := \{\widehat{\mathbb{B}}^*_t\}_{t=0,1}, \quad \text{return } \ \mathsf{pk}, \ \mathsf{sk}.\\
&\mathsf{KeyGen}(\mathsf{pk}, \ \mathsf{sk}, \ \mathbb{S} := (M, \rho)):\\
&\vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r, \ \vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}, \ s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}, \ \eta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
&\boldsymbol{k}^*_0 := (-s_0, \ 0, \ 1, \ \eta_0, \ 0)_{\mathbb{B}^*_0},\\
&\text{for } i = 1, \ldots, \ell, \quad \vec{v}_i := (v_i^{n-1}, \ldots, v_i, 1) \text{ for } \rho(i) = v_i \text{ or } \neg v_i, \ \vec{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n},\\
&\text{if } \rho(i) = v_i, \ \theta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q, \ \boldsymbol{k}^*_i := \ (\ \overbrace{s_i\vec{e}_1 + \theta_i\vec{v}_i}^{n}, \ \overbrace{0^{2n}}^{2n}, \ \overbrace{\vec{\eta}_i}^{2n}, \ \overbrace{0^n}^{n} \ )_{\mathbb{B}^*_1},
\end{aligned}
$$

if $\rho(i) = \neg v_i$, $\boldsymbol{k}_i^* := (\overbrace{\quad}^{n}\ s_i\vec{v}_i, \overbrace{\quad}^{2n}\ 0^{2n}, \overbrace{\quad}^{2n}\ \vec{\eta}_i, \overbrace{\quad}^{n}\ 0^n)_{\mathbb{B}_1^*}$,

return $\mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{k}_0^*, \boldsymbol{k}_1^*, \ldots, \boldsymbol{k}_\ell^*)$.

$\mathsf{Enc}(\mathsf{pk},\ m,\ \Gamma := \{x_1, \ldots, x_{n'} \mid x_j \in \mathbb{F}_q^\times,\ n' \leq n-1\}) : \omega, \varphi_0, \varphi_1, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

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

$\boldsymbol{c}_0 := (\omega,\ 0,\ \zeta,\ 0,\ \varphi_0)_{\mathbb{B}_0}$,

$C_{1,j} := \omega B_{1,j} + \varphi_1 B_{6,j}$, $C_{2,j} := \sum_{l=1}^{n} y_l (\omega B'_{1,j,l} + \varphi_1 B'_{6,j,l})$ for $j = 1, .., 6$,

$c_T := g_T^\zeta m$, $\mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{C_{1,j}, C_{2,j}\}_{j=1,\ldots,6}, c_T)$. return ct_Γ.

$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{k}_0^*, \boldsymbol{k}_1^*, \ldots, \boldsymbol{k}_\ell^*),\ \mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{C_{1,j}, C_{2,j}\}_{j=1,\ldots,6}, c_T)) :$

If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{x_1, \ldots, x_{n'}\}$, 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
$I \subseteq \{i \in \{1, \ldots, \ell\} \mid [\rho(i) = v_i \wedge v_i \in \Gamma] \vee [\rho(i) = \neg v_i \wedge v_i \notin \Gamma]\}$,

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

$$(D_1^*, \ldots, D_{6n}^*) := \sum_{i \in I \ \wedge\ \rho(i) = v_i} \alpha_i \boldsymbol{k}_i^* + \sum_{i \in I \ \wedge\ \rho(i) = \neg v_i} \frac{\alpha_i}{\vec{v}_i \cdot \vec{y}} \boldsymbol{k}_i^*,$$

$E_j^* := \sum_{l=1}^{n-1} y_l D_{(j-1)n+l}^*$ for $j = 1, \ldots, 6$,

$K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \cdot \prod_{j=1}^{6} \left(e(C_{1,j}, E_j^*) \cdot e(C_{2,j}, D_{jn}^*) \right)$, return $m' := c_T / K$.

Remark 3 A part of the output of $\mathsf{Setup}(1^\lambda, n)$, $\{B_{i,j}, B'_{i,j,l}\}_{i=1,6; j=1,..,6; l=1,..,n}$, can be identified with $\widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, \ldots, \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,5n+1}, .., \boldsymbol{b}_{1,6n})$ through the form of Eq. (4), while $\mathbb{B}_1 := (\boldsymbol{b}_{1,1}, \ldots, \boldsymbol{b}_{1,6n})$ is identified with $\{B_{i,j}, B'_{i,j,l}\}_{i,j=1,..,6;\, l=1,..,n}$ by Eq. (4). Decryption Dec can be alternatively described as:

$\mathsf{Dec}'(\mathsf{pk},\ \mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{k}_0^*, \boldsymbol{k}_1^*, \ldots, \boldsymbol{k}_\ell^*),\ \mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{C_{1,j}, C_{2,j}\}_{j=1,\ldots,6}, c_T)) :$

If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{x_1, \ldots, x_{n'}\}$, 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
$I \subseteq \{i \in \{1, \ldots, \ell\} \mid [\rho(i) = v_i \wedge v_i \in \Gamma] \vee [\rho(i) = \neg v_i \wedge v_i \notin \Gamma]\}$,

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

$$\boldsymbol{c}_1 := (\overbrace{\begin{matrix} y_1 C_{1,1}, .., y_{n-1} C_{1,1}, C_{2,1}, \\ y_1 C_{1,5}, .., y_{n-1} C_{1,5}, C_{2,5}, \end{matrix}}^{n} \overbrace{\begin{matrix} y_1 C_{1,2}, .., y_{n-1} C_{1,2}, C_{2,2}, \\ y_1 C_{1,6}, .., y_{n-1} C_{1,6}, C_{2,6} \end{matrix}}^{n} \cdots),$$

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

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

return $m' := c_T / K$.

[**Correctness**] If $\mathbb{S}$ accepts Γ, $e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) e(\boldsymbol{c}_1, \sum_{i \in I \wedge \rho(i) = v_i} \alpha_i \boldsymbol{k}_i^*) \cdot e(\boldsymbol{c}_1, \sum_{i \in I \wedge \rho(i) = \neg v_i} \frac{\alpha_i}{\vec{v}_i \cdot \vec{y}} \boldsymbol{k}_i^*)$
$= g_T^{-\omega s_0 + \zeta} \prod_{i \in I \wedge \rho(i) = v_i} g_T^{\omega \alpha_i s_i} \prod_{i \in I \wedge \rho(i) = \neg v_i} g_T^{\omega \alpha_i s_i (\vec{v}_i \cdot \vec{y}) / (\vec{v}_i \cdot \vec{y})} = g_T^{\omega(-s_0 + \sum_{i \in I} \alpha_i s_i) + \zeta} = g_T^\zeta$.

6 Security of the Proposed KP-ABE

6.1 Theorem 1

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

For any adversary $\mathcal{A}$, there is probabilistic machines $\mathcal{F}_1, \mathcal{F}_2$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{KP\text{-}ABE,SA}}(\lambda) \leq \mathsf{Adv}_{\mathcal{F}_{1\text{-}1}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_{1\text{-}2}}^{\mathsf{DLIN}}(\lambda) + \sum_{j=1}^{n} \left(\mathsf{Adv}_{\mathcal{F}_{2\text{-}j\text{-}1}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_{2\text{-}j\text{-}2}}^{\mathsf{DLIN}}(\lambda) \right) + \epsilon,$$

where $\mathcal{F}_{1\text{-}\iota}(\cdot) := \mathcal{F}_1(\iota, \cdot)$ and $\mathcal{F}_{2\text{-}j\text{-}\iota}(\cdot) := \mathcal{F}_2(j, \iota, \cdot)$ for $j = 1, \ldots, n$; $\iota = 1, 2$, $\epsilon := (3\nu\hat{\ell} + 10n + 10)/q$, and ν is the maximum number of $\mathcal{A}$'s key queries, $\hat{\ell}$ is the maximum number of rows in access matrices of key queries.

6.2 Proof of Theorem 1

Outline : At the top level strategy of the security proof, the dual system encryption by Waters [32] 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. Additionally, several temporary forms for keys are introduced as defined below.

To prove this theorem, we employ Game 0 (original semi-adaptive security game) through Game 4. In Game 1, the challenge ciphertext are changed to semi-functional form, and and all queried keys are changed to temporary-0 form. In Game 2-j-ι ($j = 1, \ldots, n$; $\iota = 1, 2$), all queried keys are changed to temporary-j-ι form, then, in In Game 3, they are all changed to semi-functional form. In Game 4, 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.

We have shown that the intractability of (complicated) Problems 1 and 2 is reduced to that of the DLIN Problem through several intermediate steps, or intermediate problems, as in [23]. The vertical reductions are also indicated in Figure 1. The reduction steps indicated by dotted arrows can be shown in the same manner as those in the full version of [23].

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. (9). A temporary-0 key is expressed by Eqs. (7) and (8). A temporary-j-1 (resp. j-2) key is expressed by Eqs. (7) and (10) (resp. Eqs. (7) and (11)) as well as Eq. (8) for matching attributes $v_{h,i}$. A semi-functional key is expressed by Eq. (12) and Eq. (8) for matching attributes $v_{h,i}$. A non-functional ciphertext is expressed by Eq. (13) (with $\boldsymbol{c}_1$ in Eq. (9)).

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 $\beta \xleftarrow{\mathsf{U}} \{0, 1\}$ 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 7). The advantage of Problem 1 is proven to be equivalent to twice of that of the DLIN assumption (Lemma 5). Game 2-0-2 is Game 1. Similarly, we show that the advantage gap between Games 2-($j-1$)-2 and 2-j-1 for $j = 1, \ldots, n$ is equivalent to the advantage of Problem 2 (Lemma 8),

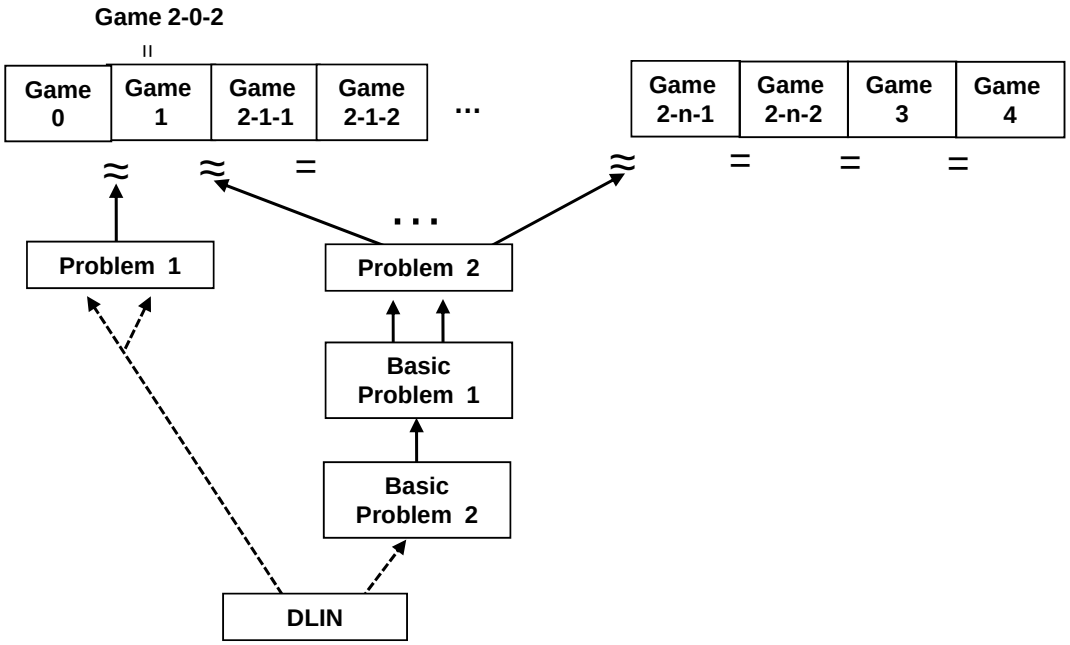


Figure 1: Structure of Reductions for the Proof of Theorem 1.

and then twice of that of the DLIN assumption (Lemma 6). We then show that Game 2-j-1 can be conceptually changed to Game 2-j-2 (Lemma 9), by using the fact that parts of bases, $\boldsymbol{b}_{1,2n+1}, \ldots, \boldsymbol{b}_{1,3n}$ and $\boldsymbol{b}^*_{1,2n+1}, \ldots, \boldsymbol{b}^*_{1,3n}$, are unknown to the adversary.

We then show that Game 2-n-2 can be conceptually changed to Game 3 (Lemma 10), by using our modified pairwise independence lemma (Lemma 3) and the information-theoretical security property of secret sharing. Finally, Game 3 can be conceptually changed to Game 4 (Lemma 11) by using the fact that parts of bases, $\boldsymbol{b}_{0,2}$ and $\boldsymbol{b}^*_{0,3}$, 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 $\boldsymbol{b}_{0,2}$ and $\boldsymbol{b}^*_{0,2}$ are random.

6.2.1 Proof of Theorem 1

To prove Theorem 1, we consider the following $2n + 4$ 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.

For notational simplicity, we use ℓ ($:= \ell_h$) for the number of rows of any key queries below.

Game 0 : Original game. That is, the reply to the h-th key query for $\mathbb{S}_h := (M_h, \rho_h)$ $(h = 1, \ldots, \nu)$ is:

$$\left.\begin{array}{l} \boldsymbol{k}^*_{h,0} := (-s_{h,0},\ \boxed{0},\ 1,\ \eta_{h,0},\ 0)_{\mathbb{B}^*_0}, \\ \quad \text{for } i = 1, \ldots, \ell, \\ \quad\quad \text{if } \rho_h(i) = v_{h,i}, \quad \boldsymbol{k}^*_{h,i} := (\ \overbrace{s_{h,i}\vec{e}_1 + \theta_{h,i}\vec{v}_{h,i},}^{n}\ \overbrace{\boxed{0^{2n}},}^{2n}\ \overbrace{\vec{\eta}_{h,i},}^{2n}\ \overbrace{0^n}^{n}\ )_{\mathbb{B}^*_1}, \\ \quad\quad \text{if } \rho_h(i) = \neg v_{h,i}, \quad \boldsymbol{k}^*_{h,i} := (\ s_{h,i}\vec{v}_{h,i},\ \boxed{0^{2n}},\ \vec{\eta}_{h,i},\ 0^n\ )_{\mathbb{B}^*_1}, \end{array}\right\} \quad (5)$$

where $\vec{f}_h \xleftarrow{\cup} \mathbb{F}_q^r$, $\vec{s}_h^{\mathrm{T}} := (s_{h,1}, \ldots, s_{h,\ell})^{\mathrm{T}} := M_h \cdot \vec{f}_h^{\mathrm{T}}$, $s_{h,0} := \vec{1} \cdot \vec{f}_h^{\mathrm{T}}, \theta_{h,i}, \eta_{h,0} \xleftarrow{\cup} \mathbb{F}_q, \vec{\eta}_{h,i} \xleftarrow{\cup} \mathbb{F}_q^{2n}, \vec{e}_1 := (1, 0, \ldots, 0) \in \mathbb{F}_q^n$, and $\vec{v}_{h,i} := (v_{h,i}^{n-1}, \ldots, v_{h,i}, 1) \in (\mathbb{F}_q^\times)^n$. The challenge ciphertext

for challenge plaintexts $(m^{(0)}, m^{(1)})$ and $\Gamma := \{x_j\}$ is:

$$\left.\begin{array}{l} \boldsymbol{c}_0 := (\omega,\ \boxed{0},\ \boxed{\zeta},\ 0,\ \varphi_0)_{\mathbb{B}_0}, \\ \boldsymbol{c}_1 := \ (\ \overbrace{\omega\vec{y},}^{n}\ \overbrace{\boxed{0^{2n}},}^{2n}\ \overbrace{0^{2n},}^{2n}\ \overbrace{\varphi_1\vec{y}}^{n}\ )_{\mathbb{B}_1}, \\ c_T := g_T^{\zeta} m^{(b)}, \end{array}\right\} \quad (6)$$

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

Game 1 : Same as Game 0 except that the reply to the h-th key query for $\mathbb{S}_h := (M_h, \rho_h)$ is:

$$\boldsymbol{k}^*_{h,0} := (-s_{h,0},\ \boxed{-r_{h,0}},\ 1,\ \eta_{h,0},\ 0)_{\mathbb{B}^*_0}, \quad (7)$$

$$\left.\begin{array}{l} \text{for } i = 1, \ldots, \ell, \\ \quad \text{if } \rho_h(i) = v_{h,i}, \quad \boldsymbol{k}^*_{h,i} := (\ \overbrace{s_{h,i}\vec{e}_1 + \theta_{h,i}\vec{v}_{h,i},}^{n}\ \overbrace{\boxed{r_{h,i}\vec{e}_1 + \widetilde{\theta}_{h,i}\vec{v}_{h,i}},\ 0^n,}^{2n}\ \overbrace{\vec{\eta}_{h,i},}^{2n}\ \overbrace{0^n}^{n}\ )_{\mathbb{B}^*_1}, \\ \quad \text{if } \rho_h(i) = \neg v_{h,i}, \quad \boldsymbol{k}^*_{h,i} := (\ s_{h,i}\vec{v}_{h,i},\ \boxed{r_{h,i}\vec{v}_{h,i}},\ 0^n,\ \vec{\eta}_{h,i},\ 0^n\ )_{\mathbb{B}^*_1}, \end{array}\right\} \quad (8)$$

where $\vec{g}_h \xleftarrow{\cup} \mathbb{F}_q^r$, $\vec{r}_h^{\mathrm{T}} := (r_{h,1}, \ldots, r_{h,\ell})^{\mathrm{T}} := M_h \cdot \vec{g}_h^{\mathrm{T}}$, $r_{h,0} := \vec{1} \cdot \vec{g}_h^{\mathrm{T}}$, $\widetilde{\theta}_{h,i} \xleftarrow{\cup} \mathbb{F}_q$. The challenge ciphertext is:

$$\left.\begin{array}{l} \boldsymbol{c}_0 := (\omega,\ \boxed{\tau},\ \zeta,\ 0,\ \varphi_0)_{\mathbb{B}_0}, \\ \boldsymbol{c}_1 := \ (\ \overbrace{\omega\vec{y},}^{n}\ \overbrace{\boxed{\tau\vec{y},\ \tau\vec{y},}}^{2n}\ \overbrace{0^{2n},}^{2n}\ \overbrace{\varphi_1\vec{y}}^{n}\ )_{\mathbb{B}_1}, \\ c_T := g_T^{\zeta} m, \end{array}\right\} \quad (9)$$

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

Game 2-j-1 ($j = 1, \ldots, n$) : Game 2-0-2 is Game 1. Game 2-j-1 is the same as Game 2-$(j-1)$-2 except the reply to the h-th key query for $\mathbb{S}_h := (M_h, \rho_h)$ are: for $i = 1, \ldots, \ell$,

$$\left.\begin{array}{l} \text{if } \rho_h(i) = v_{h,i} \ \wedge\ v_{h,i} \notin \Gamma, \\ \quad \boldsymbol{k}^*_{h,i} := \ (\ \overbrace{s_{h,i}\vec{e}_1 + \theta_{h,i}\vec{v}_{h,i},}^{n} \\ \qquad \overbrace{\boxed{\xi_{h,i,j+1}}(r_{h,i}\vec{e}_1 + \widetilde{\theta}_{h,i}\vec{v}_{h,i}),\ (r_{h,i}\vec{e}_1 + \widetilde{\theta}_{h,i}\vec{v}_{h,i}) \cdot \boxed{(\sum_{\kappa=1}^{j-1} \xi_{h,i,\kappa} Z_\kappa + \xi_{h,i,j} I_n)},}^{2n}\ \overbrace{\vec{\eta}_{h,i},}^{2n}\ \overbrace{0^n}^{n}\ )_{\mathbb{B}^*_1}, \\ \text{if } \rho_h(i) = \neg v_{h,i} \ \wedge\ v_{h,i} \in \Gamma, \\ \quad \boldsymbol{k}^*_{h,i} := \ (\ \overbrace{s_{h,i}\vec{v}_{h,i},}^{n}\ \overbrace{\boxed{\xi_{h,i,j+1}}\, r_{h,i}\vec{v}_{h,i},\ r_{h,i}\vec{v}_{h,i} \cdot \boxed{(\sum_{\kappa=1}^{j-1} \xi_{h,i,\kappa} Z_\kappa + \xi_{h,i,j} I_n)},}^{2n}\ \overbrace{\vec{\eta}_{h,i},}^{2n}\ \overbrace{0^n}^{n}\ )_{\mathbb{B}^*_1}, \end{array}\right\} \quad (10)$$

where $(\xi_{h,i,\kappa})_{\kappa=1,\ldots,j+1} \xleftarrow{\cup} \{(\xi_\kappa)_{\kappa=1,\ldots,j+1} \in \mathbb{F}_q^{j+1} \mid \sum_{i=1}^{j+1} \xi_i = 1 \ \wedge\ \xi_{n+1} = 0 \text{ if } j = n\}$ for $j = 0, \ldots, n$ and all the other variables are generated as in Game 2-$(j-1)$-2. Note that since $\xi_{h,1} = 1$ (and other $\xi_{h,\kappa} = 0$) when $j = 0$, the above distribution is equivalent to that in Game 1 (= Game 2-0-2).

Game 2-j-2 ($j = 1, \ldots, n$) : Game 2-j-2 is the same as Game 2-j-1 except the reply to the h-th key query for $\mathbb{S}_h := (M_h, \rho_h)$ are: for $i = 1, \ldots, \ell$,

$$\left.\begin{array}{l}
\text{if } \rho_h(i) = v_{h,i} \ \wedge \ v_{h,i} \notin \Gamma, \\
\boldsymbol{k}^*_{h,i} := \ (\ \overbrace{s_{h,i}\vec{e}_1 + \theta_{h,i}\vec{v}_{h,i}}^{n}, \\
\qquad \overbrace{\xi_{h,i,j+1}(r_{h,i}\vec{e}_1 + \widetilde{\theta}_{h,i}\vec{v}_{h,i}), \ (r_{h,i}\vec{e}_1 + \widetilde{\theta}_{h,i}\vec{v}_{h,i}) \cdot \boxed{(\textstyle\sum_{\kappa=1}^{j} \xi_{h,i,\kappa} Z_\kappa)}}^{2n}, \ \overbrace{\vec{\eta}_{h,i}}^{2n}, \ \overbrace{0^n}^{n} \ )_{\mathbb{B}^*_1}, \\
\text{if } \rho_h(i) = \neg v_{h,i} \ \wedge \ v_{h,i} \in \Gamma, \\
\boldsymbol{k}^*_{h,i} := \ (\ \overbrace{s_{h,i}\vec{v}_{h,i}}^{n}, \ \overbrace{\xi_{h,i,j+1} \ r_{h,i}\vec{v}_{h,i}, \ r_{h,i}\vec{v}_{h,i} \cdot \boxed{(\textstyle\sum_{\kappa=1}^{j} \xi_{h,i,\kappa} Z_\kappa)}}^{2n}, \ \overbrace{\vec{\eta}_{h,i}}^{2n}, \ \overbrace{0^n}^{n} \ )_{\mathbb{B}^*_1},
\end{array}\right\} (11)$$

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

Game 3 : Game 3 is the same as Game 2-n-2 except the i-th component of the reply to the h-th key query for $\mathbb{S}_h := (M_h, \rho_h)$ are:

$$\left.\begin{array}{l}
\boldsymbol{k}^*_0 := (-s_{h,0}, \ \boxed{w_{h,0}}, \ 1, \ \eta_{h,0}, \ 0)_{\mathbb{B}^*_0}, \\
\text{for } i = 1, \ldots, \ell, \qquad \overbrace{\phantom{s_{h,i}\vec{e}_1 + \theta_{h,i}\vec{v}_{h,i},}}^{n} \ \overbrace{}^{2n} \ \overbrace{\phantom{\vec{\eta}_{h,i},}}^{2n} \ \overbrace{}^{n} \\
\quad \text{if } \rho_h(i) = v_{h,i} \wedge v_{h,i} \notin \Gamma, \ \boldsymbol{k}^*_{h,i} := (\quad s_{h,i}\vec{e}_1 + \theta_{h,i}\vec{v}_{h,i}, \quad 0^n, \ \boxed{\vec{w}_{h,i}}, \quad \vec{\eta}_{h,i}, \quad 0^n \quad)_{\mathbb{B}^*_1}, \\
\quad \text{if } \rho_h(i) = \neg v_{h,i} \wedge v_{h,i} \in \Gamma, \ \ \boldsymbol{k}^*_{h,i} := (\quad s_{h,i}\vec{v}_{h,i}, \qquad 0^n, \ \boxed{\vec{\overline{w}}_{h,i}}, \quad \vec{\eta}_{h,i}, \quad 0^n \quad)_{\mathbb{B}^*_1},
\end{array}\right\} (12)$$

where $w_{h,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{w}_{h,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, $\vec{\overline{w}}_{h,i} \xleftarrow{\mathsf{U}} \mathsf{span}\langle\vec{y}\rangle^\perp$, and all the other variables are generated as in Game 2-n-2.

Game 4 : Same as Game 3 except that $\boldsymbol{c}_0$ and c_T of the challenge ciphertext are

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

where $\zeta' \xleftarrow{\mathsf{U}} \mathbb{F}_q$ (i.e., independent from $\zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$), and all the other variables are generated as in Game 3.

Let $\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda), \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda), \mathsf{Adv}^{(2\text{-}j\text{-}\iota)}_{\mathcal{A}}(\lambda), \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)$ and $\mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda)$ be the advantage of $\mathcal{A}$ in Game $0, 1, 2\text{-}j\text{-}\iota, 3$ and 4, respectively. $\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda)$ is equivalent to $\mathsf{Adv}^{\mathsf{KP\text{-}ABE,SA}}_{\mathcal{A}}(\lambda)$ and it is clear that $\mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda) = 0$ by Lemma 12.

We will show five lemmas (Lemmas 7-11) that evaluate the gaps between pairs of the advantages in Game 0, ..., Game 4. From these lemmas and Lemmas 5–3, we obtain $\mathsf{Adv}^{\mathsf{KP\text{-}ABE,SA}}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}2}}(\lambda) + \sum_{j=1}^{n} \left(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}j\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}j\text{-}2}}(\lambda) \right) + \epsilon$, where $\epsilon := (3\nu\hat{\ell} + 10n + 10)/q$. This completes the proof of Theorem 1. □

6.2.2 Lemmas

Definition 10 (Problem 1) *Problem 1 is to guess β, given* $(\mathsf{param}_n, \{\mathbb{B}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,1}, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_{\beta,i}\}_{i=0,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_\beta(1^\lambda, n)$, *where*

$$\begin{array}{l}
\mathcal{G}^{\mathsf{P1}}_\beta(1^\lambda, n): \quad (\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n}, \mathbb{B}^*_1) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{KP\text{-}ABE}}_{\mathsf{ob}}(1^\lambda, 6, n), \\
\quad \mathbb{B}_1 := (\boldsymbol{b}_{1,1}, \ldots, \boldsymbol{b}^*_{1,6n}) \text{ is calculated from } \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n},
\end{array}$$

$\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*, \ldots, \boldsymbol{b}_{0,5}^*)$, $\widehat{\mathbb{B}}_1^* := (\boldsymbol{b}_{1,1}^*, \ldots, \boldsymbol{b}_{1,n}^*, \boldsymbol{b}_{1,3n+1}^*, \ldots, \boldsymbol{b}_{1,6n}^*)$,
$\delta, \delta_0, \omega, \varphi_\iota \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\tau, \rho \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times$ for $\iota = 0, 1$,
$\boldsymbol{h}_{0,0}^* := (\delta, 0, 0, \delta_0, 0)_{\mathbb{B}_0^*}$, $\boldsymbol{h}_{1,0}^* := (\delta, \rho, 0, \delta_0, 0)_{\mathbb{B}_0^*}$, $\boldsymbol{e}_{0,0} := (\omega, 0, 0, 0, \varphi_0)_{\mathbb{B}_0}$, $\boldsymbol{e}_{1,0} := (\omega, \tau, 0, 0, \varphi_0)_{\mathbb{B}_0}$,
for $i = 1, \ldots, n$; $\vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n$, $\vec{\delta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n}$,

$$
\begin{array}{lcccccc}
 & & \overbrace{\phantom{\delta\vec{e}_i,}}^{n} & \overbrace{\phantom{0^{2n},}}^{2n} & \overbrace{\phantom{\vec{\delta}_i,}}^{2n} & \overbrace{}^{n} & \\
\boldsymbol{h}_{0,i}^* := & (& \delta\vec{e}_i, & 0^{2n}, & \vec{\delta}_i, & 0^n &)_{\mathbb{B}_1^*} \\
\boldsymbol{h}_{1,i}^* := & (& \delta\vec{e}_i, & \rho\vec{e}_i,\ 0^n, & \vec{\delta}_i, & 0^n &)_{\mathbb{B}_1^*} \\
\boldsymbol{e}_{0,i} := & (& \omega\vec{e}_i, & 0^{2n}, & 0^{2n}, & \varphi_1\vec{e}_i &)_{\mathbb{B}_1}, \\
\boldsymbol{e}_{1,i} := & (& \omega\vec{e}_i, & \tau\vec{e}_i,\ \tau\vec{e}_i, & 0^{2n}, & \varphi_1\vec{e}_i &)_{\mathbb{B}_1},
\end{array}
$$

return $(\mathsf{param}_n, \{\mathbb{B}_\iota, \widehat{\mathbb{B}}_\iota^*\}_{\iota=0,1}, \{\boldsymbol{h}_{\beta,i}^*, \boldsymbol{e}_{\beta,i}\}_{i=0,\ldots,n})$,

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

Lemma 5 *For any adversary $\mathcal{C}$, there exist probabilistic machines $\mathcal{F}_1$ and $\mathcal{F}_2$, whose running time are essentially the same as that of $\mathcal{C}$, such that for any security parameter λ,* $\mathsf{Adv}_{\mathcal{C}}^{\mathsf{P1}}(\lambda) \leq \mathsf{Adv}_{\mathcal{F}_1}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_2}^{\mathsf{DLIN}}(\lambda) + 10/q$.

Lemma 5 is proven in a similar manner to Lemmas 1 and 2 in [23]. □

Definition 11 (Problem 2) *Problem 2 is to guess β, given* $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \boldsymbol{f}_0^*, \boldsymbol{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}_1^*, \{\boldsymbol{f}_i^*\}_{i=1,\ldots,2n}, \{\boldsymbol{h}_{\beta,i}^*, \boldsymbol{e}_i\}_{i=1,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{P2}}(1^\lambda, n)$, *where*

$\mathcal{G}_\beta^{\mathsf{P2}}(1^\lambda, n)$: $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n}, \mathbb{B}_1^*) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}^{\mathsf{KP\text{-}ABE}}(1^\lambda, 6, n)$,
$\widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, .., \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,3n+1}, .., \boldsymbol{b}_{1,6n})$ is calculated from $\{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n}$,
$\tau, \rho \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times$, $\boldsymbol{f}_0^* := \rho\boldsymbol{b}_{0,2}^*$, $\boldsymbol{e}_0 := \tau\boldsymbol{b}_{0,2}$, $\boldsymbol{f}_i^* := \rho\boldsymbol{b}_{1,n+i}^*$ for $i = 1, \ldots, 2n$,
for $i = 1, \ldots, n$; $\vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n$, $\vec{\delta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n}$,

$$
\begin{array}{lcccccc}
 & & \overbrace{}^{n} & \overbrace{\phantom{\rho\vec{e}_i,\ 0^n,}}^{2n} & \overbrace{\phantom{\vec{\delta}_i,}}^{2n} & \overbrace{}^{n} & \\
\boldsymbol{h}_{0,i}^* := & (& 0^n, & \rho\vec{e}_i,\ 0^n, & \vec{\delta}_i, & 0^n &)_{\mathbb{B}_1^*} \\
\boldsymbol{h}_{1,i}^* := & (& 0^n, & 0^n,\ \rho\vec{e}_i, & \vec{\delta}_i, & 0^n &)_{\mathbb{B}_1^*} \\
\boldsymbol{e}_i := & (& 0^n, & \tau\vec{e}_i,\ \tau\vec{e}_i, & 0^{2n}, & 0^n &)_{\mathbb{B}_1},
\end{array}
$$

return $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \boldsymbol{f}_0^*, \boldsymbol{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}_1^*, \{\boldsymbol{f}_i^*\}_{i=1,\ldots,2n}, \{\boldsymbol{h}_{\beta,i}^*, \boldsymbol{e}_i\}_{i=1,\ldots,n})$,

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{B}$, the advantage of $\mathcal{C}$ for Problem 2, $\mathsf{Adv}_{\mathcal{C}}^{\mathsf{P2}}(\lambda)$, *is similarly defined as in Definition 10.*

Lemma 6 *For any adversary $\mathcal{C}$, there exist probabilistic machines $\mathcal{F}_1$ and $\mathcal{F}_2$, whose running times are essentially the same as that of $\mathcal{C}$, such that for any security parameter λ,* $\mathsf{Adv}_{\mathcal{C}}^{\mathsf{P2}}(\lambda) \leq \mathsf{Adv}_{\mathcal{F}_1}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_2}^{\mathsf{DLIN}}(\lambda) + 10/q$.

Lemma 7 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{C}_1$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,* $|\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{C}_1}^{\mathsf{P1}}(\lambda)$.

Lemma 8 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{C}_2$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(j-1)\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}j\text{-}1)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{C}_{2\text{-}j}}^{\mathsf{P2}}(\lambda)$, where $\mathcal{C}_{2\text{-}j}(\cdot) := \mathcal{C}_2(j, \cdot)$.*

Lemma 9 *For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}j\text{-}1)}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}j\text{-}2)}(\lambda)$.*

Lemma 10 *For any adversary $\mathcal{A}$, for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}n\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)| \leq 3\nu\hat{\ell}/q$, where ν is the maximum number of $\mathcal{A}$'s key queries, and $\hat{\ell}$ is the maximum number of rows in access matrices of key queries.*

Lemma 11 *For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)$.*

Lemma 12 *For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda) = 0$.*

6.3 Key Techniques

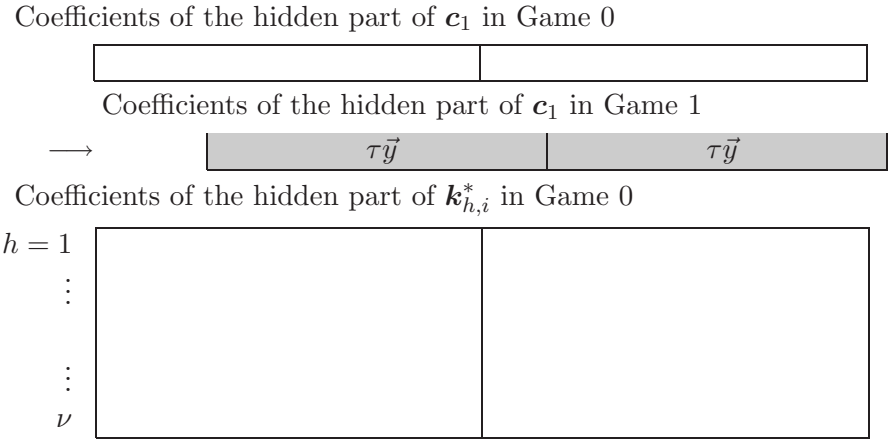
One of the aims of the above game changes is that values of shares $r_{h,i}$ for non-matching indices (h, i) (i.e., $(\rho_h(i) = v_{h,i} \wedge v_{h,i} \notin \Gamma) \vee (\rho_h(i) = \neg v_{h,i} \wedge v_{h,i} \in \Gamma)$) are made hidden from the adversary as in previous security proofs of ABE. For achieving it, random matrices $Z_{h,i} \in \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}$ are inserted in the hidden (or semi-functional) part of $\boldsymbol{k}^*_{h,i}$ for non-matching (h, i).

In high-level description, it is accomplished by the sequence of swaps and information-theoretical (conceptual) changes, similar techniques were used in [26]. Moreover, to generate random $Z_{h,i}$, we use both of additive and multiplicative structures of $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$. For the former (resp. latter), see Section 6.3.1 (resp. 6.3.2).

6.3.1 Iteration of Swaps and Conceptual Changes for Theorem 1

Theorem 1 is proven by the hybrid argument through $2n + 4$ games (given in Section 6.2).

First, in Game 0, coefficients of the hidden parts of $\boldsymbol{c}_1$ and $\boldsymbol{k}^*_{h,i}$ $(h = 1, \ldots, \nu; i = 1, \ldots, \ell)$ are all zero. Then, in the next Game 1, that of $\boldsymbol{c}_1$ is filled with $(\tau\vec{y}, \tau\vec{y}) \in \mathbb{F}_q^{2n}$ and the first n-dim. coefficient (block) of the hidden parts of $\boldsymbol{k}^*_{h,i}$ $(h = 1, \ldots, \nu)$ are changed to $\vec{p}_{h,i} \in \mathbb{F}_q^n$ such that $\vec{p}_{h,i} := r_{h,i}\vec{e}_1 + \widetilde{\psi}_{h,i}\vec{v}_{h,i}$ if $\rho_h(i) = v_{h,i}$, $\vec{p}_{h,i} := r_{h,i}\vec{v}_{h,i}$ if $\rho_h(i) = \neg v_{h,i}$, as: (Hereafter, we describe coefficients of the hidden part, i.e., $\mathsf{span}\langle \boldsymbol{b}_{1,n+1}, \ldots, \boldsymbol{b}_{1,3n} \rangle$ (resp. $\mathsf{span}\langle \boldsymbol{b}^*_{1,n+1}, \ldots, \boldsymbol{b}^*_{1,3n} \rangle$) of $\boldsymbol{c}_1$ (resp. $\boldsymbol{k}^*_{h,i}$ for *non-matching* (h, i)) and a blank indicates zero coefficients)



$$
\begin{array}{rc|c|c}
 & h=1 & \vec{p}_{1,i} & \\
 & \vdots & \vdots & \\
\longrightarrow & & & \\
 & \vdots & \vdots & \\
 & \nu & \vec{p}_{\nu,i} & \\
\hline
 & h=1 & \vec{p}_{1,i}\cdot(\sum_{\kappa=1}^{n}\xi_{1,i,\kappa}I_n) & \\
 & \vdots & \vdots & \\
= & & & \\
 & \vdots & \vdots & \\
 & \nu & \vec{p}_{\nu,i}\cdot(\sum_{\kappa=1}^{n}\xi_{\nu,i,\kappa}I_n) & \\
\end{array}
$$

Coefficients $\vec{p}_{h,i}$ in $\boldsymbol{k}^*_{h,i}$ is conceptually changed to $\vec{p}_{h,i}\cdot(\sum_{\kappa=1}^{n}\xi_{h,i,\kappa}I_n)$ using random coefficients $(\xi_{h,i,\kappa})_{\kappa=1,\ldots,n}$ with $\sum_{\kappa=1}^{n}\xi_{h,i,\kappa}=1$

After that, in turn for $j=1,\ldots,n$, the coefficient vector $\vec{p}_{h,i}\cdot\xi_{h,i,j}I_n\in\mathbb{F}_q^n$ is *swapped* to the second block of the hidden parts of $\boldsymbol{k}^*_{h,i}$ (for $h=1,\ldots,\nu; i=1,\ldots,\ell$) in Game 2-$j$-1 and the coefficient vector is *conceptually (information-theoretically) changed* to $\vec{p}_{h,i}\cdot\xi_{h,i,j}Z_j$ in Game 2-j-2 by a conceptual basis change. The swap can be securely executed under the DLIN assumption (through Problem 2). In Game 2-n-2, each $\vec{p}_{h,i}\cdot\xi_{h,i,\kappa}Z_\kappa$ ($\kappa=1,\ldots,n$) is added in the second block of hidden parts in $\boldsymbol{k}^*_{h,i}$.

Coefficients of the hidden part of $\boldsymbol{k}^*_{h,i}$ in Game 2-$(j-1)$-2

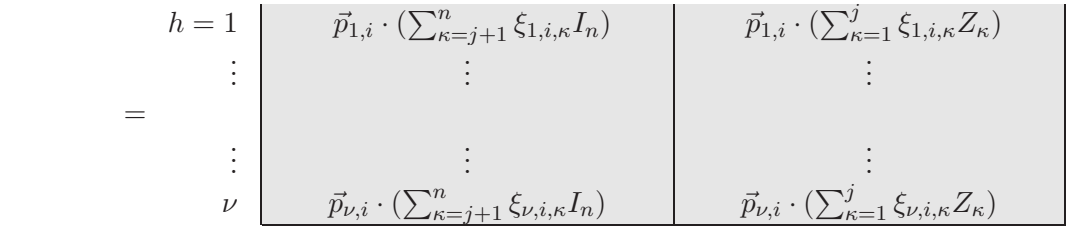
$$
\begin{array}{rc|c|c}
 & h=1 & \vec{p}_{1,i}\cdot(\sum_{\kappa=j}^{n}\xi_{1,i,\kappa}I_n) & \vec{p}_{1,i}\cdot(\sum_{\kappa=1}^{j-1}\xi_{1,i,\kappa}Z_\kappa) \\
 & \vdots & \vdots & \vdots \\
\longrightarrow\cdots\longrightarrow & & & \\
 & \vdots & \vdots & \vdots \\
 & \nu & \vec{p}_{\nu,i}\cdot(\sum_{\kappa=j}^{n}\xi_{\nu,i,\kappa}I_n) & \vec{p}_{\nu,i}\cdot(\sum_{\kappa=1}^{j-1}\xi_{\nu,i,\kappa}Z_\kappa)
\end{array}
$$

Coefficients of the hidden part of $\boldsymbol{k}^*_{h,i}$ in Game 2-j-1

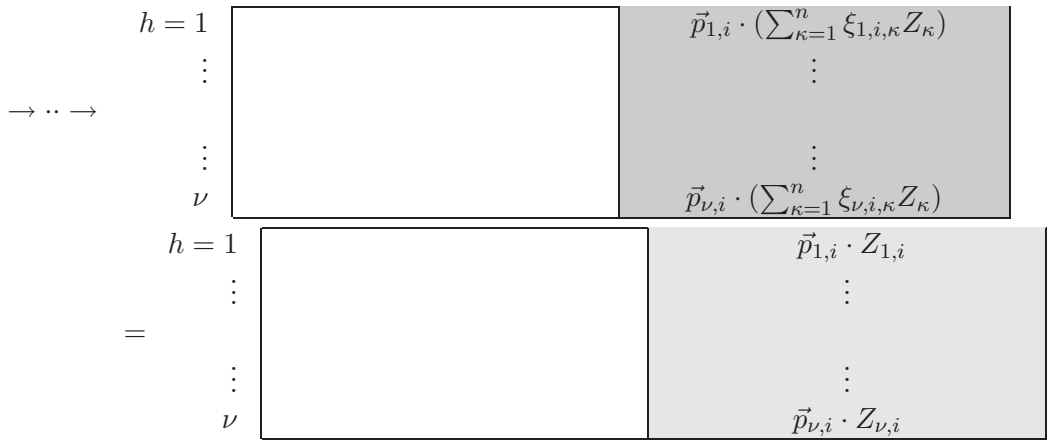
$$
\begin{array}{rc|c|c}
 & h=1 & \vec{p}_{1,i}\cdot(\sum_{\kappa=j+1}^{n}\xi_{1,i,\kappa}I_n) & \vec{p}_{1,i}\cdot(\sum_{\kappa=1}^{j-1}\xi_{1,i,\kappa}Z_\kappa+\xi_{1,i,j}I_n) \\
\text{swap } \vec{p}_{h,i}\cdot\xi_{h,i,j}I_n & \vdots & \vdots & \vdots \\
\longrightarrow & & & \\
 & \vdots & \vdots & \vdots \\
 & \nu & \vec{p}_{\nu,i}\cdot(\sum_{\kappa=j+1}^{n}\xi_{\nu,i,\kappa}I_n) & \vec{p}_{\nu,i}\cdot(\sum_{\kappa=1}^{j-1}\xi_{\nu,i,\kappa}Z_\kappa+\xi_{\nu,i,j}I_n)
\end{array}
$$

Coefficients of the hidden part of $\boldsymbol{k}^*_{h,i}$ in Game 2-j-2

$$
\begin{array}{rc|c|c}
 & h=1 & \vec{p}_{1,i}\cdot(\sum_{\kappa=j+1}^{n}\xi_{1,i,\kappa}I_n) & \vec{p}_{1,i}\cdot(\sum_{\kappa=1}^{j-1}\xi_{1,i,\kappa}Z_\kappa+\xi_{1,i,j}Z_j) \\
\text{change } \xi_{h,i,j}I_n \text{ to } \xi_{h,i,j}Z_j & \vdots & \vdots & \vdots \\
\longrightarrow & & & \\
 & \vdots & \vdots & \vdots \\
 & \nu & \vec{p}_{\nu,i}\cdot(\sum_{\kappa=j+1}^{n}\xi_{\nu,i,\kappa}I_n) & \vec{p}_{\nu,i}\cdot(\sum_{\kappa=1}^{j-1}\xi_{\nu,i,\kappa}Z_\kappa+\xi_{\nu,i,j}Z_j)
\end{array}
$$



Coefficients of the hidden part of $\boldsymbol{k}^*_{h,i}$ in Game 2-n-2



Insertion of Z_j is realized by a conceptual basis change determined by Z_j and the multiplicative group structure of $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ (see item 2 in Section 6.3.2). Moreover, the obtained distribution of vectors $\vec{p}_{h,i} \cdot (\sum_{\kappa=1}^{n} \xi_{h,i,\kappa} Z_\kappa)$ is equivalent to $\vec{p}_{h,i} \cdot Z_{h,i}$ with $Z_{h,i} \xleftarrow{\cup} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}$, which is shown by using the affine space (i.e., additive) structure of $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ (see item 3 in Section 6.3.2).

Hence, in Game 3, the coefficient vector is changed to $\vec{w}_{h,i} \xleftarrow{\cup} \mathbb{F}_q^n$ if $\rho_h(i) = v_{h,i} \wedge v_{h,i} \notin \Gamma$, $\vec{w}_{h,i} \xleftarrow{\cup} \mathsf{span}\langle \vec{y} \rangle^{\perp}$ if $\rho_h(i) = \neg v_{h,i} \wedge v_{h,i} \in \Gamma$, and then the secret value $r_{h,0}$ for decryption are information-theoretically hidden from the adversary for $h = 1, \ldots, \nu$. In Game 4, the value of challenge bit b is independent from the adversary's view, and the proof is complete.

6.3.2 Key Properties of $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$

In order to achieve the game transformations given above, in particular, change into Game 2-j-2, the transformation $(\vec{y}, \vec{v}) \mapsto (\vec{y}U, \vec{v}Z)$ by (U, Z) with $U \xleftarrow{\cup} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ and $Z := (U^{-1})^{\mathrm{T}}$ is required to satisfy the following conditions.

1. It fixes the target $\vec{y}$, i.e., $\vec{y}U = \vec{y}$, since $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ is the isotropy group of $\vec{y}$ (Lemma 1). If $\vec{y}U$ was uniformly distributed in a large subspace outside of $\mathsf{span}\langle \vec{y} \rangle$, the challenger would fail the simulation for the above game changes.

2. The fact that $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ is a subgroup of $GL(n, \mathbb{F}_q)$ (Lemma 1) realizes (iterated) information-theoretical changes into Game 2-j-2 since $(Z_1, \ldots, Z_{j-1}, I_n)Z_j = (Z_1 Z_j, \ldots, Z_{j-1} Z_j, Z_j)$ is uniformly distributed in $\left(\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}\right)^j$ if $Z_i \xleftarrow{\cup} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}$ for $i = 1, \ldots, j$.

3. $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ is described as $A_{n-1} \setminus H_{n-2}$, where $A_{n-1} := \{\vec{u}' \in \mathbb{F}_q^n \mid \vec{y} \cdot \vec{u}' = y_n\}$ is an $(n-1)$-dimensional affine space and $H_{n-2} := A_{n-1} \cap \{u'_n = 0\}$ is a hyperplane section of A_{n-1}. This additive structure generates a freshly random element by a linear combination $\sum_{\kappa=1}^{n} \xi_\kappa Z_\kappa$ with freshly random ξ_κ such that $\sum_{\kappa=1}^{n} \xi_\kappa = 1$ and $Z_\kappa \xleftarrow{\cup} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}$ (Lemma 2).

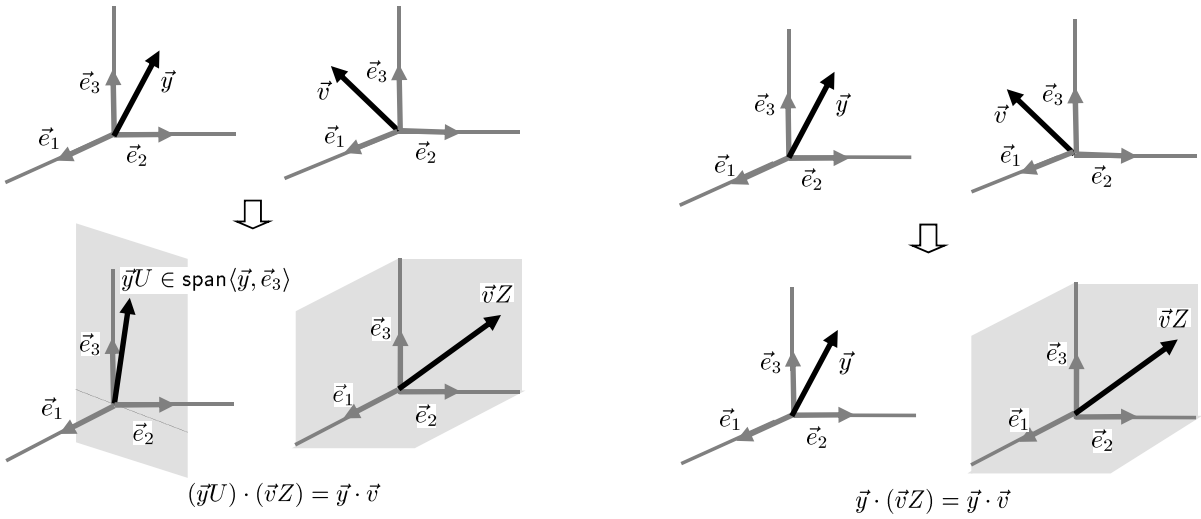


Figure 2: Three dimensional cases of Lemma 13 on the left and Lemma 3 on the right when $\vec{y} \cdot \vec{v} \neq 0$ and is uniformly random and independent from other variables. The vectors $\vec{y}U$ and $\vec{v}Z$ are uniformly distributed in the shadowed subspaces, respectively.

4. $\vec{v}Z$ distributes uniformly in $W_{\vec{y},(\vec{y}\cdot\vec{v})} := \{\vec{w} \in \mathbb{F}_q^n \setminus \mathsf{span}\langle \vec{e}_n \rangle^{\perp} \mid \vec{y} \cdot \vec{w} = \vec{y} \cdot \vec{v}\}$ (Lemma 3). That is, if $\vec{y} \cdot \vec{v} \neq 0$ and is uniformly random (resp. $\vec{y} \cdot \vec{v} = 0$), $\vec{v}Z$ distributes uniformly in $\mathbb{F}_q^n$ (resp. in the hyperplane that is perpendicular to $\vec{y}$) except for negligible probability.

Lemma 3 is considered to be a pairwise independence lemma specific to $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$. For comparison, we describe the lemma for $\mathcal{H}(n, \mathbb{F}_q)$ in [24] below. Fig. 2 compares the two lemmas when $\vec{y} \cdot \vec{v}$ $(\neq 0)$ is uniformly random and independent from other variables, which is an important case for the security proof of the proposed KP-ABE.

Lemma 13 (Pairwise Independence Lemma for $\mathcal{H}(n, \mathbb{F}_q)$ [24]) *Let $\vec{e}_n := (0, \ldots, 0, 1) \in \mathbb{F}_q^n$. For all $\vec{y} \in \mathbb{F}_q^n \setminus \mathsf{span}\langle \vec{e}_n \rangle$ and $\pi \in \mathbb{F}_q$, let $W'_{\vec{y},\pi} := \{(\vec{r}, \vec{w}) \in (\mathsf{span}\langle \vec{y}, \vec{e}_n \rangle \setminus \mathsf{span}\langle \vec{e}_n \rangle) \times (\mathbb{F}_q^n \setminus \mathsf{span}\langle \vec{e}_n \rangle^{\perp}) \mid \vec{r} \cdot \vec{w} = \pi\}$.*
For all $(\vec{y}, \vec{v}) \in \left(\mathbb{F}_q^n \setminus \mathsf{span}\langle \vec{e}_n \rangle\right) \times \left(\mathbb{F}_q^n \setminus \mathsf{span}\langle \vec{e}_n \rangle^{\perp}\right)$ and $(\vec{r}, \vec{w}) \in W'_{\vec{y},(\vec{y}\cdot\vec{v})}$, $\Pr[\vec{y}U = \vec{r} \wedge \vec{v}Z = \vec{w}] = 1/\sharp W'_{\vec{y},(\vec{y}\cdot\vec{v})}$, where $U \xleftarrow{\cup} \mathcal{H}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q)$ and $Z := (U^{-1})^{\mathrm{T}}$.

The left hand side of Fig. 2 presents the transformation $(\vec{y}, \vec{v}) \mapsto (\vec{y}U, \vec{v}Z)$ which is given in Lemma 13 using a pair of matrices (U, Z) with $U \xleftarrow{\cup} \mathcal{H}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q)$ in a three-dimensional space when $\vec{y} \cdot \vec{v}$ $(\neq 0)$ is uniformly random. The image $(\vec{y}U, \vec{v}Z)$ is spreading over $\mathsf{span}\langle \vec{y}, \vec{e}_n \rangle \times \mathbb{F}_q^n$ except for negligible probability since $(\vec{y}U) \cdot (\vec{v}Z) = \vec{y} \cdot \vec{v}$ is random. The right hand side of Fig. 2 presents the transformation which is given in Lemma 3 using (U, Z) with $U \xleftarrow{\cup} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ in a three-dimensional space when $\vec{y} \cdot \vec{v}$ $(\neq 0)$ is uniformly random. Then, $\vec{y}$ is fixed, i.e., $\vec{y}U = \vec{y}$. Only $\vec{v}Z$ is spreading over $\mathbb{F}_q^n$ except for negligible probability since $\vec{y} \cdot (\vec{v}Z) = \vec{y} \cdot \vec{v}$ is random. Since $\vec{y}$ is fixed in this conceptual change, i.e., change to Game 2-j-2, we can execute the next computational change, i.e., swap in Game 2-$(j+1)$-1, in the sequence of changes given in Section 6.3.1.

6.4 An Alternative Modular Approach

We describe an alternative proof of Theorem 1 using interactive Problem 3, which is defined below. Lemma 14 shows that the advantage of Problem 3 is bounded by $2n$-times the advantages of the DLIN problem. In addition, Lemma 15 shows that the advantage gap between Games 0 and 3 (defined in Section 6.2) is bounded by the advantage of Problem 3.

6.4.1 High-Level Problem (Problem 3)

In Problem 3, the adversary declares the challenge $\vec{y}$ in step 2 of the definition. While ciphertext elements ($\boldsymbol{e}_{\beta,0}$ and) $\boldsymbol{e}_{\beta,1}$ are generated depending on $\vec{y}$, key elements $\boldsymbol{h}^*_{\beta,0}$ and $\{\boldsymbol{h}^*_{\beta,j,i}\}$ do not depend any key query $\mathbb{S}$, but can be used for simulation of any key query. Hence, Problem 3 is considered as a "no key query" version semi-adaptive security game that can be used for the scheme's semi-adaptive security. By using the high-level problem, i.e., Problem 3, we improve *modularity* for the proof of Theorem 1. As an example, Problem 5 in Section 7.3.3, a variant of Problem 3, can be seamlessly used for *full* security proof of the proposed ABS with constant-size secret keys.

Definition 12 (Problem 3) *Problem 3 is to guess β, after running the following 2-step game:*

1. *The challenger generates*

$$
\begin{aligned}
&(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \mathbb{B}_1, \{B^*_{i,j}, B'^*_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{KP\text{-}ABE}}_{\mathsf{ob}}(1^\lambda, 6, n),\\
&\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \ldots, \boldsymbol{b}_{0,5}), \qquad \widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,3}, \ldots, \boldsymbol{b}^*_{0,5}),\\
&\widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, .., \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,3n+1}, .., \boldsymbol{b}_{1,6n}) \text{ is calculated as in Eq. (2)}\\
&\quad \text{from } \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n},\\
&\widehat{\mathbb{B}}^*_1 := (\boldsymbol{b}^*_{1,1}, .., \boldsymbol{b}^*_{1,n}, \boldsymbol{b}^*_{1,3n+1}, .., \boldsymbol{b}^*_{1,6n}),
\end{aligned}
$$

   and gives $\varrho_1 := (\mathsf{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,1})$ to the adversary.

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

$$
\begin{aligned}
&\delta, \delta_0, \omega, \varphi_0, \varphi_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q, \ \tau, \rho \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,\\
&\boldsymbol{h}^*_{0,0} := (\delta, 0, 0, \delta_0, 0)_{\mathbb{B}^*_0}, \quad \boldsymbol{h}^*_{1,0} := (\delta, \rho, 0, \delta_0, 0)_{\mathbb{B}^*_0},\\
&\boldsymbol{e}_{0,0} := (\omega, 0, 0, 0, \varphi_0)_{\mathbb{B}_0}, \quad \boldsymbol{e}_{1,0} := (\omega, \tau, 0, 0, \varphi_0)_{\mathbb{B}_0},\\
&\text{for } j = 1, .., n; \ i = 1, .., n; \quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \ \vec{\delta}_{j,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n},\\
&\quad U_j \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q), \quad Z_j := (U_j^{-1})^{\mathrm{T}},
\end{aligned}
$$

$$
\begin{array}{lcccccc}
 & & \overbrace{\phantom{\delta\vec{e}_i,}}^{n} & \overbrace{\phantom{0^{2n},\ \rho\vec{e}_i \cdot Z_j,}}^{2n} & \overbrace{\phantom{\vec{\delta}_{j,i},}}^{2n} & \overbrace{}^{n} & \\
\boldsymbol{h}^*_{0,j,i} := & (& \delta\vec{e}_i, & 0^{2n}, & \vec{\delta}_{j,i}, & 0^n &)_{\mathbb{B}^*_1}\\
\boldsymbol{h}^*_{1,j,i} := & (& \delta\vec{e}_i, & 0^n,\ \rho\vec{e}_i \cdot Z_j, & \vec{\delta}_{j,i}, & 0^n &)_{\mathbb{B}^*_1}\\
\boldsymbol{e}_{0,1} := & (& \omega\vec{y}, & 0^{2n}, & 0^{2n}, & \varphi_1\vec{y} &)_{\mathbb{B}_1},\\
\boldsymbol{e}_{1,1} := & (& \omega\vec{y}, & \tau\vec{y}, \quad \tau\vec{y}, & 0^{2n}, & \varphi_1\vec{y} &)_{\mathbb{B}_1},
\end{array}
$$

   for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$, and return $\varrho_2 := (\boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{h}^*_{\beta,j,i}\}_{j=1,\ldots,n;\, i=1,\ldots,n}, \boldsymbol{e}_{\beta,1})$ to the adversary.

For a probabilistic adversary $\mathcal{B}$, we define the advantage of $\mathcal{B}$ as the quantity

$$
\begin{aligned}
\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) := \big|&\mathsf{Pr}\left[\mathcal{B} \text{ outputs } 1 \,|\varrho_1 \text{ and } \varrho_2 \text{ with } \beta = 0 \text{ are given to } \mathcal{B}\right] -\\
&\mathsf{Pr}[\mathcal{B} \text{ outputs } 1 \,|\varrho_1 \text{ and } \varrho_2 \text{ with } \beta = 1 \text{ are given to } \mathcal{B}]\big|\,.
\end{aligned}
$$

Lemma 14 *Problem 3 is computationally intractable under the DLIN assumption.*

For any adversary $\mathcal{B}$, there are probabilistic machines $\mathcal{F}_{j,\iota}$ $(j = 0, \ldots, n;\ \iota = 1, 2)$, whose running times are essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) \leq \sum_{j=0}^{n} \sum_{\iota=1}^{2} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{j,\iota}}(\lambda) + (10n + 10)/q$.

The proof of Lemma 14 is given in Appendix A.3.

6.4.2 Proof of Theorem 1 using Problem 3

To prove Theorem 1 using Problem 3, we only consider 3 games, Game 0 (original semi-adaptive security game), Game 3 and Game 4, which are given in Section 6.2.

We will show Lemma 15 that evaluate the gap between $\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda)$ and $\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)$. From the lemma and Lemmas 11 and 14, we obtain $\mathsf{Adv}^{\mathsf{KP\text{-}ABE}}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) \leq \left|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)\right| + \left|\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda)\right| \leq \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) + 3\nu\hat{\ell}/q \leq \sum_{j=0}^{n} \sum_{\iota=1}^{2} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{j,\iota}}(\lambda) + (3\nu\hat{\ell} + 10n + 10)/q$. This completes the proof of Theorem 1 using Problem 3. □

Lemma 15 *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, $|\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) + 3\nu\hat{\ell}/q$, where ν is the maximum number of $\mathcal{A}$'s key queries, $\hat{\ell}$ is the maximum number of rows in access matrices of key queries.*

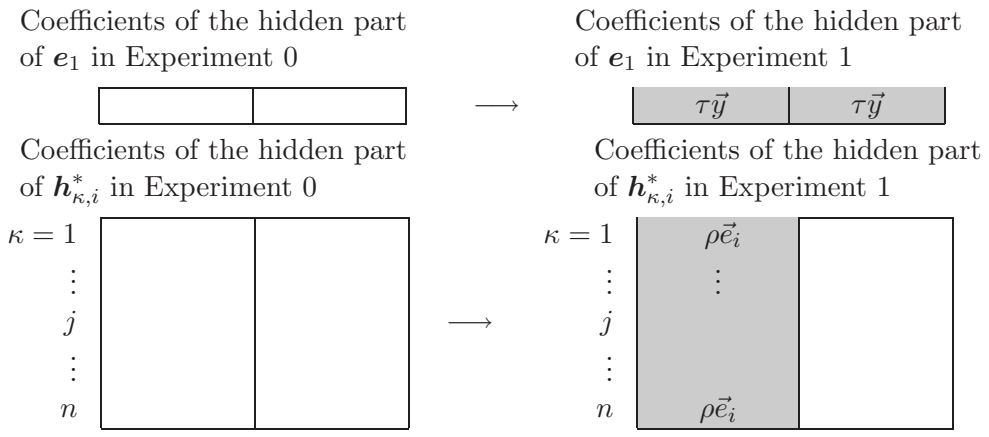
The proof of Lemma 15 is given in Appendix A.3.

6.4.3 Iteration of Swaps and Conceptual Changes for Lemma 14

For comparison of the proofs in Sections 6.2 and 6.4, we describe the (simple) iteration of swaps and conceptual changes for the proof of Lemma 14 here. Refer to Section 6.3.1 for comparison.

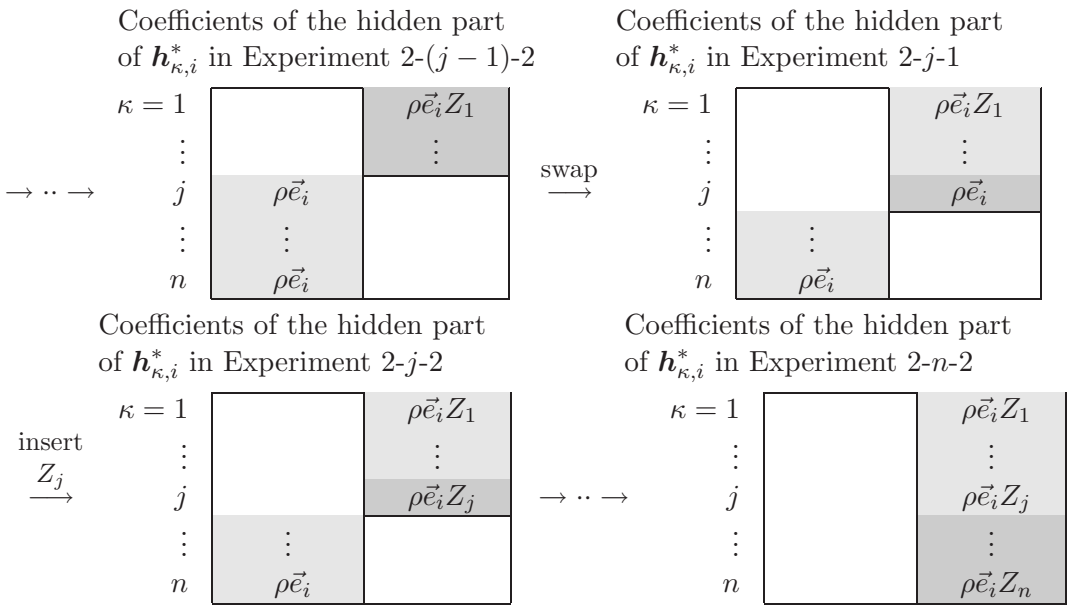
Lemma 14 is proven by the hybrid argument through $2n+2$ experiments (given in Appendix A.3.1): Experiment 0 $\Rightarrow$ Experiment 1 $\Rightarrow$ for $j = 1, \ldots, n$; Experiment 2-j-1 $\Rightarrow$ Experiment 2-j-2

First, in a $\beta = 0$ instance of Problem 3 (Experiment 0), coefficients of the hidden parts of $\boldsymbol{e}_1$ and $\boldsymbol{h}^*_{\kappa,i}$ $(\kappa = 1, \ldots, n)$ are all zero. Then, in the next Experiment 1, that of $\boldsymbol{e}_1$ is filled with $(\tau\vec{y}, \tau\vec{y}) \in \mathbb{F}_q^{2n}$ and the first n-dim. coefficient (block) of the hidden parts of $\boldsymbol{h}^*_{\kappa,i}$ $(\kappa = 1, \ldots, n)$ are changed to $\rho\vec{e}_i \in \mathbb{F}_q^n$ as: (Hereafter, a blank indicates zero coefficients)



After that, in turn for $j = 1, \ldots, n$, the coefficient vector $\rho\vec{e}_i \in \mathbb{F}_q^n$ is *swapped* to the second block of the hidden parts of $\boldsymbol{h}^*_{j,i}$ 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 swap can be securely executed under the DLIN assumption. At the final Experiment 2-n-2, each $\rho\vec{e}_i Z_j$ $(j = 1, \ldots, n)$ is embedded in the second block of hidden parts in $\boldsymbol{h}^*_{j,i}$, i.e., an instance of Experiment 2-n-2 is equivalent to a $\beta = 1$ instance of Problem 3.



Insertion of Z_j is realized by a conceptual basis change determined by Z_j (see item 2 in Section 6.3.2).

7 Proposed Fully Secure ABS Scheme with Constant-Size Secret Keys

We propose a *fully secure* (*adaptive*-predicate unforgeable and private) ABS scheme with constant-size secret keys. This is because the *adaptive*-predicate unforgeability of the ABS can be guaranteed by the *non-adaptive* payload-hiding security of the underlying CP-ABE under the Naor transform[1].

7.1 Building Blocks for the Proposed ABS

7.1.1 Dual Orthonormal Basis Generator

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

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

[1]Non-adaptive security of CP-ABE means that the adversary's key queries may not depend on the challenge ciphertext [1].

$\boldsymbol{b}^*_{t,i} := (\chi_{t,i,1}, .., \chi_{t,i,N_t})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \chi_{t,i,j} \boldsymbol{a}_j$ for $i = 1, .., N_t$, $\mathbb{B}^*_t := (\boldsymbol{b}^*_{t,1}, .., \boldsymbol{b}^*_{t,N_t})$ for $t = 0, 2$,
$B^*_{i,j} := \mu_{i,j} G$, $B'^*_{i,j,l} := \mu'_{i,j,l} G$ for $i, j = 1, \ldots, 6; l = 1, \ldots, n$,
for $t = 0, 1, 2$, $(\vartheta_{t,i,j})_{i,j=1,\ldots,N_t} := \psi \cdot (X_t^{\mathrm{T}})^{-1}$,
$\boldsymbol{b}_{t,i} := (\vartheta_{t,i,1}, .., \vartheta_{t,i,N_t})_{\mathbb{A}} = \sum_{j=1}^{N_t} \vartheta_{t,i,j} \boldsymbol{a}_j$ for $i = 1, .., N_t$, $\mathbb{B}_t := (\boldsymbol{b}_{t,1}, .., \boldsymbol{b}_{t,N_t})$,
return $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \mathbb{B}_1, \{B^*_{i,j}, B'^*_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n}, \mathbb{B}_2, \mathbb{B}^*_2)$.

Remark 4 From Remark 2, $\{B^*_{i,j}, B'^*_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n}$ is identified with basis $\mathbb{B}^*_1 := (\boldsymbol{b}^*_{1,1}, \ldots, \boldsymbol{b}^*_{1,6n})$ dual to $\mathbb{B}_1$.

7.1.2 Collision Resistant (CR) Hash Functions

Let $\lambda \in \mathbb{N}$ be a security parameter. A collision resistant (CR) hash function family, H, associated with $\mathcal{G}_{\mathsf{bpg}}$ and a polynomial, $poly(\cdot)$, 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, $\mathsf{hk} \xleftarrow{\mathsf{R}} \mathsf{KH}_\lambda$ and $\mathsf{D} := \{0,1\}^{poly(\lambda)}$. Each such hash function $\mathsf{H}^{\lambda,\mathsf{D}}_{\mathsf{hk}}$ maps an element of D to an element of $\mathbb{F}_q^\times$ with q that is the first element of output $\mathsf{param}_{\mathbb{G}}$ of $\mathcal{G}_{\mathsf{bpg}}(1^\lambda)$. There must exist a deterministic polynomial-time algorithm that on input 1^λ, hk and $\varrho \in \mathsf{D}$, outputs $\mathsf{H}^{\lambda,\mathsf{D}}_{\mathsf{hk}}(\varrho)$.

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

7.2 Construction

$\mathsf{Setup}(1^\lambda, n)$: $\mathsf{hk} \xleftarrow{\mathsf{R}} \mathsf{KH}_\lambda$,
$(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \mathbb{B}_1, \{B^*_{i,j}, B'^*_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n}, \mathbb{B}_2, \mathbb{B}^*_2) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{ABS}}_{\mathsf{ob}}(1^\lambda, 6, n)$,
$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,4})$, $\widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, \ldots, \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,4n+1}, \ldots, \boldsymbol{b}_{1,6n})$, $\widehat{\mathbb{B}}_2 := (\boldsymbol{b}_{2,1}, \boldsymbol{b}_{2,2}, \boldsymbol{b}_{2,7})$,
$\widehat{\mathbb{B}}^*_1 := (\boldsymbol{b}^*_{1,1}, \ldots, \boldsymbol{b}^*_{1,n}, \boldsymbol{b}^*_{1,3n+1}, \ldots, \boldsymbol{b}^*_{1,4n}) = \{B^*_{i,j}, B'^*_{i,j,l}\}_{i=1,4;j=1,\ldots,6;l=1,\ldots,n}$,
$\widehat{\mathbb{B}}^*_2 := (\boldsymbol{b}^*_{2,1}, \boldsymbol{b}^*_{2,2}, \boldsymbol{b}^*_{2,5}, \boldsymbol{b}^*_{2,6})$,
return $\mathsf{sk} := \boldsymbol{b}^*_{0,1}$, $\mathsf{pk} := (1^\lambda, \mathsf{hk}, \mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t\}_{t=0,1,2}, \{\widehat{\mathbb{B}}^*_t\}_{t=1,2}, \boldsymbol{b}^*_{0,3})$.
$\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \Gamma := \{x_1, \ldots, x_{n'} \mid x_j \in \mathbb{F}_q^\times\})$:
$\omega, \varphi_0, \varphi_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{y} := (y_1, \ldots, y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \cdot \prod_{j=1}^{n'} (z - x_j)$,
$\boldsymbol{k}^*_0 := (\omega, 0, \varphi_0, 0)_{\mathbb{B}^*_0}$,
$L^*_{1,j} := \omega B^*_{1,j} + \varphi_1 B^*_{4,j}$, $L^*_{2,j} := \sum_{l=1}^{n} y_l (\omega B'^*_{1,j,l} + \varphi_1 B'^*_{4,j,l})$ for $j = 1, \ldots, 6$,
$\boldsymbol{k}^*_{2,1} := (\omega(1,0), 0, 0, \varphi_{2,1,1}, \varphi_{2,1,2}, 0)_{\mathbb{B}^*_2}$, $\boldsymbol{k}^*_{2,2} := (\omega(0,1), 0, 0, \varphi_{2,2,1}, \varphi_{2,2,2}, 0)_{\mathbb{B}^*_2}$,
return $\mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}^*_0, \{L^*_{1,j}, L^*_{2,j}\}_{j=1,\ldots,6}, \{\boldsymbol{k}^*_{2,\iota}\}_{\iota=1,2})$.
Remark From $\{L^*_{1,j}, L^*_{2,j}\}_{j=1,\ldots,6}$ and $\vec{y}$, $\boldsymbol{k}^*_1$ is defined as

$$\boldsymbol{k}_1^* := \Big(\overbrace{y_1 L_{1,1}^*, .., y_{n-1} L_{1,1}^*, L_{2,1}^*,}^{n} \overbrace{y_1 L_{1,2}^*, .., y_{n-1} L_{1,2}^*, L_{2,2}^*,}^{n} \cdots$$
$$\overbrace{y_1 L_{1,5}^*, .., y_{n-1} L_{1,5}^*, L_{2,5}^*,}^{} \overbrace{y_1 L_{1,6}^*, .., y_{n-1} L_{1,6}^*, L_{2,6}^*}^{} \Big),$$

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

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

then compute $\vec{y} := (y_1, \ldots, y_n)$ 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

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

$\xi \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,\ \ (\beta_i) \xleftarrow{\mathsf{U}} \{(\beta_1,\ldots,\beta_\ell) \ |\ \sum_{i=1}^{\ell} \beta_i M_i = \vec{0}\}$,

$\boldsymbol{s}_0^* := \xi \boldsymbol{k}_0^* + \boldsymbol{r}_0^*$, where $\boldsymbol{r}_0^* \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}_{0,3}^* \rangle$,

$\boldsymbol{s}_i^* := \gamma_i \cdot \xi \boldsymbol{k}_1^* + \sum_{\iota=1}^{n} \mu_{i,\iota} \cdot \boldsymbol{b}_{t,\iota}^* + \boldsymbol{r}_i^*,\ \ \vec{v}_i := (v_i^{n-1}, \ldots, v_i, 1)$ for $i = 1,\ldots,\ell$,

where $\boldsymbol{r}_i^* \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}_{1,3n+1}^*, \ldots, \boldsymbol{b}_{1,4n}^* \rangle$, and $\gamma_i, \vec{\mu}_i := (\mu_{i,1}, \ldots, \mu_{i,n})$ are defined as

if $i \in I \ \wedge\ \rho(i) = v_i$, $\quad \gamma_i := \alpha_i,\ \ \vec{\mu}_i \xleftarrow{\mathsf{U}} \{\vec{\mu}_i \ |\ \vec{\mu}_i \cdot \vec{v}_i = 0 \ \wedge\ \mu_{i,1} = \beta_i\}$,

if $i \in I \ \wedge\ \rho(i) = \neg v_i$, $\quad \gamma_i := \alpha_i / (\vec{v}_i \cdot \vec{y}),\ \ \vec{\mu}_i \xleftarrow{\mathsf{U}} \{\vec{\mu}_i \ |\ \vec{\mu}_i \cdot \vec{\mu}_i = \beta_i\}$,

if $i \notin I \ \wedge\ \rho(i) = v_i$, $\quad \gamma_i := 0,\ \ \vec{\mu}_i \xleftarrow{\mathsf{U}} \{\vec{\mu}_i \ |\ \vec{\mu}_i \cdot \vec{v}_i = 0 \ \wedge\ \mu_{i,1} = \beta_i\}$,

if $i \notin I \ \wedge\ \rho(i) = \neg v_i$, $\quad \gamma_i := 0,\ \ \vec{\mu}_i \xleftarrow{\mathsf{U}} \{\vec{\mu}_i \ |\ \vec{\mu}_i \cdot \vec{v}_i = \beta_i\}$,

$\boldsymbol{s}_{\ell+1}^* := \xi(\boldsymbol{k}_{2,1}^* + \mathsf{H}_{\mathsf{hk}}^{\lambda,\mathsf{D}}(m \,||\, \mathbb{S}) \cdot \boldsymbol{k}_{2,2}^*) + \boldsymbol{r}_{\ell+1}^*$, where $\boldsymbol{r}_{\ell+1}^* \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}_{2,5}^*, \boldsymbol{b}_{2,6}^* \rangle$,

return $\vec{\boldsymbol{s}}^* := (\boldsymbol{s}_0^*, \ldots, \boldsymbol{s}_{\ell+1}^*)$.

$\mathsf{Ver}(\mathsf{pk},\ m,\ \mathbb{S} := (M,\rho), \vec{\boldsymbol{s}}^*)$: $\quad \vec{f} \xleftarrow{\mathsf{R}} \mathbb{F}_q^r,\ \vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$,

$s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}},\ \eta_0, \eta_{\ell+1}, \theta_{\ell+1}, s_{\ell+1} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \qquad \boldsymbol{c}_0 := (-s_0 - s_{\ell+1}, 0, 0, \eta_0)_{\mathbb{B}_0}$,

for $i = 1,\ldots,\ell$, $\quad \vec{v}_i := (v_i^{n-1}, \ldots, v_i, 1)$, $\quad \vec{e}_1 := (1, 0, \ldots, 0)$,

if $\rho(i) = v_i$, $\quad$ return 0 if $\boldsymbol{s}_i^* \notin \mathbb{V}_1$, $\quad$ else $\theta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \vec{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n}$,

$$\boldsymbol{c}_i := \Big(\overbrace{s_i\vec{e}_1 + \theta_i\vec{v}_i,}^{n} \overbrace{0^{2n},}^{2n} \overbrace{0^n,}^{n} \overbrace{\vec{\eta}_i}^{2n} \Big)_{\mathbb{B}_1},$$

if $\rho(i) = \neg v_i$, $\quad$ return 0 if $\boldsymbol{s}_i^* \notin \mathbb{V}_t$, $\quad$ else $\vec{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n}$,

$$\boldsymbol{c}_i := \Big(\overbrace{s_i\vec{v}_i,}^{n} \overbrace{0^{2n},}^{2n} \overbrace{0^n,}^{n} \overbrace{\vec{\eta}_i}^{2n} \Big)_{\mathbb{B}_1},$$

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

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

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

[**Correctness**] If $\vec{\boldsymbol{s}}^*$ is a correctly generated signature,

$$\prod_{i=0}^{\ell+1} e(\boldsymbol{c}_i, \boldsymbol{s}_i^*) = e(\boldsymbol{c}_0, \boldsymbol{k}_0^*)^{\xi} \cdot \prod_{i\in I} e(\boldsymbol{c}_i, \boldsymbol{k}_1^*)^{\gamma_i \xi} \cdot \prod_{i=1}^{\ell} \prod_{\iota=1}^{2} e(\boldsymbol{c}_i, \boldsymbol{b}_{t,\iota}^*)^{\mu_{i,\iota}} \cdot e(\boldsymbol{c}_{\ell+1}, \boldsymbol{s}_{\ell+1}^*)$$
$$= g_T^{\xi\delta(-s_0 - s_{\ell+1})} \cdot \prod_{i\in I} g_T^{\xi\delta\alpha_i s_i} \cdot \prod_{i=1}^{\ell} g_T^{\beta_i s_i} \cdot g_T^{\xi\delta s_{\ell+1}} = g_T^{\xi\delta(-s_0 - s_{\ell+1})} \cdot g_T^{\xi\delta s_0} \cdot g_T^{\xi\delta s_{\ell+1}} = 1.$$

7.3 Security

7.3.1 Theorems

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 [27] (privacy of the ABS scheme in [27]).

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 $\mathcal{F}_0, \ldots, \mathcal{F}_4$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,

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

where $\mathcal{F}_{l\text{-}h\text{-}0}(\cdot) := \mathcal{F}_l(h, 0, \cdot), \mathcal{F}_{l\text{-}h\text{-}j\text{-}\iota}(\cdot) := \mathcal{F}_l(h, j, \iota, \cdot)$ for $l = 1, 2$, $\mathcal{F}_{l\text{-}h}(\cdot) := \mathcal{F}_l(h, \cdot)$ for $l = 3, 4$, ν_K (resp. ν_S) is the maximum number of $\mathcal{A}$'s reveal key (resp. signature) queries, $\hat{\ell}$ is the maximum number of rows in access matrices M of key queries, and $\epsilon := (6\nu_K\hat{\ell} + 20\nu_K n + 10\nu_K + 10\nu_S + 5)/q$.

7.3.2 Proof of Theorem 3

To prove Theorem 3, we consider the following $2\nu_K + \nu_S + 3$ games. In Game 0, a part framed by a box indicates positions of 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.

For notational simplicity, we use ℓ ($:= \ell_h$) for the number of rows of any key queries below.

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

$$\boldsymbol{k}^*_0 := (\omega,\ \boxed{0},\ \varphi_0,\ 0)_{\mathbb{B}^*_0}, \tag{13}$$

$$\left.\begin{aligned}\boldsymbol{k}^*_1 :=\ & (\overbrace{\quad\omega\vec{y},\quad}^{n}\ \overbrace{\quad\boxed{0^{2n}},\quad}^{2n}\ \overbrace{\quad\varphi_1\vec{y},\quad}^{n}\ \overbrace{\quad 0^{2n}\quad}^{2n})_{\mathbb{B}^*_1}, \\ \boldsymbol{k}^*_{2,1} :=\ & (\omega(1,0), 0, 0, \varphi_{2,1,1}, \varphi_{2,1,2}, 0)_{\mathbb{B}^*_2}, \quad \boldsymbol{k}^*_{2,2} := (\omega(0,1), 0, 0, \varphi_{2,2,1}, \varphi_{2,2,2}, 0)_{\mathbb{B}^*_2},\end{aligned}\right\} \tag{14}$$

where $\omega, \varphi_0, \varphi_1, \varphi_{2,1,1}, \ldots, \varphi_{2,2,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and $\vec{y} := (y_1, \ldots, y_n)$ 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:

$$\left.\begin{aligned}&\boldsymbol{s}^*_0 := (\ \widetilde{\delta},\ \boxed{0},\ \sigma_0,\ 0\ )_{\mathbb{B}^*_0}, \qquad \boldsymbol{s}^*_i := (\quad \vec{t}_i,\quad 0^{2n},\quad \vec{\sigma}_i,\quad 0^{2n}\ )_{\mathbb{B}^*_1}\ \text{ for } i = 1, \ldots, \ell, \\ &\boldsymbol{s}^*_{\ell+1} := (\ \widetilde{\delta}(1, \mathsf{H}^{\lambda,\mathsf{D}}_{\mathsf{hk}}(m\,||\,\mathbb{S})),\ \boxed{0^2},\ \vec{\sigma}_{\ell+1},\ 0\ )_{\mathbb{B}^*_2},\end{aligned}\right\} \tag{15}$$

where, $\widetilde{\delta} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\times}$, $\sigma_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\sigma}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, $\vec{\sigma}_{\ell+1} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$, $(\zeta_i) \xleftarrow{\mathsf{U}} \{(\zeta_i) \mid \sum_{i=1}^{\ell} \zeta_i M_i = \vec{1}\}$, and for $i = 1, \ldots, \ell$, if $\rho(i) = v_i$, then $\vec{t}_i \xleftarrow{\mathsf{U}} \{\vec{t}_i \mid \vec{t}_i \cdot \vec{v}_i = 0,\ t_{i,1} = \widetilde{\delta}\zeta_i\}$, if $\rho(i) = \neg v_i$, then $\vec{t}_i \xleftarrow{\mathsf{U}} \{\vec{t}_i \mid \vec{t}_i \cdot \vec{v}_i = \widetilde{\delta}\zeta_i\}$ with $\vec{v}_i := (v_i^{n-1}, \ldots, v_i, 1) \in \mathbb{F}_q^n$. The verification text for $(m', \mathbb{S}')$ with

$\mathbb{S}' := (M, \rho)$ is:

$$\left.\begin{array}{l} \boldsymbol{c}_0 := (\ \boxed{-s_0 - s_{\ell+1}},\ \boxed{0},\ 0,\ \eta_0\ )_{\mathbb{B}_0}, \\ \text{for } i = 1, \ldots, \ell, \qquad \overbrace{}^{n}\ \overbrace{}^{2n}\ \overbrace{}^{n}\ \overbrace{}^{2n} \\ \quad \text{if } \rho(i) = v_i,\ \ \boldsymbol{c}_i := \quad (\ s_i\vec{e}_1 + \theta_i\vec{v}_i,\ \boxed{0^{2n}},\ 0^n,\ \vec{\eta}_i\ )_{\mathbb{B}_1}, \\ \quad \text{if } \rho(i) = \neg v_i,\ \ \boldsymbol{c}_i := \quad (\ s_i\vec{v}_i,\ \boxed{0^{2n}},\ 0^n,\ \vec{\eta}_i\ )_{\mathbb{B}_1}, \\ \boldsymbol{c}_{\ell+1} := (\ s_{\ell+1}\vec{e}_1 + \theta_{\ell+1}(-\mathsf{H}^{\lambda,\mathsf{D}}_{\mathsf{hk}}(m' \,||\, \mathbb{S}'),\ 1),\ \boxed{0^2},\ 0^2,\ \eta_{\ell+1}\ )_{\mathbb{B}_2}, \end{array}\right\} \quad (16)$$

where $\vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$, $\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$, $s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$, $\theta_i, s_{\ell+1}, \eta_0, \eta_{\ell+1} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n}, \vec{e}_1 = (1, 0, \ldots, 0) \in \mathbb{F}_q^n$, and $\vec{v}_i := (v_i^{n-1}, \ldots, v_i, 1) \in \mathbb{F}_q^n$.

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

$$\left.\begin{array}{l} \boldsymbol{c}_0 := (-s_0 - s_{\ell+1},\ \boxed{-r_0 - r_{\ell+1}},\ 0,\ \eta_0)_{\mathbb{B}_0}, \\ \text{for } i = 1, \ldots, \ell, \qquad \overbrace{}^{n}\ \overbrace{}^{2n}\ \overbrace{}^{n}\ \overbrace{}^{2n} \\ \quad \text{if } \rho(i) = v_i,\ \ \boldsymbol{c}_i := \quad (\ s_i\vec{e}_1 + \theta_i\vec{v}_i,\ \boxed{r_i\vec{e}_1 + \psi_i\vec{v}_i},\ 0^n,\ 0^n,\ \vec{\eta}_i\ )_{\mathbb{B}_1}, \\ \quad \text{if } \rho(i) = \neg v_i,\ \ \boldsymbol{c}_i := \quad (\ s_i\vec{v}_i,\ \boxed{r_i\vec{v}_i},\ 0^n,\ 0^n,\ \vec{\eta}_i\ )_{\mathbb{B}_1}, \\ \boldsymbol{c}_{\ell+1} := (\ s_{\ell+1}\vec{e}_1 + \theta_{\ell+1}(-\mathsf{H}^{\lambda,\mathsf{D}}_{\mathsf{hk}}(m' \,||\, \mathbb{S}'),\ 1),\ \boxed{\vec{\psi}_{\ell+1}},\ 0^2,\ \eta_{\ell+1}\ )_{\mathbb{B}_2}, \end{array}\right\} \quad (17)$$

where $\vec{g} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$, $\vec{r}^{\mathrm{T}} := (r_1, \ldots, r_\ell)^{\mathrm{T}} := M \cdot \vec{g}^{\mathrm{T}}$, $r_0 := \vec{1} \cdot \vec{g}^{\mathrm{T}}$, $r_{\ell+1}, \psi_i \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{\psi}_{\ell+1} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$, and all the other variables are generated as in Game 0.

Game 2-h-1 ($h = 1, \ldots, \nu_K$) : 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:

$$\begin{array}{l} \boldsymbol{k}^*_0 := (\omega,\ \boxed{\tau'},\ \varphi_0,\ 0)_{\mathbb{B}^*_0}, \qquad (18) \\ \qquad\qquad \overbrace{}^{n}\ \overbrace{}^{2n}\ \overbrace{}^{n}\ \overbrace{}^{2n} \\ \boldsymbol{k}^*_1 := \quad (\ \omega\vec{y},\ \boxed{\tau\vec{y},\ \tau\vec{y}},\ \varphi_1\vec{y},\ 0^{2n}\ )_{\mathbb{B}^*_1}, \end{array}$$

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

$$\begin{array}{l} \text{for } i = 1, \ldots, \ell, \qquad \overbrace{}^{n}\ \overbrace{}^{2n}\ \overbrace{}^{n}\ \overbrace{}^{2n} \\ \quad \text{if } \rho(i) = v_i \wedge v_i \notin \Gamma,\ \ \boldsymbol{c}_i := \quad (\ s_i\vec{e}_1 + \theta_i\vec{v}_i,\ 0^n,\ \boxed{\vec{w}_i},\ 0^n,\ \vec{\eta}_i\ )_{\mathbb{B}_1}, \\ \quad \text{if } \rho(i) = \neg v_i \wedge v_i \in \Gamma,\ \ \boldsymbol{c}_i := \quad (\ s_i\vec{v}_i,\ 0^n,\ \boxed{\vec{\overline{w}}_i},\ 0^n,\ \vec{\eta}_i\ )_{\mathbb{B}_1}, \end{array}$$

where $\vec{w}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, $\vec{\overline{w}}_i \xleftarrow{\mathsf{U}} \mathsf{span}\langle\vec{y}\rangle^\perp$, all the other variables are generated as in Game 2-$(h-1)$-2.

Game 2-h-2 ($h = 1, \ldots, \nu_K$) : Game 2-h-2 is the same as Game 2-h-1 except the i-th component $\boldsymbol{c}_i$ of the verification text for $(m', \mathbb{S}')$ with $\mathbb{S}' := (M, \rho)$ are given by Eq. (17), and the components $\boldsymbol{k}^*_1$, $\boldsymbol{k}^*_{2,1}$ and $\boldsymbol{k}^*_{2,2}$ of the reply to the h-th key query for Γ is given by Eq. (14) (and $\boldsymbol{k}^*_0$ is given by Eq. (18)). all the other variables are generated as in Game 2-h-1.

Game 3-h ($h = 1, \ldots, \nu_S$) : Game 3-0 is Game 2-ν_K-2. Game 3-h is the same as Game 3-$(h-1)$ except that $\boldsymbol{s}^*_0, \boldsymbol{s}^*_{\ell+1}$ of the reply to the h-th reveal signature query for $(m, \mathbb{S})$ are:

$$\boldsymbol{s}^*_0 := (\ \widetilde{\delta},\ \boxed{\pi_0},\ \sigma_0,\ 0\ )_{\mathbb{B}^*_0}, \qquad \boldsymbol{s}^*_{\ell+1} := (\ \widetilde{\delta}(1, \mathsf{H}^{\lambda,\mathsf{D}}_{\mathsf{hk}}(m \,||\, \mathbb{S})),\ \boxed{\vec{\pi}_{\ell+1}},\ \vec{\sigma}_{\ell+1},\ 0\ )_{\mathbb{B}^*_2},$$

where $\pi_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\pi}_{\ell+1} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$, and all the other variables are generated as in Game 3-$(h-1)$.
Game 4 : Same as Game 3-ν_S except that $\boldsymbol{c}_0$ generated in Ver for verifying the output of the adversary is:

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

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

Let $\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}\iota)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h)}(\lambda)$, and $\mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)$ be the advantage of $\mathcal{A}$ in Game 0,1,2-h-ι,3-h and 4, respectively. $\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda)$ is equivalent to $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{ABS,UF}}(\lambda)$ and it is obtained that $\mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda) = 1/q$ by Lemma 24.

We will show five lemmas (Lemmas 19–23) that evaluate the gaps between pairs of subsequent games. From these lemmas and Lemmas 6–16, we obtain $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{ABS,UF}}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) \leq \left|\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)\right| + \sum_{h=1}^{\nu_K}(\left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1)\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda)\right| + \left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2)}(\lambda)\right|) + \sum_{h=1}^{\nu_S}\left|\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}(h-1))}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h)}(\lambda)\right| + \left|\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}\nu_S)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)\right| + \mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda) \leq \mathsf{Adv}_{\mathcal{F}_0}^{\mathsf{DLIN}}(\lambda) + \sum_{l=1}^{2}\sum_{h=1}^{\nu_K}(\mathsf{Adv}_{\mathcal{F}_{l\text{-}h\text{-}0}}^{\mathsf{DLIN}}(\lambda) + \sum_{j=1}^{n}\sum_{\iota=1}^{2}\mathsf{Adv}_{\mathcal{F}_{l\text{-}h\text{-}j\text{-}\iota}}^{\mathsf{DLIN}}(\lambda)) + \sum_{h=1}^{\nu_S}(\mathsf{Adv}_{\mathcal{F}_{3\text{-}h}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_{4\text{-}h}}^{\mathsf{H,CR}}(\lambda)) + (6\nu_K\hat{\ell} + 20\nu_K n + 10\nu_K + 10\nu_S + 5)/q$. This completes the proof of Theorem 3. □

7.3.3 Lemmas

We will show Lemmas 16–18 for the proof of Theorem 3.

Definition 13 (Problem 4) *Problem 4 is to guess β, given $(\mathsf{param}_n, \{\mathbb{B}_\iota, \widehat{\mathbb{B}}_\iota^*\}_{\iota=0,1,2}, \{\boldsymbol{e}_{\beta,i}\}_{i=0,\ldots,n+1}, \boldsymbol{f}) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{P4}}(1^\lambda, n)$, where*

$$\begin{aligned}
&\mathcal{G}_\beta^{\mathsf{P4}}(1^\lambda, n): \quad (\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1, \{B_{i,j}^*, B_{i,j,l}'^*\}_{i,j=1,\ldots,6;l=1,\ldots,n}, \mathbb{B}_2, \mathbb{B}_2^*) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}^{\mathsf{ABS}}(1^\lambda, 6, n),\\
&\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*, \boldsymbol{b}_{0,4}^*),\\
&\widehat{\mathbb{B}}_1^* := (\boldsymbol{b}_{1,1}^*, .., \boldsymbol{b}_{1,n}^*, \boldsymbol{b}_{1,3n+1}^*, .., \boldsymbol{b}_{1,6n}^*) \text{ is calculated as in Eq. (2) from } \{B_{i,j}^*, B_{i,j,l}'^*\}_{i,j=1,\ldots,6;l=1,\ldots,n},\\
&\widehat{\mathbb{B}}_2^* := (\boldsymbol{b}_{2,1}^*, \boldsymbol{b}_{2,2}^*, \boldsymbol{b}_{2,5}^*, .., \boldsymbol{b}_{2,7}^*), \quad \delta, \delta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \rho \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,\ \vec{\psi} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2,\\
&\boldsymbol{e}_{0,0} := (\delta, 0, 0, \delta_0)_{\mathbb{B}_0}, \quad \boldsymbol{e}_{1,0} := (\delta, \rho, 0, \delta_0)_{\mathbb{B}_0},\\
&\text{for } i = 1, \ldots, n; \quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \quad \vec{\delta}_{j,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n},\\
&\qquad\qquad \overbrace{\qquad}^{n} \quad \overbrace{\qquad\qquad}^{2n} \quad \overbrace{\qquad}^{n} \quad \overbrace{\qquad\qquad}^{2n}\\
&\boldsymbol{e}_{0,i} := (\ \delta\vec{e}_i,\ 0^{2n},\ 0^n,\ \vec{\delta}_{j,i}\ )_{\mathbb{B}_1},\\
&\boldsymbol{e}_{1,i} := (\ \delta\vec{e}_i,\ \rho\vec{e}_i,\ 0^n,\ 0^n,\ \vec{\delta}_{j,i}\ )_{\mathbb{B}_1},\\
&\boldsymbol{e}_{0,n+1} := (\delta, 0, 0^2, 0^2, \delta_0)_{\mathbb{B}_2}, \quad \boldsymbol{e}_{1,n+1} := (\delta, 0, \vec{\psi}, 0^2, \delta_0)_{\mathbb{B}_2}, \quad \boldsymbol{f} := \delta\boldsymbol{b}_{2,2},\\
&\text{return } (\mathsf{param}_n, \{\mathbb{B}_\iota, \widehat{\mathbb{B}}_\iota^*\}_{\iota=0,1,2}, \{\boldsymbol{e}_{\beta,i}\}_{i=0,\ldots,n+1}, \boldsymbol{f}),
\end{aligned}$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic machine $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 4, $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P4}}(\lambda)$, is similarly defined as in Definition 10.

Lemma 16 *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, $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P4}}(\lambda) \leq \mathsf{Adv}_{\mathcal{F}}^{\mathsf{DLIN}}(\lambda) + 5/q$.*

Lemma 16 is proven similarly to Lemma 1 in [23]. □

Definition 14 (Problem 5) *Problem 5 is to guess β, after running the following 2-step game:*

1. *The challenger generates*

$$(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1, \{B_{i,j}^*, B_{i,j,l}'^*\}_{i,j=1,\ldots,6;l=1,\ldots,n}, \mathbb{B}_2, \mathbb{B}_2^*) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}^{\mathsf{ABS}}(1^\lambda, 6, n),$$
$$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,4}), \qquad \widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, .., \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,3n+1}, .., \boldsymbol{b}_{1,6n}),$$
$$\widehat{\mathbb{B}}_1^* := (\boldsymbol{b}_{1,1}^*, .., \boldsymbol{b}_{1,n}^*, \boldsymbol{b}_{1,3n+1}^*, .., \boldsymbol{b}_{1,6n}^*) \text{ is calculated as in Eq. (2) from } \{B_{i,j}^*, B_{i,j,l}'^*\}_{i,j=1,\ldots,6;l=1,\ldots,n},$$

and gives $\varrho_1 := (\mathsf{param}_n, \widehat{\mathbb{B}}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}_1, \widehat{\mathbb{B}}_1^*, \mathbb{B}_2, \mathbb{B}_2^*)$ to the adversary.

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

$$\delta, \delta_0, \omega, \varphi_0, \varphi_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q, \ \tau, \rho \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,$$
$$\boldsymbol{h}_{0,0}^* := (\omega, 0, \varphi_0, 0)_{\mathbb{B}_0^*}, \quad \boldsymbol{h}_{1,0}^* := (\omega, \tau, \varphi_0, 0)_{\mathbb{B}_0^*}, \quad \boldsymbol{e}_0 := (\delta, \rho, 0, \delta_0)_{\mathbb{B}_0},$$
$$\text{for } j = 1, \ldots, n; \ i = 1, \ldots, n; \quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \quad \vec{\delta}_{j,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n},$$
$$U_j \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q), \quad Z_j := (U_j^{-1})^{\mathrm{T}},$$

$$\begin{array}{lc} & \overbrace{\phantom{\omega\vec{y},}}^{n} \ \overbrace{\phantom{0^{2n},}}^{2n} \ \overbrace{\phantom{\varphi_1\vec{y},}}^{n} \ \overbrace{\phantom{0^{2n}}}^{2n} \\ \boldsymbol{h}_{0,1}^* := & (\ \omega\vec{y}, \quad 0^{2n}, \quad \varphi_1\vec{y}, \quad 0^{2n} \ )_{\mathbb{B}_1^*}, \\ \boldsymbol{h}_{1,1}^* := & (\ \omega\vec{y}, \quad \tau\vec{y}, \ \tau\vec{y}, \quad \varphi_1\vec{y}, \quad 0^{2n} \ )_{\mathbb{B}_1^*}, \\ \boldsymbol{e}_{0,j,i} := & (\ \delta\vec{e}_i, \quad \rho\vec{e}_i, \ 0^n, \quad 0^n, \quad \vec{\delta}_{j,i} \ )_{\mathbb{B}_1}, \\ \boldsymbol{e}_{1,j,i} := & (\ \delta\vec{e}_i, \quad 0^n, \ \rho\vec{e}_i \cdot Z_j, \quad 0^n, \quad \vec{\delta}_{j,i} \ )_{\mathbb{B}_1}, \end{array}$$
$$\text{for } i = 1, 2, \ \boldsymbol{h}_{2,i}^* := \omega \boldsymbol{b}_{2,i}^*,$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$, and returns $\varrho_2 := (\boldsymbol{h}_{\beta,0}^*, \boldsymbol{e}_0, \boldsymbol{h}_{\beta,1}^*, \{\boldsymbol{e}_{\beta,j,i}\}_{j=1,\ldots,n;\, i=1,\ldots,n}, \{\boldsymbol{h}_{2,i}^*\}_{i=1,2})$ to the adversary.

For a probabilistic adversary $\mathcal{B}$, we define the advantage of $\mathcal{B}$ as the quantity
$$\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P5}}(\lambda) := |\mathsf{Pr}[\mathcal{B} \text{ outputs } 1 \,|\varrho_1 \text{ and } \varrho_2 \text{ with } \beta = 0 \text{ are given to } \mathcal{B}] - \mathsf{Pr}[\mathcal{B} \text{ outputs } 1 \,|\varrho_1 \text{ and } \varrho_2 \text{ with } \beta = 1 \text{ are given to } \mathcal{B}]|.$$

Lemma 17 *For any adversary $\mathcal{B}$, there are probabilistic machines $\mathcal{F}_0, \mathcal{F}$, whose running times are essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P5}}(\lambda) \leq \mathsf{Adv}_{\mathcal{F}_0}^{\mathsf{DLIN}}(\lambda) + \sum_{j=1}^{n}\sum_{\iota=1}^{2} \mathsf{Adv}_{\mathcal{F}_{j\text{-}\iota}}^{\mathsf{DLIN}}(\lambda) + (10n+5)/q$, where $\mathcal{F}_{j\text{-}\iota}(\cdot) := \mathcal{F}(j, \iota, \cdot)$.*

Lemma 17 is proven in a similar manner to Lemma 14.

Definition 15 (Problem 6) *Problem 6 is to guess $\beta \in \{0,1\}$, given $(\mathsf{param}_n, \{\widehat{\mathbb{B}}_t, \mathbb{B}_t^*\}_{t=0,2}, \mathbb{B}_1, \mathbb{B}_1^*, \boldsymbol{h}_{\beta,0}^*, \boldsymbol{e}_0, \{\boldsymbol{h}_{1,i}^*\}_{i=1,..,n}, \{\boldsymbol{h}_{\beta,2,i}^*, \boldsymbol{e}_{2,i}\}_{i=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{P6}}(1^\lambda, n)$, where*

$$\mathcal{G}_\beta^{\mathsf{P6}}(1^\lambda, n): \ (\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1, \{B_{i,j}^*, B_{i,j,l}'^*\}_{i,j=1,\ldots,6;l=1,\ldots,n}, \mathbb{B}_2, \mathbb{B}_2^*) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}^{\mathsf{ABS}}(1^\lambda, 6, n),$$
$$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,4}), \quad \widehat{\mathbb{B}}_2 := (\boldsymbol{b}_{2,1}, \boldsymbol{b}_{2,2}, \boldsymbol{b}_{2,5}, \ldots, \boldsymbol{b}_{2,7}),$$
$$\mathbb{B}_1^* := (\boldsymbol{b}_{1,1}^*, .., \boldsymbol{b}_{1,6n}^*) \text{ is calculated as in Eq. (2) from } \{B_{i,j}^*, B_{i,j,l}'^*\}_{i,j=1,\ldots,6;l=1,\ldots,n},$$
$$\sigma, \tau \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times, \ \omega, \delta, \delta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad \boldsymbol{h}_{0,0}^* := (\delta, 0, \delta_0, 0)_{\mathbb{B}_0^*}, \ \boldsymbol{h}_{1,0}^* := (\delta, \sigma, \delta_0, 0)_{\mathbb{B}_0^*}, \ \boldsymbol{e}_0 := (\omega, \tau, 0, 0)_{\mathbb{B}_0},$$
$$\boldsymbol{h}_{1,i}^* := \delta \boldsymbol{b}_{1,i}^* \ \text{ for } i = 1, \ldots, n, \quad U \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q), \quad Z := (U^{-1})^{\mathrm{T}},$$
$$\text{for } i = 1, 2; \quad \vec{e}_i := (0^{i-1}, \ 1, \ 0^{2-i}), \quad \vec{\delta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^2,$$

$$
\begin{array}{rcccccc}
\boldsymbol{h}^*_{0,2,i} := & (& \delta\vec{e}_i, & 0^2 & \vec{\delta}_i, & 0 &)_{\mathbb{B}^*_2}, \\
\boldsymbol{h}^*_{1,2,i} := & (& \delta\vec{e}_i, & \sigma\vec{e}_i U, & \vec{\delta}_i, & 0 &)_{\mathbb{B}^*_2}, \\
\boldsymbol{e}_{2,i} := & (& \omega\vec{e}_i, & \tau\vec{e}_i Z, & 0^2, & 0 &)_{\mathbb{B}_2},
\end{array}
$$

$$
\text{return } (\mathsf{param}_n, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t\}_{t=0,2}, \mathbb{B}_1, \mathbb{B}^*_1, \boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{1,i}\}_{i=1,..,n}, \{\boldsymbol{h}^*_{\beta,2,i}, \boldsymbol{e}_{2,i}\}_{i=1,2}),
$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. *For a probabilistic machine* $\mathcal{B}$, *the advantage of* $\mathcal{B}$ *for Problem 6,* $\mathsf{Adv}^{\mathsf{P6}}_{\mathcal{B}}(\lambda)$, *is similarly defined as in Definition 10.*

Lemma 18 *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, $\mathsf{Adv}^{\mathsf{P6}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}}(\lambda) + 5/q$.

Lemma 18 is proven in a manner similar to Lemma 2 in the full version of [23].

Lemma 19 *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, $|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}_0}(\lambda)$.

Lemma 19 is proven in a manner similar to Lemma 9 in the full version of [23].

Lemma 20 *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, $|\mathsf{Adv}^{(2\text{-}(h-1)\text{-}2)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P5}}_{\mathcal{B}_{1\text{-}h}}(\lambda) + 3\hat{\ell}/q$, *where* $\mathcal{B}_{1\text{-}h}(\cdot) := \mathcal{B}_1(h, \cdot)$ *and* $\hat{\ell}$ *is the maximum number of rows in access matrices of key queries.*

The proof of Lemma 20 is given in Appendix A.4.

Lemma 21 *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, $|\mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}2)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P5}}_{\mathcal{B}_{2\text{-}h}}(\lambda) + 3\hat{\ell}/q$, *where* $\mathcal{B}_{2\text{-}h}(\cdot) := \mathcal{B}_2(h, \cdot)$ *and* $\hat{\ell}$ *is the maximum number of rows in access matrices of key queries.*

The proof of Lemma 21 is given in Appendix A.4.

Lemma 22 *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, $|\mathsf{Adv}^{(3\text{-}(h-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3\text{-}h)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P6}}_{\mathcal{B}_{3\text{-}h}}(\lambda) + \mathsf{Adv}^{\mathsf{H,CR}}_{\mathcal{F}_{4\text{-}h}}(\lambda) + 3/q$, *where* $\mathcal{B}_{3\text{-}h}(\cdot) := \mathcal{B}_3(h, \cdot)$ *and* $\mathcal{F}_{4\text{-}h}(\cdot) := \mathcal{F}_4(h, \cdot)$.

Lemma 22 is proven in a manner similar to Lemma 16 in the full version of [27].

Lemma 23 *For any adversary* $\mathcal{A}$, *for any security parameter* λ, $|\mathsf{Adv}^{(3\text{-}\nu_S)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda)| \leq 1/q$.

Lemma 23 is proven in a manner similar to Lemma 17 in the full version of [27].

Lemma 24 *For any adversary* $\mathcal{A}$, *for any security parameter* λ, $\mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda) = 1/q$.

Lemma 24 is proven in a manner similar to Lemma 18 in the full version of [27].

References

[1] Shweta Agrawal, Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Functional encryption: New perspectives and lower bounds. In Canetti and Garay [8], pages 500–518.

[2] Nuttapong Attrapadung. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT*, volume 8441 of *LNCS*, pages 557–577. Springer, 2014.

[3] Nuttapong Attrapadung, Benoît Libert, and Elie de Panafieu. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In Catalano et al. [9], pages 90–108.

[4] Amos Beimel. Secure schemes for secret sharing and key distribution. *PhD Thesis, Israel Institute of Technology, Technion, Haifa*, 1996.

[5] Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size ciphertext. In Cramer [13], pages 440–456.

[6] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In Matthew K. Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 41–55. Springer, 2004.

[7] Dan Boneh, Craig Gentry, and Brent Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Victor Shoup, editor, *CRYPTO*, volume 3621 of *Lecture Notes in Computer Science*, pages 258–275. Springer, 2005.

[8] Ran Canetti and Juan A. Garay, editors. *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II*, volume 8043 of *Lecture Notes in Computer Science*. Springer, 2013.

[9] Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors. *Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings*, volume 6571 of *LNCS*. Springer, 2011.

[10] Cheng Chen, Jie Chen, Hoon Wei Lim, Zhenfeng Zhang, Dengguo Feng, San Ling, and Huaxiong Wang. Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures. In Ed Dawson, editor, *CT-RSA*, volume 7779 of *LNCS*, pages 50–67. Springer, 2013.

[11] Jie Chen and Hoeteck Wee. Semi-adaptive attribute-based encryption and improved delegation for boolean formula. *IACR Cryptology ePrint Archive*, 2014:465, 2014. To appear in SCN 2014.

[12] Jung Hee Cheon. Security analysis of the strong diffie-hellman problem. In Vaudenay [31], pages 1–11.

[13] Ronald Cramer, editor. *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *LNCS*. Springer, 2005.

[14] Cécile Delerablée. Identity-based broadcast encryption with constant size ciphertexts and private keys. In Kaoru Kurosawa, editor, *ASIACRYPT*, volume 4833 of *LNCS*, pages 200–215. Springer, 2007.

[15] Keita Emura, Atsuko Miyaji, Akito Nomura, Kazumasa Omote, and Masakazu Soshi. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. In Feng Bao, Hui Li, and Guilin Wang, editors, *ISPEC 2009*, volume 5451 of *LNCS*, pages 13–23. Springer, 2009.

[16] Sanjam Garg, Craig Gentry, Shai Halevi, Amit Sahai, and Brent Waters. Attribute-based encryption for circuits from multilinear maps. In Canetti and Garay [8], pages 479–499.

[17] Craig Gentry. Practical identity-based encryption without random oracles. In Vaudenay [31], pages 445–464.

[18] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Attribute-based encryption for circuits. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *STOC*, pages 545–554. ACM, 2013.

[19] Javier Herranz, Fabien Laguillaumie, and Carla Ràfols. Constant size ciphertexts in threshold attribute-based encryption. In Phong Q. Nguyen and David Pointcheval, editors, *PKC 2010*, volume 6056 of *LNCS*, pages 19–34. Springer, 2010.

[20] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. Attribute-based signatures. In Aggelos Kiayias, editor, *CT-RSA*, volume 6558 of *Lecture Notes in Computer Science*, pages 376–392. Springer, 2011.

[21] Shigeo Mitsunari, Ryuichi Sakai, and Masao Kasahara. A new traitor tracing. *IEICE Trans. Fundamentals*, E85-A(2):481–484, 2002.

[22] Tatsuaki Okamoto and Katsuyuki Takashima. Hierarchical predicate encryption for inner-products. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 214–231. Springer, 2009.

[23] Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 191–208. Springer, 2010. Full version is available at `http://eprint.iacr.org/2010/563`.

[24] Tatsuaki Okamoto and Katsuyuki Takashima. Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. In Dongdai Lin, Gene Tsudik, and Xiaoyun Wang, editors, *CANS 2011*, volume 7092 of *LNCS*, pages 138–159. Springer, 2011. Full version is available at `http://eprint.iacr.org/2011/648`.

[25] Tatsuaki Okamoto and Katsuyuki Takashima. Efficient attribute-based signatures for non-monotone predicates in the standard model. In Catalano et al. [9], pages 35–52. This is an extended abstract of a preliminary version of [27].

[26] Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure unbounded inner-product and attribute-based encryption. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT*, volume 7658 of *Lecture Notes in Computer Science*, pages 349–366. Springer, 2012. Full version is available at `http://eprint.iacr.org/2012/671`.

[27] Tatsuaki Okamoto and Katsuyuki Takashima. Efficient attribute-based signatures for non-monotone predicates in the standard model. *To appear in IEEE Trans. Cloud Computing*, 2014. Full version is available at `http://eprint.iacr.org/2011/700`.

[28] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In Cramer [13], pages 457–473.

[29] Yumi Sakemi, Goichiro Hanaoka, Tetsuya Izu, Masahiko Takenaka, and Masaya Yasuda. Solving a discrete logarithm problem with auxiliary input on a 160-bit elliptic curve. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC*, volume 7293 of *LNCS*, pages 595–608. Springer, 2012.

[30] Elaine Shi and Brent Waters. Delegating capabilities in predicate encryption systems. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *ICALP (2) 2008*, volume 5126 of *LNCS*, pages 560–578. Springer, 2008.

[31] Serge Vaudenay, editor. *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*, volume 4004 of *LNCS*. Springer, 2006.

[32] Brent Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 619–636. Springer, 2009.

[33] Shota Yamada, Nuttapong Attrapadung, Goichiro Hanaoka, and Noboru Kunihiro. A framework and compact constructions for non-monotonic attribute-based encryption. In Hugo Krawczyk, editor, *PKC 2014*, volume 8383 of *LNCS*, pages 275–292. Springer, 2014.

A Proofs of Lemmas

A.1 Proofs of Lemmas in Section 4

A.1.1 Proof of Lemma 2

Lemma 2 *$\mathcal{H}_{\vec{y}}(n,\mathbb{F}_q)$ has a linear structure as $\mathcal{H}_{\vec{y}}(n,\mathbb{F}_q) \cong A_{n-1} \setminus H_{n-2}$, where $A_{n-1} := \{\vec{u}' \in \mathbb{F}_q^n \,|\, \vec{y}\cdot\vec{u}' = y_n\}$ is an $(n-1)$-dimensional affine space and $H_{n-2} := A_{n-1} \cap \{u'_n = 0\}$ is a hyperplane section of A_{n-1}.*

For all $(Z_\kappa \in \mathcal{H}_{\vec{y}}(n,\mathbb{F}_q)^{\mathrm{T}})_{\kappa=1,\ldots,n}$ such that $(\widetilde{Z}_\kappa := Z_\kappa - Z_1)_{\kappa=2,\ldots,n}$ is a basis of linear subspace $V_{n-1} := \{\vec{u}' \in \mathbb{F}_q^n \,|\, \vec{y}\cdot\vec{u}' = 0\}$ over $\mathbb{F}_q$, the distribution of $Z := \sum_{\kappa=1}^n \xi_\kappa Z_\kappa$ with $(\xi_\kappa) \xleftarrow{\cup} \{(\xi_\kappa)_{\kappa=1,\ldots,n} : \sum_{\kappa=1}^n \xi_\kappa = 1\}$ is equivalent to uniform one, i.e., $Z \xleftarrow{\cup} \mathcal{H}_{\vec{y}}(n,\mathbb{F}_q)^{\mathrm{T}}$ except with negligible probability $1/q$.

Proof. It is directly verified that $\mathcal{H}_{\vec{y}}(n,\mathbb{F}_q)$ has a linear structure as $\mathcal{H}_{\vec{y}}(n,\mathbb{F}_q) \cong A_{n-1} \setminus H_{n-2}$. For $(\xi_\kappa) \xleftarrow{\cup} \{(\xi_\kappa)_{\kappa=1,\ldots,n} : \sum_{\kappa=1}^n \xi_\kappa = 1\}$,

$$Z := \sum_{\kappa=1}^n \xi_\kappa Z_\kappa = \sum_{\kappa=1}^n \xi_\kappa Z_1 + \sum_{\kappa=1}^n \xi_\kappa (Z_\kappa - Z_1) = Z_1 + \sum_{\kappa=2}^n \xi_\kappa \widetilde{Z}_\kappa, \tag{19}$$

where $\widetilde{Z}_\kappa := Z_\kappa - Z_1$. Since $(\widetilde{Z}_\kappa)_{\kappa=2,\ldots,n}$ is a basis of V_{n-1} and ξ_κ for $\kappa = 2,\ldots,n$ are independently and uniformly distributed in $\mathbb{F}_q$, Z given by Eq. (19) is uniformly distributed in affine space A_{n-1}. Moreover, Z is outside of H_{n-2} except with probability $1/q$, hence, uniformly distributed in $\mathcal{H}_{\vec{y}}(n,\mathbb{F}_q)^{\mathrm{T}}$ except with negligible probability $1/q$. □

A.1.2 Proof of Lemma 3

Lemma 3 *For all $\vec{y} \in \mathbb{F}_q^n - \mathsf{span}\langle \vec{e}_n \rangle$ and $\pi \in \mathbb{F}_q$, let $W_{\vec{y},\pi} := \{\vec{w} \in \mathbb{F}_q^n - \mathsf{span}\langle \vec{e}_n \rangle^{\perp} \mid \vec{y} \cdot \vec{w} = \pi\}$, where $\mathsf{span}\langle \vec{e}_n \rangle^{\perp} := \{\vec{w} \in \mathbb{F}_q^n \mid \vec{w} \cdot \vec{e}_n = 0\}$.*

For all $(\vec{y}, \vec{v}) \in \left(\mathbb{F}_q^n - \mathsf{span}\langle \vec{e}_n \rangle\right) \times \left(\mathbb{F}_q^n - \mathsf{span}\langle \vec{e}_n \rangle^{\perp}\right)$, if U and Z are generated as $U \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q), Z := (U^{-1})^{\mathrm{T}}$, then $\vec{v}Z$ is uniformly distributed in $W_{\vec{y},(\vec{y}\cdot\vec{v})}$.

Proof. Let $\begin{pmatrix} 1 & & u'_1 \\ & \ddots & \vdots \\ & 1 & u'_{n-1} \\ & & u'_n \end{pmatrix} := U$, $\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ -(u'_n)^{-1}u'_1 & \cdots & -(u'_n)^{-1}u'_{n-1} & (u'_n)^{-1} \end{pmatrix} := (U^{-1})^{\mathrm{T}} := Z$, and $\vec{u}' := (u'_1, \ldots, u'_n)$. Note that $\vec{u}' \cdot \vec{y} = y_n$. For $\vec{y} := (y_1, \ldots, y_n)$ and $\vec{v} := (v_1, \ldots, v_n)$ with $v_n \neq 0$, let

$$\begin{aligned} \vec{w} := \vec{v}Z &= (v_1 - u'_1(u'_n)^{-1}v_n, \ldots, v_{n-1} - u'_{n-1}(u'_n)^{-1}v_n, (u'_n)^{-1}v_n) \\ &= (u'_n)^{-1}v_n \cdot \left(\left(u'_n(v_1 v_n^{-1}) - u'_1\right), \ldots, \left(u'_n(v_{n-1}v_n^{-1}) - u'_{n-1}\right),\ 1\right) \\ &= (u'_n)^{-1}v_n \cdot (\widetilde{u}_1, \ldots, \widetilde{u}_{n-1}, 1), \end{aligned}$$

where $\widetilde{u}_j := u'_n(v_j v_n^{-1}) - u'_j$ for $j = 1, \ldots, n-1$ and $y_n := \vec{y} \cdot \vec{u}'$. Then,

$$\vec{y} \cdot \vec{v} = (u'_n)^{-1} v_n \left(\textstyle\sum_{j=1}^{n-1} y_j \widetilde{u}_j + y_n\right) = \vec{y} \cdot \vec{w}. \tag{20}$$

Case that $\vec{y} \cdot \vec{v} \neq 0$: Since $\vec{y}\cdot\vec{v} \neq 0$, $\vec{u}'$ can be generated as: $(\widetilde{u}_1, \ldots, \widetilde{u}_{n-1}) \xleftarrow{\mathsf{U}} \{(\widetilde{u}_j)_{j=1,\ldots,n-1} \in \mathbb{F}_q^{n-1} \mid \sum_{j=1}^{n-1} y_j\widetilde{u}_j + y_n \neq 0\}$, $u'_n := v_n(\sum_{j=1}^{n-1} y_j\widetilde{u}_j + y_n)/(\vec{y} \cdot \vec{v})$, and $u'_j := u'_n(v_j v_n^{-1}) - \widetilde{u}_j$ for $j = 1, \ldots, n-1$. We note that the condition $\sum_{j=1}^{n-1} y_j\widetilde{u}_j + y_n \neq 0$ among $\widetilde{u}_j$ $(j = 1, \ldots, n-1)$ is equivalent to the condition $u'_n \neq 0$.

Since $(\widetilde{u}_1, \ldots, \widetilde{u}_{n-1}) \xleftarrow{\mathsf{U}} \{(\widetilde{u}_j)_{j=1,\ldots,n-1} \in \mathbb{F}_q^{n-1} \mid \sum_{j=1}^{n-1} y_j\widetilde{u}_j + y_n \neq 0\}$ and $u'_n := v_n(\sum_{j=1}^{n-1} y_j\widetilde{u}_j + y_n)/(\vec{y} \cdot \vec{v})$, $\vec{w} := (u'_n)^{-1} v_n \cdot (\widetilde{u}_1, \ldots, \widetilde{u}_{n-1}, 1)$ is uniformly distributed in $W_{\vec{y},(\vec{y}\cdot\vec{v})}$.

Case that $\vec{y} \cdot \vec{v} = 0$: Since $\vec{y} \cdot \vec{v} = 0$, Eq. (20) is given as $\sum_{j=1}^{n-1} y_j\widetilde{u}_j + y_n = 0$. Since $\vec{y} \notin \mathsf{span}\langle \vec{e}_n \rangle$, there exists an index $j_0 \in \{1, \ldots, n-1\}$ such that $y_{j_0} \neq 0$. Using the index j_0, $\vec{u}'$ can be generated as: $\widetilde{u}_j \xleftarrow{\mathsf{U}} \mathbb{F}_q$ $(j = 1, \ldots, j_0 - 1, j_0 + 1, \ldots, n-1)$, $u'_{j_0} := (-\sum_{j=1,\ldots,j_0-1,j_0+1,n-1} y_j u'_j - y_n)/y_{j_0}$, $u'_n \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\times}$ and $u'_j := u'_n(v_j v_n^{-1}) - \widetilde{u}_j$ for $j = 1, \ldots, n-1$.

Since $(\widetilde{u}_1, \ldots, \widetilde{u}_{n-1}) \xleftarrow{\mathsf{U}} \{(\widetilde{u}_j)_{j=1,\ldots,n-1} \in \mathbb{F}_q^{n-1} \mid \sum_{j=1}^{n-1} y_j\widetilde{u}_j + y_n = 0\}$ and $u'_n \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\times}$, $\vec{w} := (u'_n)^{-1} v_n \cdot (\widetilde{u}_1, \ldots, \widetilde{u}_{n-1}, 1)$ is uniformly distributed in $W_{\vec{y},0}$. □

A.2 Proofs of Lemmas in Section 6.2.2

A.2.1 Proof of Lemma 5

Lemma 5 *For any adversary $\mathcal{C}$, there exist probabilistic machines $\mathcal{F}_1$ and $\mathcal{F}_2$, whose running time are essentially the same as that of $\mathcal{C}$, such that for any security parameter λ, $\mathsf{Adv}_{\mathcal{C}}^{\mathsf{P1}}(\lambda) \leq \mathsf{Adv}_{\mathcal{F}_1}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_2}^{\mathsf{DLIN}}(\lambda) + 10/q$.*

Lemma 5 is proven in a similar manner to Lemmas 1 and 2 in [23]. □

A.2.2 Proof of Lemma 6

Lemma 6 *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, $\mathsf{Adv}_{\mathcal{C}}^{\mathsf{P2}}(\lambda) \leq$*

$\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_1}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_2}(\lambda) + 10/q$.

Proof. To prove Lemma 6, we use an intermediate problem, Basic Problems 1, as indicated below.

Definition 16 (Basic Problem 1) *Basic Problem 1 is to guess β, given* $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \boldsymbol{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}^*_1, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i\}_{i=1,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{BP1}}_\beta(1^\lambda, n)$, *where*

$\mathcal{G}^{\mathsf{BP1}}_\beta(1^\lambda, n)$: $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n}, \mathbb{B}^*_1) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{KP\text{-}ABE}}_{\mathsf{ob}}(1^\lambda, 6, n)$,

$\widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, .., \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,3n+1}, .., \boldsymbol{b}_{1,6n})$ is calculated as in Eq. (2) from $\{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n}$,

$\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,\ \theta, \psi \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad \boldsymbol{e}_0 := \tau \boldsymbol{b}_{0,2}$,

for $i = 1, \ldots, n$; $\quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \quad \vec{\delta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$,

$$
\begin{array}{lcccccc}
 & & \overbrace{}^{n} & \overbrace{\phantom{0^{2n}}}^{2n} & \overbrace{\phantom{\psi\vec{e}_i,\ \vec{\delta}_i}}^{2n} & \overbrace{}^{n} & \\
\boldsymbol{h}^*_{0,i} := & (& 0^n, & 0^{2n}, & \psi\vec{e}_i,\ \vec{\delta}_i, & 0^n &)_{\mathbb{B}^*_1} \\
\boldsymbol{h}^*_{1,i} := & (& 0^n, & \theta\vec{e}_i,\ -\theta\vec{e}_i, & \psi\vec{e}_i,\ \vec{\delta}_i, & 0^n &)_{\mathbb{B}^*_1} \\
\boldsymbol{e}_i := & (& 0^n, & \tau\vec{e}_i,\ \tau\vec{e}_i, & 0^{2n}, & 0^n &)_{\mathbb{B}_1},
\end{array}
$$

return $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \boldsymbol{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}^*_1, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i\}_{i=1,\ldots,n})$,

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{D}$, the advantage of $\mathcal{D}$ for Basic Problem 1, $\mathsf{Adv}^{\mathsf{BP1}}_{\mathcal{D}}(\lambda)$, *is similarly defined as in Definition 10.*

Lemma 25 *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,* $\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{C}}(\lambda) \leq \mathsf{Adv}^{\mathsf{BP1}}_{\mathcal{D}_1}(\lambda) + \mathsf{Adv}^{\mathsf{BP1}}_{\mathcal{D}_2}(\lambda)$.

Lemma 26 *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,* $\mathsf{Adv}^{\mathsf{BP1}}_{\mathcal{D}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}}(\lambda) + 5/q$.

From Lemmas 25 and 26, we obtain Lemma 6. □

Below, we give proofs of Lemmas 25 and 26 in turn.

Proof of Lemma 25 To prove Lemma 25, we consider the following experiments. Problem 3 is the hybrid of the following Experiments $0, \ldots, 3$, i.e., $\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{C}}(\lambda) = \left|\mathsf{Pr}\left[\mathsf{Exp}^0_{\mathcal{C}}(\lambda) \to 1\right] - \mathsf{Pr}\left[\mathsf{Exp}^3_{\mathcal{C}}(\lambda) \to 1\right]\right|$. Therefore, from Lemmas 27–29, we obtain Lemma 25.

For a probabilistic adversary $\mathcal{C}$, we define Experiment 0, $\mathsf{Exp}^0_{\mathcal{C}}$, using Problem P2 generator $\mathcal{G}^{\mathsf{P2}}_0(1^\lambda, n)$ in Definition 11 as follows:

1. $\mathcal{C}$ is given $\varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P2}}_0(1^\lambda, n)$.
2. Output $\beta' \xleftarrow{\mathsf{R}} \mathcal{C}(1^\lambda, \varrho)$.

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

Experiment 0 $(\mathsf{Exp}^0_{\mathcal{C}})$ **:** $\beta = 0$ case of Basic Problem 3. That is,

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

where all variables are generated as in Basic Problem 3.

Experiment 1 ($\mathsf{Exp}^1_{\mathcal{C}}$) **:** Same as Experiment 0 except that

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

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

Experiment 2 ($\mathsf{Exp}^2_{\mathcal{C}}$) **:** Same as Experiment 1 except that

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

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

Experiment 3 ($\mathsf{Exp}^3_{\mathcal{C}}$) **:** Same as Experiment 2 except that

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

where all variables are generated as in Experiment 2.

Lemma 27 *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, $|\mathsf{Pr}[\mathsf{Exp}^1_{\mathcal{C}}(\lambda)\to 1]-\mathsf{Pr}[\mathsf{Exp}^0_{\mathcal{C}}(\lambda)\to 1]| \le \mathsf{Adv}^{\mathsf{BP1}}_{\mathcal{D}_1}(\lambda)$.*

Proof. Given a BP1 instance $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \boldsymbol{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}^*_1, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i\}_{i=1,\dots,n})$, $\mathcal{D}_1$ calculates $\rho \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\boldsymbol{f}^*_0 := \rho\boldsymbol{b}^*_{0,2}$, $\widetilde{\boldsymbol{h}}^*_i := \boldsymbol{h}^*_{\beta,i}+\rho\boldsymbol{b}^*_{1,n+i}+\boldsymbol{r}^*_i$ for $i=1,\dots,n$, where $\boldsymbol{r}^*_i \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}^*_{1,3n+1},\dots,\boldsymbol{b}^*_{1,5n}\rangle$ and $\boldsymbol{f}^*_i := \rho\boldsymbol{b}^*_{1,n+i}$ for $i=1,\dots,2n$. $\mathcal{D}_1$ then gives $\varrho := (\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \boldsymbol{f}^*_0, \boldsymbol{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}^*_1, \{\boldsymbol{f}^*_i\}_{i=1,\dots,2n}, \{\widetilde{\boldsymbol{h}}^*_{\beta,i}, \boldsymbol{e}_i\}_{i=1,\dots,n})$ 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 27. □

Lemma 28 *For any adversary $\mathcal{C}$, for any security parameter λ, $\mathsf{Pr}[\mathsf{Exp}^2_{\mathcal{C}}(\lambda)\to 1] = \mathsf{Pr}[\mathsf{Exp}^1_{\mathcal{C}}(\lambda)\to 1]$.*

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

Lemma 29 *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, $|\mathsf{Pr}[\mathsf{Exp}^3_{\mathcal{C}}(\lambda)\to 1]-\mathsf{Pr}[\mathsf{Exp}^2_{\mathcal{C}}(\lambda)\to 1]| \le \mathsf{Adv}^{\mathsf{BP1}}_{\mathcal{D}_2}(\lambda)$.*

Proof. Lemma 29 is proven in a similar manner to Lemma 27. □

Proof of Lemma 26 To prove Lemma 26, we use an intermediate problem, Basic Problems 2, as indicated below.

Definition 17 (Basic Problem 2) *Basic Problem 2 is to guess β, given* $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}_1, \mathbb{B}_1^*, \{\boldsymbol{h}^*_{\beta,i}\}_{i=1,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{BP2}}(1^\lambda, n)$, *where*

$$\mathcal{G}_\beta^{\mathsf{BP2}}(1^\lambda, n): \quad (\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n}, \mathbb{B}_1^*) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}^{\mathsf{KP\text{-}ABE}}(1^\lambda, 6, n),$$

$\widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, .., \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,3n+1}, .., \boldsymbol{b}_{1,6n})$ is calculated as in Eq. (2) from $\{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n}$,

$\theta, \psi \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

for $i = 1, \ldots, n$; $\quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n$, $\quad \vec{\delta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$,

$$\begin{array}{rcccccccc}
 & & \overbrace{\quad}^{n} & & \overbrace{\quad\quad}^{2n} & & \overbrace{\quad\quad\quad}^{2n} & & \overbrace{\quad}^{n} & \\
\boldsymbol{h}^*_{0,i} := & (& 0^n, & & 0^{2n}, & & \psi\vec{e}_i, \quad \vec{\delta}_i, & & 0^n &)_{\mathbb{B}_1^*} \\
\boldsymbol{h}^*_{1,i} := & (& 0^n, & & \theta\vec{e}_i, \quad 0^n, & & \psi\vec{e}_i, \quad \vec{\delta}_i, & & 0^n &)_{\mathbb{B}_1^*}
\end{array}$$

return $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}_1, \mathbb{B}_1^*, \{\boldsymbol{h}^*_{\beta,i}\}_{i=1,\ldots,n})$,

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{E}$, the advantage of $\mathcal{E}$ for Basic Problem 2, $\mathsf{Adv}_{\mathcal{E}}^{\mathsf{BP2}}(\lambda)$, *is similarly defined as in Definition 10.*

Lemma 30 *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,* $\mathsf{Adv}_{\mathcal{D}}^{\mathsf{BP1}}(\lambda) \leq \mathsf{Adv}_{\mathcal{E}}^{\mathsf{BP2}}(\lambda)$.

Proof. Given a BP2 instance $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}_1, \mathbb{B}_1^*, \{\boldsymbol{h}^*_{\beta,i}\}_{i=1,\ldots,n})$, $\mathcal{E}$ calculates $\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\boldsymbol{e}_0 := \tau\boldsymbol{b}_{0,2}$, $\boldsymbol{e}_i := \tau\boldsymbol{b}_{1,2n+i}$ for $i = 1, \ldots, n$ and $\widehat{\mathbb{B}}'_1 := (\boldsymbol{b}_{1,1}, \ldots, \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,3n+1}, \ldots, \boldsymbol{b}_{1,6n})$.

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

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

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

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

Therefore, when $\beta = 0$ (resp. $\beta = 1$), the distribution of ϱ is exactly same as that of instances from $\mathcal{G}_0^{\mathsf{BP1}}$ (resp. $\mathcal{G}_1^{\mathsf{BP1}}$). This completes the proof of Lemma 30. □

Lemma 31 *For any adversary $\mathcal{E}$, there is a probabilistic machine $\mathcal{F}$, whose running time is essentially the same as that of $\mathcal{E}$, such that for any security parameter λ,* $\mathsf{Adv}_{\mathcal{E}}^{\mathsf{BP2}}(\lambda) \leq \mathsf{Adv}_{\mathcal{F}}^{\mathsf{DLIN}}(\lambda) + 5/q$.

Lemma 31 is proven in a similar manner to Lemma 4 in the full version of [24]. □

A.2.3 Proofs of Lemmas 7–12

Lemma 7 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{C}_1$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,* $|\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) -$

$\mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{C}_1}(\lambda)$.

Lemma 7 is proven in a similar manner to Lemma 4 in [23]. Note that the simulator (challenger) provides $\mathcal{A}$ a part of the given Problem 1 instance as a public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_n, \{\widehat{\mathbb{B}}'_t\}_{t=0,1})$, which is independent from the target $\vec{y}$. □

Lemma 8 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{C}_2$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(2\text{-}(j-1)\text{-}2)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}j\text{-}1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{C}_{2\text{-}j}}(\lambda)$, where $\mathcal{C}_{2\text{-}j}(\cdot) := \mathcal{C}_2(j, \cdot)$.*

Proof. In order to prove Lemma 8, we construct a probabilistic machine $\mathcal{C}_2$ against Problem 2 using an adversary $\mathcal{A}$ in a security game (Game 2-$(j-1)$-2 or 2-j-1) as a black box as follows:

1. $\mathcal{C}_2$ is given an index j and a Problem 2 instance, $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \boldsymbol{f}^*_0, \boldsymbol{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}^*_1, \{\boldsymbol{f}^*_i\}_{i=1,\ldots,2n}, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i\}_{i=1,\ldots,n})$.

2. $\mathcal{C}_2$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.

3. $\mathcal{C}_2$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_n, \{\widehat{\mathbb{B}}'_t\}_{t=0,1})$ of Game 2-$(j-1)$-2 (and 2-j-1), where $\widehat{\mathbb{B}}'_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$ and $\widehat{\mathbb{B}}'_1 := (\boldsymbol{b}_{1,1}, \ldots, \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,5n+1}, \ldots, \boldsymbol{b}_{1,6n})$, that are obtained from the Problem 2 instance.

4. Then, $\mathcal{C}_2$ (or challenger) obtains challenge attributes Γ with $\Gamma := \{x_1, \ldots, x_{n'}\}$, and $\mathcal{C}_2$ calculates $\vec{y} := (y_1, \ldots, y_n)$ such that $\sum_{i=0}^{n-1} y_{n-i} z^i = z^{n-1-n'} \cdot \prod_{i=1}^{n'} (z - x_i)$. $\mathcal{C}_2$ generates $Z_\kappa := (\chi_{\kappa,\iota,l})_{\iota,l} \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}$ for $\kappa = 1, \ldots, j-1$.

5. When the h-th key query is issued for access structure $\mathbb{S}_h := (M_h, \rho_h)$, $\mathcal{C}_2$ generates $\vec{f}_h, \vec{g}_h \xleftarrow{\mathsf{U}} \mathbb{F}_q^r, (s_{h,1}, \ldots, s_{h,\ell})^{\mathrm{T}} := M_h \cdot \vec{f}_h^{\mathrm{T}}, (r_{h,1}, \ldots, r_{h,\ell})^{\mathrm{T}} := M_h \cdot \vec{g}_h^{\mathrm{T}}$, $s_{h,0} := \vec{1} \cdot \vec{f}_h^{\mathrm{T}}, r_{h,0} := \vec{1} \cdot \vec{g}_h^{\mathrm{T}}$, and answers as follows:

   $\mathcal{C}_2$ calculates $\boldsymbol{k}^*_0$ as given in Eq. (7) using $\mathbb{B}^*_0$ of the Problem 2 instance and $s_{h,0}, r_{h,0}$ above, and the i-th component,

$$\boldsymbol{k}^*_{h,i} := \boldsymbol{k}^{*\,\mathsf{norm}}_{h,i} + \sum_{\iota=1}^{n} p_{h,i,\iota} \left(\xi_{h,i,j+1} \boldsymbol{f}^*_\iota + \sum_{\kappa=1}^{j-1} \xi_{h,i,\kappa} \sum_{l=1}^{n} \chi_{\kappa,\iota,l} \boldsymbol{f}^*_{n+l} + \xi_{h,i,j} \boldsymbol{h}^*_{\beta,\iota} \right),$$

   where $\boldsymbol{k}^{*\,\mathsf{norm}}_{h,i}$ is a normal form given in Eq. (5) that is computed using $\mathbb{B}^*_1$ of the Problem 2 instance and $s_{h,i}$ above, $\vec{p}_{h,i} := (p_{h,i,1}, \ldots, p_{h,i,n})$ are given as $\vec{p}_{h,i} := r_{h,i}\vec{e}_1 + \widetilde{\psi}_{h,i}\vec{v}_{h,i}$ if $\rho_h(i) = v_{h,i}$, $\vec{p}_{h,i} := r_{h,i}\vec{v}_{h,i}$ if $\rho_h(i) = \neg v_{h,i}$, and $(\xi_{h,i,\kappa})_{\kappa=1,\ldots,j+1} \xleftarrow{\mathsf{U}} \{(\xi_\kappa)_{\kappa=1,\ldots,j+1} \in \mathbb{F}_q^{j+1} \mid \sum_{\kappa=1}^{j+1} \xi_\kappa = 1 \ \wedge \ \xi_{n+1} = 0 \text{ if } j = n\}$. $\mathcal{C}_2$ sends key $\mathsf{sk}_{\mathbb{S}_h} := (\mathbb{S}_h, \{\boldsymbol{k}^*_{h,i}\}_{i=0,\ldots,\ell})$ to $\mathcal{A}$.

6. When $\mathcal{C}_2$ receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ from $\mathcal{A}$, $\mathcal{C}_2$ selects (challenge) bit $b \xleftarrow{\mathsf{U}} \{0,1\}$. $\mathcal{C}_2$ computes the challenge ciphertext $(\boldsymbol{c}_0, \boldsymbol{c}_1, c_T)$ such that

$$\boldsymbol{c}_0 := \omega \boldsymbol{b}_{0,1} + \boldsymbol{e}_0 + \zeta \boldsymbol{b}_{0,3} + \varphi_0 \boldsymbol{b}_{0,5}, \quad \boldsymbol{c}_1 := \textstyle\sum_{\iota=1}^{n} y_\iota (\omega \boldsymbol{b}_{1,\iota} + \boldsymbol{e}_\iota + \varphi_1 \boldsymbol{b}_{1,5n+\iota}), \quad c_T := g_T^\zeta m^{(b)},$$

   where $\omega, \zeta, \varphi_0, \varphi_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and $(\boldsymbol{e}_0, \{\boldsymbol{e}_\iota\}_{\iota=1,\ldots,n})$, $\mathbb{B}_0, \widehat{\mathbb{B}}_1$ are a part of the Problem 2 instance.

7. When a key query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{C}_2$ executes the same procedure as that of step 5.

8. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{C}_2$ outputs $\beta' := 1$. Otherwise, $\mathcal{C}_2$ outputs $\beta' := 0$.

When $\beta = 0$ (resp. $\beta = 1$), the view of $\mathcal{A}$ is equivalent to that in Game 2-$(j-1)$-2 (resp. 2-j-1). This completes the proof of Lemma 8. □

Lemma 9 *For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}j\text{-}1)}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}j\text{-}2)}(\lambda)$.*

Proof. To prove Lemma 9, we will show distribution $(\mathsf{param}_n, \{\widehat{\mathbb{B}}_t\}_{t=0,1}, \{\mathsf{sk}_{\mathbb{S}}^{(j)*}\}_{j=1,\ldots,\nu}, \mathsf{ct}_\Gamma)$ in Games 2-j-1 and 2-j-2 are equivalent. For that purpose, we define new subbases $\boldsymbol{d}_{1,2n+1}, \ldots, \boldsymbol{d}_{1,3n}$ and $\boldsymbol{d}^*_{1,2n+1}, \ldots, \boldsymbol{d}^*_{1,3n}$ of $\mathbb{V}_1$ as follows:

For the target vector $\vec{y}$, we generate $U \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$. Then, let $Z := (U^{-1})^{\mathrm{T}}$. We note that $\vec{y} \cdot U = \vec{y}$. Then we set $(\boldsymbol{d}_{1,2n+1}, \ldots, \boldsymbol{d}_{1,3n})^{\mathrm{T}} := Z \cdot (\boldsymbol{b}_{1,2n+1}, \ldots, \boldsymbol{b}_{1,3n})^{\mathrm{T}}$ and $(\boldsymbol{d}^*_{1,2n+1}, \ldots, \boldsymbol{d}^*_{1,3n})^{\mathrm{T}} := U \cdot (\boldsymbol{b}^*_{1,2n+1}, \ldots, \boldsymbol{b}^*_{1,3n})^{\mathrm{T}}$ and

$$\mathbb{D}_1 := (\boldsymbol{b}_{1,1}, \ldots, \boldsymbol{b}_{1,2n}, \boldsymbol{d}_{1,2n+1}, \ldots, \boldsymbol{d}_{1,3n}, \boldsymbol{b}_{1,3n+1}, \ldots, \boldsymbol{b}_{1,6n}),$$
$$\mathbb{D}^*_1 := (\boldsymbol{b}^*_{1,1}, \ldots, \boldsymbol{b}^*_{1,2n}, \boldsymbol{d}^*_{1,2n+1}, \ldots, \boldsymbol{d}^*_{1,3n}, \boldsymbol{b}^*_{1,3n+1}, \ldots, \boldsymbol{b}^*_{1,6n}).$$

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 $\mathbb{B}^*_1$. The i-th component of the h-th queried keys $\{\boldsymbol{k}^*_{h,i}\}$ in Game 2-j-1 are expressed over bases $\mathbb{B}^*_1$ and $\mathbb{D}^*_1$ as follows.

$$\text{if } (\rho_h(i) = v_{h,i} \ \wedge \ v_{h,i} \notin \Gamma) \ \vee \ (\rho_h(i) = \neg v_{h,i} \ \wedge \ v_{h,i} \in \Gamma),$$
$$\boldsymbol{k}^*_{h,i} = (\ \overbrace{\cdots}^{2n} \ \overbrace{\vec{p}_{h,i} \cdot (\textstyle\sum_{\kappa=1}^{j-1} \xi_{h,i,\kappa} Z_\kappa + \xi_{h,i,j} I_n),}^{n} \ \overbrace{\cdots}^{3n} \ )_{\mathbb{B}^*_1}$$
$$= (\ \cdots \ \vec{p}_{h,i} \cdot (\textstyle\sum_{\kappa=1}^{j-1} \xi_{h,i,\kappa} Z_\kappa + \xi_{h,i,j} I_n) \cdot Z, \ \cdots \ )_{\mathbb{D}^*_1},$$
$$= (\ \cdots \ \vec{p}_{h,i} \cdot (\textstyle\sum_{\kappa=1}^{j} \xi_{h,i,\kappa} \widetilde{Z}_\kappa), \ \cdots \ )_{\mathbb{D}^*_1},$$
$$\text{otherwise,}$$
$$\boldsymbol{k}^*_{h,i} = (\ \overbrace{\cdots}^{2n} \ \overbrace{0^n,}^{n} \ \overbrace{\cdots}^{3n} \ )_{\mathbb{B}^*_1} = (\ \overbrace{\cdots}^{2n} \ \overbrace{0^n,}^{n} \ \overbrace{\cdots}^{3n} \ )_{\mathbb{D}^*_1},$$

where $\vec{p}_{h,i}$ are given as $\vec{p}_{h,i} := r_{h,i}\vec{e}_1 + \widetilde{\psi}_{h,i}\vec{v}_{h,i}$ if $\rho_h(i) = v_{h,i}$, $\vec{p}_{h,i} := r_{h,i}\vec{v}_{h,i}$ if $\rho_h(i) = \neg v_{h,i}$, $(\xi_{h,i,\kappa})_{\kappa=1,\ldots,j+1} \xleftarrow{\mathsf{U}} \{(\xi_\kappa)_{\kappa=1,\ldots,j+1} \in \mathbb{F}_q^{j+1} \mid \sum_{\kappa=1}^{j+1} \xi_\kappa = 1 \ \wedge \ \xi_{n+1} = 0 \text{ if } j = n\}$, and $\widetilde{Z}_\kappa := Z_\kappa Z$ for $\kappa = 1, \ldots, j-1$, $\widetilde{Z}_j := Z$ are independently and uniformly distributed in $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}$ since $Z_\kappa, Z \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}$.

Therefore, the distribution $(\mathsf{param}_n, \{\widehat{\mathbb{D}}_t\}_{t=0,1}, \{\mathsf{sk}_{\mathbb{S}}^{(j)*}\}_{j=1,\ldots,\nu}, \mathsf{ct}_\Gamma)$ is equivalent to that in Game 2-j-2. This completes the proof of Lemma 9. □

Lemma 10 *For any adversary $\mathcal{A}$, for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}n\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)| \leq 3\nu\hat{\ell}/q$, where ν is the maximum number of $\mathcal{A}$'s key queries, and $\hat{\ell}$ is the maximum number of rows in access matrices of key queries.*

Proof. The i-th component of the h-th queried key $\{\boldsymbol{k}^*_{h,i}\}$ in Game 2-n-2 is expressed over basis $\mathbb{B}^*_1$ as follows.

$$\text{if } (\rho_h(i) = v_{h,i} \ \wedge \ v_{h,i} \notin \Gamma) \ \vee \ (\rho_h(i) = \neg v_{h,i} \ \wedge \ v_{h,i} \in \Gamma),$$
$$\boldsymbol{k}^*_{h,i} = (\ \overbrace{\cdots}^{2n} \ \overbrace{\vec{p}_{h,i} \cdot (\textstyle\sum_{\kappa=1}^{n} \xi_{h,i,\kappa} Z_\kappa),}^{n} \ \overbrace{\cdots}^{3n} \ )_{\mathbb{B}^*_1},$$
$$\text{otherwise, } \boldsymbol{k}^*_{h,i} = (\ \overbrace{\cdots}^{2n} \ \overbrace{0^n,}^{n} \ \overbrace{\cdots}^{3n} \ )_{\mathbb{B}^*_1},$$

where $\vec{p}_{h,i}$ are given as $\vec{p}_{h,i} := r_{h,i}\vec{e}_1 + \widetilde{\psi}_{h,i}\vec{v}_{h,i}$ if $\rho_h(i) = v_{h,i}$, $\vec{p}_{h,i} := r_{h,i}\vec{v}_{h,i}$ if $\rho_h(i) = \neg v_{h,i}$, $(\xi_{h,i,\kappa})_{\kappa=1,\ldots,n} \xleftarrow{\mathsf{U}} \{(\xi_\kappa)_{\kappa=1,\ldots,n} \in \mathbb{F}_q^n \mid \sum_{\kappa=1}^n \xi_\kappa = 1\}$, and $Z_\kappa \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}$ for $\kappa = 1, \ldots, n$.

We note that $\{\widetilde{Z}_\kappa := Z_\kappa - Z_1\}_{\kappa=2,\ldots,n}$ (given by $\{\vec{u}'_\kappa := (u'_{\kappa,1}, \ldots, u'_{\kappa,n}) \in \mathbb{F}_q^n\}_{\kappa=2,\ldots,n}$) are linearly independent except that the matrix $(\vec{u}'_\kappa)_{\kappa=2,\ldots,n} \in \mathbb{F}_q^{(n-1)\times n}$ does not have maximal rank $n-1$, i.e., except for probability $1/q$. Therefore, from Lemma 2, since $(\xi_{h,i,\kappa})_{\kappa=1,\ldots,n}$ are freshly random for each key component indexed by (h,i) and $\sum_{\kappa=1}^n \xi_{h,i,\kappa} = 1$, each $Z_{h,i} := \sum_{\kappa=1}^n \xi_{h,i,\kappa} Z_\kappa$ in the hidden subspace is freshly random except with negligible probability $1/q$. Therefore, $\boldsymbol{k}^*_{h,i}$ are distributed as

$$\text{if } (\rho_h(i) = v_{h,i} \ \wedge \ v_{h,i} \notin \Gamma) \ \vee \ (\rho_h(i) = \neg v_{h,i} \ \wedge \ v_{h,i} \in \Gamma),$$

$$\boldsymbol{k}^*_{h,i} = (\ \overbrace{\cdots}^{n} \ \overbrace{\qquad 0^n,\ \vec{p}_{h,i} \cdot Z_{h,i},\qquad}^{2n} \ \overbrace{\cdots}^{3n}\ )_{\mathbb{B}^*_1},$$

$$\text{otherwise, } \boldsymbol{k}^*_{h,i} = (\ \overbrace{\cdots}^{n} \ \overbrace{\qquad \vec{p}_{h,i},\ 0^n,\qquad}^{2n} \ \overbrace{\cdots}^{3n}\ )_{\mathbb{B}^*_1},$$

where $Z_{h,i}$ are freshly random (except with negligible probability).

From Lemma 3, $\vec{w}_{h,i} := \vec{p}_{h,i} \cdot Z_{h,i}$ are distributed as $\vec{w}_{h,i} \xleftarrow{\mathsf{U}} \{\vec{w} \mid \vec{w} \cdot \vec{y} = (r_{h,i}\vec{e}_1 + \widetilde{\psi}_{h,i}\vec{v}_{h,i}) \cdot \vec{y}\}$ if $\rho_h(i) = v_{h,i}$, $\vec{w}_{h,i} \xleftarrow{\mathsf{U}} \{\vec{w} \mid \vec{w} \cdot \vec{y} = r_{h,i}\vec{v}_{h,i} \cdot \vec{y}\}$ if $\rho(i) = \neg v_i$. Hence, $\vec{w}_{h,i}$ are distributed as $\vec{w}_{h,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ if $\rho_h(i) = v_{h,i} \wedge v_{h,i} \notin \Gamma$ and $\vec{w}_{h,i} \xleftarrow{\mathsf{U}} \mathsf{span}\langle\vec{y}\rangle^\perp$ if $\rho_h(i) = \neg v_{h,i} \wedge v_{h,i} \in \Gamma$ except with negligible probability $1/q$, i.e., $\boldsymbol{k}^*_{h,i}$ are distributed as in Eq. (12). The corresponding shares $r_{h,i}$ are information-theoretically hidden from the adversary $\mathcal{A}$. Also, $r_{h,i}$ obtained from the other indexes i for the h-th query are independent from a central secret $r_{h,0}$. From this independence, Game 2-n-2 can be conceptually changed to Game 3, i.e., $\boldsymbol{k}^*_{h,0}$ are distributed as in Eq. (12). This completes the proof of Lemma 10. □

Lemma 11 *For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda)$.*

Proof. Lemma 11 is proven in a similar manner to Lemma 7 in [23]. □

Lemma 12 *For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda) = 0$.*

Proof. The value of b is independent from the adversary's view in Game 4. Hence, $\mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda) = 0$. □

A.3 Proofs of Lemmas in Section 6.4

A.3.1 Proof of Lemma 14

Lemma 14 *Problem 3 is computationally intractable under the DLIN assumption.*

For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{F}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ,
$\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) \ \leq \sum_{j=0}^{n} \sum_{\iota=1}^{2} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{j\text{-}\iota}}(\lambda) + (10n+10)/q$, *where $\mathcal{F}_{j\text{-}\iota}(\cdot) := \mathcal{F}(j, \iota, \cdot)$.*

To prove Lemma 14, we consider the following $2n+3$ experiments. For a probabilistic adversary $\mathcal{B}$, we define Experiment 0, $\mathsf{Exp}^0_{\mathcal{B}}$, using Problem 3 generator (or challenger) in Definition 12 as follows:

1. $\mathcal{B}$ is given the first part of a P3 instance ϱ_1 given in step 1 in Definition 12.

2. $\mathcal{B}$ outputs the target $\vec{y}$ to the challenger, and is given the second part of a P3 instance ϱ_2 given in step 2 in Definition 12.

3. $\mathcal{B}$ outputs $\beta' \in \{0,1\}$.

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

In Experiment 0, a part framed by a box indicates positions of 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 ($\mathsf{Exp}^0_{\mathcal{B}}$) **:** Experiment 0 is defined by using $\beta = 0$ instance of Problem 3 as above. That is, $\delta, \delta_0, \omega, \varphi_0, \varphi_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\tau, \rho \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\times}$, and

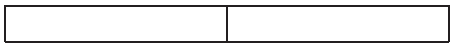
$$\boldsymbol{h}^*_0 := (\delta, \boxed{0}, 0, \delta_0, 0)_{\mathbb{B}^*_0}, \quad \boldsymbol{e}_0 := (\omega, \boxed{0}, 0, 0, \varphi_0)_{\mathbb{B}_0},$$

$$\text{for } j = 1, \ldots, n;\ i = 1, \ldots, n; \quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \quad \vec{\delta}_{j,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n},$$

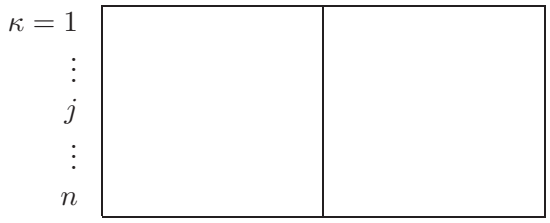
$$\begin{array}{lccccccc} & \overbrace{}^{n} & & \overbrace{}^{2n} & & \overbrace{}^{2n} & \overbrace{}^{n} & \\ \boldsymbol{h}^*_{j,i} := & (& \delta\vec{e}_i, & \boxed{0^{2n}}, & & \vec{\delta}_{j,i}, & 0^n &)_{\mathbb{B}^*_1} \\ \boldsymbol{e}_1 := & (& \omega\vec{y}, & \boxed{0^{2n}}, & & 0^{2n}, & \varphi_1\vec{y} &)_{\mathbb{B}_1}, \end{array}$$

Below, we describe coefficients of the hidden part, i.e., $\mathsf{span}\langle \boldsymbol{b}_{1,n+1}, \ldots, \boldsymbol{b}_{1,3n} \rangle$ (resp. $\mathsf{span}\langle \boldsymbol{b}^*_{1,n+1}, \ldots, \boldsymbol{b}^*_{1,3n} \rangle$) of $\boldsymbol{e}_1$ (resp. $\boldsymbol{h}^*_{\kappa,i}$) w.r.t. these bases vectors for $\kappa = 1, \ldots, n$. 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 $\boldsymbol{e}_1$ in Experiment 0



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



Experiment 1 ($\mathsf{Exp}^1_{\mathcal{B}}$) **:** Same as Experiment 0 except that $\boldsymbol{h}^*_0, \boldsymbol{h}^*_{j,i}$ and $\boldsymbol{e}_0, \boldsymbol{e}_1$ are:

$$\boldsymbol{h}^*_0 := (\delta, \boxed{\rho}, 0, \delta_0, 0)_{\mathbb{B}^*_0}, \quad \boldsymbol{e}_0 := (\omega, \boxed{\tau}, 0, 0, \varphi_0)_{\mathbb{B}_0},$$

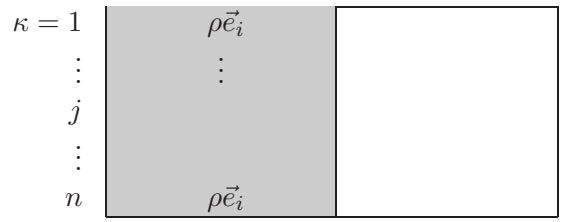
$$\text{for } j = 1, \ldots, n;\ i = 1, \ldots, n; \quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \quad \vec{\delta}_{j,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n},$$

$$\begin{array}{lccccccc} & \overbrace{}^{n} & & \overbrace{}^{2n} & & \overbrace{}^{2n} & \overbrace{}^{n} & \\ \boldsymbol{h}^*_{j,i} := & (& \delta\vec{e}_i, & \boxed{\rho\vec{e}_i}, & 0^n, & \vec{\delta}_{j,i}, & 0^n &)_{\mathbb{B}^*_1} \\ \boldsymbol{e}_1 := & (& \omega\vec{y}, & \boxed{\tau\vec{y}}, & \boxed{\tau\vec{y}}, & 0^{2n}, & \varphi_1\vec{y} &)_{\mathbb{B}_1}, \end{array}$$

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

Coefficients of the hidden part of $\boldsymbol{e}_1$ in Experiment 1

Coefficients of the hidden part of $\boldsymbol{h}^*_{\kappa,i}$ in Experiment 1



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

$\tau\vec{y}$	$\tau\vec{y}$

Coefficients of the hidden part of $\boldsymbol{h}^*_{\kappa,i}$ 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 $(\mathsf{Exp}^{\text{2-}j\text{-1}}_{\mathcal{B}}, \boldsymbol{j = 1, \ldots, n})$ **:** 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 $\boldsymbol{h}^*_{j,i}$ are:

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

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

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

$\tau\vec{y}$	$\tau\vec{y}$

Coefficients of the hidden part of $\boldsymbol{h}^*_{\kappa,i}$ 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 $(\mathsf{Exp}^{\text{2-}j\text{-2}}_{\mathcal{B}}, \boldsymbol{j = 1, \ldots, n})$ **:** Experiment 2-j-2 is the same as Experiment 2-j-1 except the j-th component $\boldsymbol{h}^*_{j,i}$ are:

$$\text{for } i = 1, \ldots, n; \qquad U_j \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q), \quad Z_j := (U_j^{-1})^{\mathrm{T}},$$

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

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

Coefficients of the hidden part of $\boldsymbol{e}_1$ in Experiment 2-j-2

$\tau\vec{y}$	$\tau\vec{y}$

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

$\kappa = 1$		$\rho\vec{e}_i Z_1$
$\vdots$		$\vdots$
j		$\rho\vec{e}_i Z_j$
$\vdots$	$\vdots$	
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.

Coefficients of the hidden part of $\boldsymbol{e}_1$ in Experiment 2-n-2

$\tau\vec{y}$	$\tau\vec{y}$

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

$\kappa = 1$		$\rho\vec{e}_i Z_1$
$\vdots$		$\vdots$
j		$\rho\vec{e}_i Z_j$
$\vdots$		$\vdots$
n		$\rho\vec{e}_i Z_n$

We will show three lemmas (Lemmas 32-34) that evaluate the gaps between pairs of $\mathsf{Pr}[\mathsf{Exp}^0_{\mathcal{B}}(\lambda) \to 1], \mathsf{Pr}[\mathsf{Exp}^1_{\mathcal{B}}(\lambda) \to 1]$ and $\mathsf{Pr}[\mathsf{Exp}^{2\text{-}j\text{-}\iota}_{\mathcal{B}}(\lambda) \to 1]$ for $j = 1, \ldots, n$; $\iota = 1, 2$. From these lemmas and Lemmas 5 and 6, we obtain $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) = |\mathsf{Pr}[\mathsf{Exp}^0_{\mathcal{B}}(\lambda) \to 1] - \mathsf{Pr}[\mathsf{Exp}^{2\text{-}n\text{-}2}_{\mathcal{B}}(\lambda) \to 1]| \leq \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{C}_0}(\lambda) + \sum_{j=1}^{n} \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{C}_j}(\lambda) \leq \sum_{j=0}^{n}\sum_{\iota=1}^{2} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{j,\iota}}(\lambda) + (10n+10)/q$. This completes the proof of Lemma 14. □

Lemma 32 *For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{C}_0$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $|\mathsf{Pr}[\mathsf{Exp}^1_{\mathcal{B}}(\lambda) \to 1] - \mathsf{Pr}[\mathsf{Exp}^0_{\mathcal{B}}(\lambda) \to 1]| \leq \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{C}_0}(\lambda)$.*

Proof. $\mathcal{C}_0$ is given a P1 instance $(\mathsf{param}_n, \{\mathbb{B}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,1}, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_{\beta,i}\}_{i=0,\ldots,n})$ and a target vector $\vec{y}$. $\mathcal{C}_0$ then calculates $(\mathsf{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,1})$ in Experiment 0, and calculates $\boldsymbol{e}'_0 := \boldsymbol{e}_{\beta,0}, \boldsymbol{e}'_1 := \sum_{\iota=1}^{n} y_\iota \boldsymbol{e}_{\beta,\iota}, \boldsymbol{h}'^*_0 := \boldsymbol{h}^*_{\beta,0}, \{\boldsymbol{h}'^*_{j,i} := \boldsymbol{h}^*_{\beta,i} + \sum_{\iota=1}^{n} \delta_{j,i,\iota} \boldsymbol{b}_{1,3n+\iota}\}_{j=1,\ldots,n;\, i=1,\ldots,n}$ with $\delta_{j,i,\iota} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, sends $\varrho := (\mathsf{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,1}, \boldsymbol{h}'^*_0, \boldsymbol{e}'_0, \{\boldsymbol{h}'^*_{j,i}\}_{j=1,\ldots,n;\, i=1,\ldots,n}, \boldsymbol{e}'_1)$ to $\mathcal{B}$. $\mathcal{C}_0$ 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 32. □

Lemma 33 *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, $|\mathsf{Pr}[\mathsf{Exp}^{2\text{-}(j-1)\text{-}2}_{\mathcal{B}}(\lambda) \to 1] - \mathsf{Pr}[\mathsf{Exp}^{2\text{-}j\text{-}1}_{\mathcal{B}}(\lambda) \to 1]| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{C}_j}(\lambda)$, where $\mathcal{C}_j(\cdot) := \mathcal{C}(j, \cdot)$ $(j \geq 1)$.*

Proof. $\mathcal{C}$ is given a P2 instance $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \boldsymbol{f}^*_0, \boldsymbol{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}^*_1, \{\boldsymbol{f}^*_i\}_{i=1,\ldots,2n}, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i\}_{i=1,\ldots,n})$, a target vector $\vec{y}$ and an index j. $\mathcal{C}$ then calculates $(\mathsf{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,1}, \boldsymbol{h}'^*_0 := \delta \boldsymbol{b}^*_{0,1} + \boldsymbol{f}^*_0 + \delta_0 \boldsymbol{b}^*_{0,5}, \boldsymbol{e}'_0 := \omega \boldsymbol{b}_{0,1} + \boldsymbol{e}_0 + \varphi_0 \boldsymbol{b}_{0,5}, \boldsymbol{e}'_1 := \sum_{\iota=1}^{n} y_\iota(\omega \boldsymbol{b}_{1,\iota} + \boldsymbol{e}_\iota + \varphi_1 \boldsymbol{b}_{1,5n+\iota}))$ in Experiment 2-$(j-1)$-2 with $\delta, \delta_0, \omega, \varphi_0, \varphi_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and calculates

$$
\begin{aligned}
&\text{if } \kappa < j;\ \text{for } i = 1, \ldots, n,\ \boldsymbol{h}'^*_{\kappa,i} := \delta \boldsymbol{b}^*_{1,i} + \textstyle\sum_{\iota=1}^{n} (\chi_{\kappa,i,\iota} \boldsymbol{f}^*_{n+\iota} + \delta_{\kappa,i,\iota} \boldsymbol{b}^*_{1,3n+\iota}) \\
&\qquad \text{where } Z_\kappa \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}},\ (\chi_{\kappa,i,1}, \ldots, \chi_{\kappa,i,n}) := \vec{e}_i \cdot Z_\kappa,\ \delta_{\kappa,i,\iota} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \\
&\text{if } \kappa = j;\ \text{for } i = 1, \ldots, n,\ \boldsymbol{h}'^*_{j,i} := \delta \boldsymbol{b}^*_{1,i} + \boldsymbol{h}^*_{\beta,i} + \textstyle\sum_{\iota=1}^{n} \delta_{j,i,\iota} \boldsymbol{b}^*_{1,3n+\iota} \text{ where } \delta_{j,i,\iota} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \\
&\text{if } \kappa > j;\ \text{for } i = 1, \ldots, n,\ \boldsymbol{h}'^*_{\kappa,i} := \delta \boldsymbol{b}^*_{1,i} + \boldsymbol{f}^*_i + \textstyle\sum_{\iota=1}^{n} \delta_{\kappa,i,\iota} \boldsymbol{b}^*_{1,3n+\iota} \text{ where } \delta_{\kappa,i,\iota} \xleftarrow{\mathsf{U}} \mathbb{F}_q,
\end{aligned}
$$

and sends $\varrho := (\mathsf{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,1}, \boldsymbol{h}'^*_0, \boldsymbol{e}'_0, \{\boldsymbol{h}'^*_{j,i}\}_{j=1,\ldots,n;\, i=1,\ldots,n}, \boldsymbol{e}'_1)$ 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 33. □

Lemma 34 *For any adversary $\mathcal{B}$, for any security parameter λ,*
$\mathsf{Pr}[\mathsf{Exp}^{2\text{-}j\text{-}1}_{\mathcal{B}}(\lambda) \to 1] = \mathsf{Pr}[\mathsf{Exp}^{2\text{-}j\text{-}2}_{\mathcal{B}}(\lambda) \to 1]$.

Proof. To prove Lemma 34, we will show distribution $(\mathsf{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,1}, \boldsymbol{h}^*_0, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{j,i}\}_{j=1,\ldots,n;\, i=1,\ldots,n}, \boldsymbol{e}_1)$ in Experiments 2-j-1 and 2-j-2 are equivalent. For that purpose, we define new subbases $\boldsymbol{d}_{1,2n+1}, \ldots, \boldsymbol{d}_{1,3n}$ and $\boldsymbol{d}^*_{1,2n+1}, \ldots, \boldsymbol{d}^*_{1,3n}$ of $\mathbb{V}_1$ as follows:

For the target vector $\vec{y} := (y_1, \ldots, y_n)$, we generate $U \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ and $Z := (U^{-1})^{\mathrm{T}}$. We note that $\vec{y} \cdot U = \vec{y}$. Then we set $(\boldsymbol{d}_{1,2n+1}, \ldots, \boldsymbol{d}_{1,3n})^{\mathrm{T}} := Z \cdot (\boldsymbol{b}_{1,2n+1}, \ldots, \boldsymbol{b}_{1,3n})^{\mathrm{T}}$ and $(\boldsymbol{d}^*_{1,2n+1}, \ldots, \boldsymbol{d}^*_{1,3n})^{\mathrm{T}} := U \cdot (\boldsymbol{b}^*_{1,2n+1}, \ldots, \boldsymbol{b}^*_{1,3n})^{\mathrm{T}}$ and

$$\mathbb{D}_1 := (\boldsymbol{b}_{1,1}, \ldots, \boldsymbol{b}_{1,2n}, \boldsymbol{d}_{1,2n+1}, \ldots, \boldsymbol{d}_{1,3n}, \boldsymbol{b}_{1,3n+1}, \ldots, \boldsymbol{b}_{1,6n}),$$
$$\mathbb{D}^*_1 := (\boldsymbol{b}^*_{1,1}, \ldots, \boldsymbol{b}^*_{1,2n}, \boldsymbol{d}^*_{1,2n+1}, \ldots, \boldsymbol{d}^*_{1,3n}, \boldsymbol{b}^*_{1,3n+1}, \ldots, \boldsymbol{b}^*_{1,6n}).$$

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 $\{\boldsymbol{h}^*_{j,i}\}$ in Experiment 2-j-1 are expressed over bases $\mathbb{B}^*_1$ and $\mathbb{D}^*_1$ as follows.

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

where $Z_j := Z$ and $\{Z'_\kappa := Z_\kappa \cdot Z\}_{\kappa<j}$ are independently and uniformly distributed in $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}$ since $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ is a subgroup of $GL(n, \mathbb{F}_q)$ (Lemma 1). Since $\vec{y} \cdot U = \vec{y}$, $\boldsymbol{e}_1$ has the same representations over both $\mathbb{B}_1$ and $\mathbb{D}_1$.

Therefore, the distribution of $(\mathsf{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,1}, \boldsymbol{h}^*_0, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{j,i}\}_{j=1,\ldots,n;\, i=1,\ldots,n}, \boldsymbol{e}_1)$ in Experiments 2-j-1 and 2-j-2 are equivalent. This completes the proof of Lemma 34. □

A.3.2 Proof of Lemma 15

Lemma 15 *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, $|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) + 3\nu\hat{\ell}/q$, where ν is the maximum number of $\mathcal{A}$'s key queries, $\hat{\ell}$ is the maximum number of rows in access matrices of key queries.*

Proof. In order to prove Lemma 15, we construct a probabilistic machine $\mathcal{B}$ against Problem 3 using an adversary $\mathcal{A}$ in a security game (Game 0 or 3) as a black box as follows:

1. $\mathcal{B}$ is given the first part of a Problem 3 instance, which is given in step 1 in Definition 12, $(\mathsf{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,1})$.
2. $\mathcal{B}$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.
3. $\mathcal{B}$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_n, \{\widehat{\mathbb{B}}'_t\}_{t=0,1})$ of Game 2-$(j-1)$-2 (and 2-j-1), where $\widehat{\mathbb{B}}'_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$ and $\widehat{\mathbb{B}}'_1 := (\boldsymbol{b}_{1,1}, \ldots, \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,5n+1}, \ldots, \boldsymbol{b}_{1,6n})$, that are obtained from the Problem 3 instance.
4. When $\mathcal{B}$ (or challenger) obtains challenge attributes Γ with $\Gamma := \{x_1, \ldots, x_{n'}\}$ in the first step of the game, $\mathcal{B}$ calculates $\vec{y} := (y_1, \ldots, y_n)$ 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 gives $\vec{y}$ to the challenger of Problem 3. Then, $\mathcal{B}$ is given the second part of the Problem 3 instance, which is given in step 2 in Definition 12, $(\boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{h}^*_{\beta,j,i}\}_{j=1,\ldots,n;\, i=1,\ldots,n}, \boldsymbol{e}_{\beta,1})$.

5. When the h-th key query is issued for access structure $\mathbb{S}_h := (M_h, \rho_h)$, $\mathcal{B}$ generates $\vec{f}_h, \vec{g}_h \xleftarrow{\mathsf{U}} \mathbb{F}_q^r, (s_{h,1}, \ldots, s_{h,\ell})^{\mathrm{T}} := M_h \cdot \vec{f}_h^{\mathrm{T}}, (r_{h,1}, \ldots, r_{h,\ell})^{\mathrm{T}} := M_h \cdot \vec{g}_h^{\mathrm{T}}$, $s_{h,0} := \vec{1} \cdot \vec{f}_h^{\mathrm{T}}, r_{h,0} := \vec{1} \cdot \vec{g}_h^{\mathrm{T}}$, and answers as follows: $\mathcal{B}$ calculates

$$\boldsymbol{k}_0^* := \boldsymbol{h}_0^* + \boldsymbol{b}_{0,3}^*, \quad \boldsymbol{k}_{h,i}^* := \boldsymbol{k}_{h,i}^{*\,\mathsf{norm}} + \sum_{j,\iota=1}^{n} \xi_{h,i,j} p_{h,i,\iota} \boldsymbol{h}_{\beta,j,\iota}^* \text{ for } i = 1, \ldots, \ell,$$

where $\boldsymbol{k}_{h,i}^{*\,\mathsf{norm}}$ is a normal form given in Eq. (5) that is computed using $\mathbb{B}_1^*$ of the Problem 3 instance and $s_{h,i}$ above, $\vec{p}_{h,i} := (p_{h,i,1}, \ldots, p_{h,i,n})$ are given as $\vec{p}_{h,i} := r_{h,i}\vec{e}_1 + \widetilde{\psi}_{h,i}\vec{v}_{h,i}$ if $\rho_h(i) = v_{h,i}$, $\vec{p}_{h,i} := r_{h,i}\vec{v}_{h,i}$ if $\rho_h(i) = \neg v_{h,i}$, and $(\xi_{h,i,j})_{j=1,\ldots,n} \xleftarrow{\mathsf{U}} \{(\xi_j)_{j=1,\ldots,n} \in \mathbb{F}_q^n \mid \sum_{j=1}^n \xi_j = 1\}$.

6. When $\mathcal{B}$ receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ from $\mathcal{A}$, $\mathcal{B}$ selects (challenge) bit $b \xleftarrow{\mathsf{U}} \{0,1\}$. $\mathcal{B}$ computes the challenge ciphertext $(\boldsymbol{c}_0, \boldsymbol{c}_1, c_T)$ such that

$$\boldsymbol{c}_0 := \boldsymbol{e}_{\beta,0} + \zeta \boldsymbol{b}_{0,3}, \quad \boldsymbol{c}_1 := \boldsymbol{e}_{\beta,1}, \quad c_T := g_T^{\zeta} m^{(b)},$$

where $\zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and $(\boldsymbol{e}_{\beta,0}, \boldsymbol{b}_{0,3}, \boldsymbol{e}_{\beta,1})$ is a part of the Problem 3 instance.

7. When a key query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{B}$ executes the same procedure as that of step 5.

8. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}$ outputs $\beta' := 0$.

When $\beta = 0$ (resp. $\beta = 1$), the view of $\mathcal{A}$ is equivalent to that in Game 0 (resp. 3) except with negligible probability $3\nu\hat{\ell}/q$ (see the proof of Lemma 10). This completes the proof of Lemma 15. □

A.4 Proofs of Lemmas in Section 7.3.3

Lemma 20 *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, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1)\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{1\text{-}h}}^{\mathsf{P5}}(\lambda) + 3\hat{\ell}/q$, where $\mathcal{B}_{1\text{-}h}(\cdot) := \mathcal{B}_1(h, \cdot)$ and $\hat{\ell}$ is the maximum number of rows in access matrices of key queries.*

Proof. In order to prove Lemma 20, we construct a probabilistic machine $\mathcal{B}_1$ against Problem 5 using an adversary $\mathcal{A}$ in a security game (Game 2-$(h-1)$-2 or 2-h-1) as a black box as follows:

1. $\mathcal{B}_1$ is given an index h and the first part of a Problem 5 instance, which is given in step 1 in Definition 14, $(\mathsf{param}_n, \widehat{\mathbb{B}}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}_1, \widehat{\mathbb{B}}_1^*, \mathbb{B}_2, \mathbb{B}_2^*)$.

2. $\mathcal{B}_1$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.

3. $\mathcal{B}_1$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1^\lambda, \mathsf{hk}, \mathsf{param}_n, \{\widehat{\mathbb{B}}_t'\}_{t=0,1,2})$ of Game 2-$(h-1)$-2 (and 2-h-1), where $\mathsf{hk} \xleftarrow{\mathsf{R}} \mathsf{KH}_\lambda, \widehat{\mathbb{B}}_0' := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,4}), \widehat{\mathbb{B}}_1' := (\boldsymbol{b}_{1,1}, \ldots, \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,4n+1}, \ldots, \boldsymbol{b}_{1,6n})$ and $\widehat{\mathbb{B}}_2' := (\boldsymbol{b}_{2,1}, \boldsymbol{b}_{2,2}, \boldsymbol{b}_{2,7})$, that are obtained from the Problem 5 instance.

4. When $\mathcal{B}_1$ (or challenger) obtains the κ-th key reveal query for attributes Γ with $\Gamma := \{x_1, \ldots, x_{n'}\}$, $\mathcal{B}_1$ calculates $\vec{y} := (y_1, \ldots, y_n)$ such that $\sum_{i=0}^{n-1} y_{n-i} z^i = z^{n-1-n'} \cdot \prod_{i=1}^{n'} (z - x_i)$, and generates key components as follows:

(a) if $\kappa < h$, $\boldsymbol{k}_0^*$ is calculated as in Eq. (18) and $\boldsymbol{k}_1^*$, $\boldsymbol{k}_{2,1}^*$ and $\boldsymbol{k}_{2,2}^*$ are calculated as in Eq. (14) using fresh $\omega, \tau', \varphi_0, \varphi_1, \varphi_{2,1,1}, \ldots, \varphi_{2,2,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$.

(b) if $\kappa = h$, $\mathcal{B}_1$ gives $\vec{y}$ to the challenger of Problem 5. Then, $\mathcal{B}_1$ is given the second part of the Problem 5 instance, which is given in step 2 in Definition 17, $(\boldsymbol{h}_{\beta,0}^*, \boldsymbol{e}_0, \boldsymbol{h}_{\beta,1}^*, \{\boldsymbol{e}_{\beta,j,\iota}\}_{j=1,\ldots,n;\,\iota=1,\ldots,n}, \{\boldsymbol{h}_{2,i}^*\}_{i=1,2})$. $\mathcal{B}_1$ calculates $\boldsymbol{k}_0^* := \boldsymbol{h}_{\beta,0}^*$, $\boldsymbol{k}_1^* := \boldsymbol{h}_{\beta,1}^*$, and $\boldsymbol{k}_{2,i}^* := \boldsymbol{h}_{2,i}^* + \boldsymbol{r}_i^*$ with $\boldsymbol{r}_i^* \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}_{2,5}^*, \boldsymbol{b}_{2,6}^* \rangle$.

(c) if $\kappa > h$, $\boldsymbol{k}_0^*$ is calculated as in Eq. (13) and $\boldsymbol{k}_1^*$, $\boldsymbol{k}_{2,1}^*$ and $\boldsymbol{k}_{2,2}^*$ are calculated as in Eq. (14) using fresh $\omega, \varphi_0, \varphi_1, \varphi_{2,1,1}, \ldots, \varphi_{2,2,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$.

$\mathcal{B}_1$ sends (constant-size) key $\mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}_0^*, \boldsymbol{k}_1^*, \boldsymbol{k}_{2,1}^*, \boldsymbol{k}_{2,2}^*)$ to $\mathcal{A}$.

5. When $\mathcal{B}_1$ obtains a signature reveal query for $\mathbb{S} := (M, \rho)$, $\mathcal{B}_1$ generates a normal form signature as in Eq. (15), and sends it to $\mathcal{A}$

6. When $\mathcal{B}_1$ receives an output $(m', \mathbb{S}', \vec{\boldsymbol{s}}')$ from $\mathcal{A}$, $\mathcal{B}_1$ calculates verification text $(\boldsymbol{c}_0, \ldots, \boldsymbol{c}_{\ell+1})$ as follows: $\mathcal{B}_1$ generates $\vec{f}, \vec{g} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r, (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}, (r_1, \ldots, r_\ell)^{\mathrm{T}} := M \cdot \vec{g}^{\mathrm{T}}$, $s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}, r_0 := \vec{1} \cdot \vec{g}^{\mathrm{T}}, s_{\ell+1}, r_{\ell+1}, \psi_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and $\mathcal{B}_1$ calculates

$$\boldsymbol{c}_0 := \boldsymbol{c}_0^{\mathsf{norm}} + r_0 \boldsymbol{e}_0 - r_{\ell+1} \boldsymbol{b}_{0,2}, \quad \boldsymbol{c}_i := \boldsymbol{c}_i^{\mathsf{norm}} + \sum_{j,\iota=1}^{n} \xi_{i,j} p_{i,\iota} \boldsymbol{e}_{\beta,j,\iota} \text{ for } i = 1, \ldots, \ell,$$

$$\boldsymbol{c}_{\ell+1} := \boldsymbol{c}_{\ell+1}^{\mathsf{norm}} + p'_{\ell+1,1} \boldsymbol{b}_{2,3} + p'_{\ell+1,2} \boldsymbol{b}_{2,4},$$

where $\boldsymbol{c}_i^{\mathsf{norm}}$ is a normal form given in Eq. (16) that is computed using $\widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}_1, \mathbb{B}_2$ of the Problem 5 instance and s_i above, $\vec{p}_i := (p_{i,1}, \ldots, p_{i,n})$ are given as $\vec{p}_i := r_i \vec{e}_1 + \psi_i \vec{v}_i$ if $\rho(i) = v_i$, $\vec{p}_i := r_i \vec{v}_i$ if $\rho(i) = \neg v_i$, and $(\xi_{i,j})_{j=1,\ldots,n} \xleftarrow{\mathsf{U}} \{(\xi_j)_{j=1,\ldots,n} \in \mathbb{F}_q^n \mid \sum_{j=1}^n \xi_j = 1\}$ and $\vec{p}'_{\ell+1} := (p'_{\ell+1,1}, p'_{\ell+1,2})$ is given as $\vec{p}'_{\ell+1} := r_{\ell+1} \vec{e}_1 + \psi_{\ell+1}(-\mathsf{H}_{\mathsf{hk}}^{\lambda,\mathsf{D}}(m' \,||\, \mathbb{S}'),\ 1)$. $\mathcal{B}_1$ verifies the signature $(m', \mathbb{S}', \vec{\boldsymbol{s}}')$ using Ver with the above $(\boldsymbol{c}_0, \ldots, \boldsymbol{c}_{\ell+1})$, and outputs $\beta' := 0$ if the verification succeeds, $\beta' := 1$ otherwise.

When $\beta = 0$ (resp. $\beta = 1$), the view of $\mathcal{A}$ is equivalent to that in Game 2-$(h-1)$-2 (resp. 2-h-1) except with negligible probability $3\hat{\ell}/q$ (see the proof of Lemma 10). This completes the proof of Lemma 20. □

Lemma 21 *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, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{2\text{-}h}}^{\mathsf{P5}}(\lambda) + 3\hat{\ell}/q$. where $\mathcal{B}_{2\text{-}h}(\cdot) := \mathcal{B}_2(h, \cdot)$ and $\hat{\ell}$ is the maximum number of rows in access matrices of key queries.*

Proof. In order to prove Lemma 21, we construct a probabilistic machine $\mathcal{B}_2$ against Problem 5 using an adversary $\mathcal{A}$ in a security game (Game 2-h-1 or 2-h-2) as a black box. $\mathcal{B}_2$ acts in the same way as $\mathcal{B}_1$ in the proof of Lemma 20 except the following two points:

1. In case (b) of step 4; $\boldsymbol{k}_0^*$ is calculated as $\boldsymbol{k}_0^* := \boldsymbol{h}_{\beta,0}^* + \tau'_0 \boldsymbol{b}_{0,2}^*$, where $\tau'_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and $\boldsymbol{h}_{\beta,0}^*, \boldsymbol{b}_{0,2}^*$ are in the Problem 5 instance.

2. In the last step; if the verification succeeds, $\mathcal{B}_2$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_2$ outputs $\beta' := 0$.

When $\beta = 0$ (resp. $\beta = 1$), the view of $\mathcal{A}$ is equivalent to that in Game 2-h-2 (resp. 2-h-1) except with negligible probability $3\hat{\ell}/q$ (see the proof of Lemma 10). This completes the proof of Lemma 21. □