PAPER Special Section on Cryptography and Information Security

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

Katsuyuki TAKASHIMA[†a)], ***Senior Member***

SUMMARY We propose a key-policy attribute-based encryption (KP-ABE) scheme with *constant-size ciphertexts*, whose almost tightly 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 an *efficient, 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 dual system security proofs.

key words: *attribute-based encryption, constant-size ciphertexts, attribute-based signatures, constant-size signing keys, non-monotone span programs, decisional linear assumption*

1. Introduction

1.1 Backgrounds

The notion of *attribute-based encryption* (ABE) introduced by Sahai and Waters [2] 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 [3]). Non-monotone predicates should be used in many ABE applications, for example, in CP-ABE, some individuals or group members can be easily excluded from decryptable users just by using non-monotone predicates on attributes in ciphertexts.

While general (polynomial size) circuits are supported [4], [5] 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. [6], Herranz et al. [7], and Chen et al. [8] constructed ABE schemes with constant-size ciphertexts, but their access structures are very limited. Attrapadung, Libert and Panafieu [9] 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 [10]–[14]) show an interesting approach to achieving constant-size ciphertexts with expressive access structures, the security are proven only based on q-type assumptions (e.g., 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. [15] and Boneh et al. [16], various kinds of q-type assumptions have been widely used in order to achieve efficient cryptographic primitives [7], [17]–[20]. However, the assumptions (and also the associated schemes) suffered a special attack which was presented by Cheon [21] at Eurocrypt 2006. Subsequently, Sakemi et al. [22] 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

Manuscript received March 15, 2019.
Manuscript revised July 11, 2019.

[†] The author is with the Information Technology R&D Center, Mitsubishi Electric Corporation, Kamakura-shi, 247-8501 Japan.

[*] An extended abstract of a preliminary version of this paper was presented in [1] at SCN 2014. This provides significant technical contributions over [1], e.g., the full security proofs with better (i.e., semi-adaptive) security than selective one in [1] for our KP-ABE scheme, and scheme description and security proof of our ABS with short secret keys (with the underlying CP-ABE scheme). Refer to Sects. 6, 7 and Appendices A–E.

a) E-mail: Takashima.Katsuyuki@aj.MitsubishiElectric.co.jp

DOI: 10.1587/transfun.2019CIP0009

Table 1 Comparison of our scheme with KP-ABE *for span programs with constant-size ciphertexts* in [9], [11], [23], where $|\mathbb{G}|$, $|\mathbb{G}_T|$, $n, \ell, \mathfrak{r}$, ν_1 and ν 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, the number of rows and columns in access structure matrix for the secret key, the maximum number of the adversary's pre-challenge key queries, and that of the adversary's all key queries, respectively. PK, SK, CT, and (N)M-SP stand for public key, secret key, ciphertext, and (non-)monotone span program, respectively.

	ALP11 [9]	CW14 [23]	AC16 [24]	A16 [12]	AC17 [13]	A19 [14]	Proposed
Universe	large	small	large	large	large	large	large
Security	selective	semi-adaptive	semi-adaptive	adaptive	adaptive	adaptive	semi-adaptive
Reduction factor	$O(n)$	$O(n)$	$O(n)$	$O(\nu_1)$	$O(\nu)$	$O(\nu_1)$	$O(n)$
Order of $\mathbb{G}$	prime	composite	prime	prime	prime	prime	prime
Assumption	n-DBDHE	static assump.	k-LIN	EDHEp3 & 4 parametrized by $n, \ell, \mathfrak{r}$	q-ratio$_{\text{dsg}}$	q-ratio	DLIN
Access structures	NM-SP	M-SP	M-SP	M-SP	M-SP	NM-SP	NM-SP
PK size	$O(n)\,\lvert\mathbb{G}\rvert$	$O(n)\,\lvert\mathbb{G}\rvert$	$O(kn)\,\lvert\mathbb{G}\rvert$	$O(n)\,\lvert\mathbb{G}\rvert$	$O(n)\,\lvert\mathbb{G}\rvert$	$O(n^2)\,\lvert\mathbb{G}\rvert$	$O(n)\,\lvert\mathbb{G}\rvert$
SK size	$O(\ell n)\,\lvert\mathbb{G}\rvert$	$O(\ell n)\,\lvert\mathbb{G}\rvert$	$O(k\ell n)\,\lvert\mathbb{G}\rvert$	$O(\ell n)\,\lvert\mathbb{G}\rvert$	$O(\ell n)\,\lvert\mathbb{G}\rvert$	$O(\ell n^3)\,\lvert\mathbb{G}\rvert$	$O(\ell n)\,\lvert\mathbb{G}\rvert$
CT size	$3\,\lvert\mathbb{G}\rvert+$ $1\,\lvert\mathbb{G}_T\rvert^*$	$2\,\lvert\mathbb{G}\rvert+$ $1\,\lvert\mathbb{G}_T\rvert$	$O(k)\,\lvert\mathbb{G}\rvert+$ $1\,\lvert\mathbb{G}_T\rvert$	$18\,\lvert\mathbb{G}\rvert+$ $1\,\lvert\mathbb{G}_T\rvert$	$O(1)\,\lvert\mathbb{G}\rvert+$ $1\,\lvert\mathbb{G}_T\rvert$	$O(1)\,\lvert\mathbb{G}\rvert+$ $1\,\lvert\mathbb{G}_T\rvert$	$17\,\lvert\mathbb{G}\rvert+$ $1\,\lvert\mathbb{G}_T\rvert$

* In a subsequent work [10], CT size is reduced to $2\,|\mathbb{G}| + 1\,|\mathbb{G}_T|$.

[23] 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. In [23], they also constructed a small-universe, almost tightly semi-adaptive KP-ABE scheme with constant-size ciphertexts on *composite-order groups*, where almost tight security means that the reduction factor from a static assumption is a polynomial in security parameter λ and does not depend on the (maximum) number of key queries [25]. Agrawal and Chase [24] presented a generic construction for several kinds of ABE including KP- and CP-ABE with constant-size ciphertexts (which are given in Appendice E and D in the full version [24]). While the generic approach is attractive, however, the obtained short-ciphertext ABE schemes treat with only *monotone* span programs for access policies.

Hence, to construct an (almost) tightly secure, *constant-size ciphertext* KP-ABE scheme *with non-monotone span program access policies from a static assumption in the prime-order groups* remains an interesting open problem in terms of practical and theoretical aspects on ABE.

The above technique can be applied to construct a new attribute-based signature (ABS) scheme. The concept of ABS was introduced by Maji et al. in 2008 [26]. Since then, many ABS constructions have been proposed including [27]–[33]. A generic construction given in [30] is interesting, however, it cannot achieve the standard ABS security, i.e., unforgeability and anonymity, simultaneously, as pointed out in [31]. El Kaafarani-Katsumata's scheme [31] is proven just in the *random oracle model*. While most of existing works (in the standard model) [27], [28], [32], [33] give no constant-size secret key ABS schemes, Sakai et al.'s ABS scheme [29] not only has expressive policies but also has constant-size keys. However, as pointed out in Remark 3.1 in [33], it is impractical for using in real world applications, since the available policies are given by *binary* circuits. Hence, our target w.r.t. ABS is as follows: *Can we construct a constant-size secret key ABS scheme which is proven fully secure in the standard model and efficient enough for real world applications ?*

1.2 Our Results

- We propose a KP-ABE scheme with *constant-size ciphertexts*, whose almost tightly semi-adaptive security is proven from the *DLIN assumption* in the standard model (Sects. 5 and 6). 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 comparison of our scheme with previous KP-ABE for span programs with constant-size ciphertexts, see Table 1 (in which a composite order group based one given in [11] is omitted since it is surpassed by a more desirable prime-order based one [12] by the same author).
- As an application of our KP-ABE construction, we also propose a *fully secure* ABS scheme with constant-size secret (signing) keys from the DLIN assumption in the standard model (Sect. 7). The policies for the ABS are also given by non-monotone span programs with input attributes from large universes, and the proposed scheme is efficient enough for using in real world applications.
- For achieving the above results, we extend the sparse matrix technique on dual pairing vector spaces (DPVS) [3], [34], [35] developed in [36]. In particular, several algebraic properties of an elaborately chosen sparse matrix group $\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ are applied to the dual system security proofs. For the details, see Sects. 1.3, 4 and

6.4.

1.3 Key Techniques

We extend the sparse matrix technique on DPVS developed in [36], 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 [36], 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 Sect. 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 Sects. 6.4.1 and 6.4.2, respectively.

1.4 Notations

When A is a random variable or distribution, $y \overset{\mathsf{R}}{\leftarrow} A$ denotes that y is randomly selected from A according to its distribution. When A is a set, $y \overset{\mathsf{U}}{\leftarrow} A$ denotes that y is uniformly selected from A. When A is a set and B is a subset of A, $A \setminus B$ is the difference set. 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 $(\overbrace{0\cdots0}^{j-1},1,\overbrace{0\cdots0}^{n-j}) \in \mathbb{F}_q^n$. $GL(N,\mathbb{F}_q)$ 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) [34], [35] constructed using symmetric bilinear pairing groups. For the asymmetric version of DPVS, see Appendix A.2 of the full version of [3].

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 [16]): The DLIN problem is to guess $\beta \in \{0,1\}$, given $(\mathsf{param}_{\mathbb{G}}, G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta) \overset{\mathsf{R}}{\leftarrow} \mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda)$, where $\mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda)$: $\mathsf{param}_{\mathbb{G}} := (q,\mathbb{G},\mathbb{G}_T,G,e) \overset{\mathsf{R}}{\leftarrow} \mathcal{G}_{\mathsf{bpg}}(1^\lambda), \kappa,\delta,\xi,\sigma \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$, $Y_0 := (\delta+\sigma)G$, $Y_1 \overset{\mathsf{U}}{\leftarrow} \mathbb{G}$, return$(\mathsf{param}_{\mathbb{G}}, G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta)$, for $\beta \overset{\mathsf{U}}{\leftarrow} \{0,1\}$. For a probabilistic machine $\mathcal{E}$, we define the advantage of $\mathcal{E}$ for the DLIN problem as:

$\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) := \left| \Pr\left[\mathcal{E}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{DLIN}}_0(1^\lambda) \right] - \Pr\left[\mathcal{E}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{DLIN}}_1(1^\lambda) \right] \right|$. The DLIN assumption is: For any probabilistic polynomial-time adversary $\mathcal{E}$, the advantage $\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda)$ 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 [37]): $\mathcal{U}$ ($\subset \{0,1\}^*$) 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 $(\ell \times \mathfrak{r})$ 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 $\ell \times \mathfrak{r}$ matrix. Let column vector $\vec{f}^{\mathrm{T}} := (f_1, \ldots, f_{\mathfrak{r}})^{\mathrm{T}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\mathfrak{r}}$. Then, $s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}} = \sum_{k=1}^{\mathfrak{r}} f_k$ 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 Setup, KeyGen, Enc and Dec. They are given as follows:

Setup takes as input security parameter 1^λ and a bound on the number of attributes per ciphertext n. It outputs public parameters pk and master secret key sk.

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

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 $\mathsf{Adv}^{\mathsf{KP\text{-}ABE,SA}}_{\mathcal{A}}(\lambda) := \Pr[\mathcal{A} \text{ wins }] - 1/2$ 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, $\Gamma := \{x_j\}_{1\le j\le n'}$, 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 $(\mathsf{sk}, \mathsf{pk}) \overset{\mathsf{R}}{\leftarrow} \mathsf{Setup}(1^\lambda, n)$, all messages m, all attribute sets Γ, all signing keys $\mathsf{sk}_\Gamma \overset{\mathsf{R}}{\leftarrow} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \Gamma)$, all access structures $\mathbb{S}$ such that $\mathbb{S}$ accepts Γ, and all signatures $\sigma \overset{\mathsf{R}}{\leftarrow} \mathsf{Sig}(\mathsf{pk}, \mathsf{sk}_\Gamma, m, \mathbb{S})$, 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 $(\mathsf{sk}, \mathsf{pk}) \overset{\mathsf{R}}{\leftarrow} \mathsf{Setup}(1^\lambda, n)$, all messages m, all attribute sets Γ_1 and Γ_2, all signing keys $\mathsf{sk}_{\Gamma_1} \overset{\mathsf{R}}{\leftarrow} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \Gamma_1)$ and $\mathsf{sk}_{\Gamma_2} \overset{\mathsf{R}}{\leftarrow} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \Gamma_2)$, 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 $\mathsf{Adv}^{\mathsf{ABS,UF}}_{\mathcal{A}}(\lambda)$ 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 $(\mathsf{sk}, \mathsf{pk}) \overset{\mathsf{R}}{\leftarrow} \mathsf{Setup}(1^\lambda, n)$ 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 attribute set 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 reveal key oracle, and $\mathsf{Ver}(\mathsf{pk}, m', \mathbb{S}', \sigma') = 1$.

Remark 1: Since a signing query in the unforgeability definition in [27], [28] 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 [27], [28] is problematic.

To address this issue, as in [38], 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 [39]. 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 1–4 are key lemmas for the security proof for our KP-ABE and ABS schemes. The proofs of Lemmas 2, 3 and 4 are given in Appendix A.

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

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

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

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, $\mathcal{H}_{\vec{y}}(n,\mathbb{F}_q) = \{U \in \mathcal{H}(n,\mathbb{F}_q) \cap GL(n,\mathbb{F}_q) \mid \vec{y}U = \vec{y}\}$.

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 $A_{n-1} := \{\vec{u}' \in \mathbb{F}_q^n \mid \vec{y}\cdot\vec{u}' = y_n\}$ 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}.

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

Next is a key lemma for applying the proof techniques in [3] to our KP-ABE and ABS schemes.

Lemma 3: For all $\vec{y} \in \mathbb{F}_q^n \setminus \mathsf{span}\langle\vec{e}_n\rangle$ and $\pi \in \mathbb{F}_q$, let $W_{\vec{y},\pi} := \{\vec{w} \in \mathbb{F}_q^n \setminus \mathsf{span}\langle\vec{e}_n\rangle^\perp \mid \vec{y}\cdot\vec{w} = \pi\}$, 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 $(\vec{y},\vec{v}) \in \left(\mathbb{F}_q^n \setminus \mathsf{span}\langle\vec{e}_n\rangle\right) \times \left(\mathbb{F}_q^n \setminus \mathsf{span}\langle\vec{e}_n\rangle^\perp\right)$, if U and Z are generated as $U \overset{\mathsf{U}}{\leftarrow} \mathcal{H}_{\vec{y}}(n,\mathbb{F}_q), Z := (U^{-1})^{\mathrm{T}}$, then $\vec{v}Z$ is uniformly distributed in $W_{\vec{y},(\vec{y}\cdot\vec{v})}$.

Let

$$\mathcal{L}(w,n,\mathbb{F}_q) := \left\{ X := \begin{pmatrix} X_{1,1} & \cdots & X_{1,w} \\ \vdots & & \vdots \\ X_{w,1} & \cdots & X_{w,w} \end{pmatrix} \middle| \right.$$

$$\left. X_{i,j} := \begin{pmatrix} \mu_{i,j} & & & \mu'_{i,j,1} \\ & \ddots & & \vdots \\ & & \mu_{i,j} & \mu'_{i,j,n-1} \\ & & & \mu'_{i,j,n} \end{pmatrix} \begin{matrix} \in \mathcal{H}(n,\mathbb{F}_q) \\ \text{for } i,j = \\ 1,\dots,w \end{matrix} \right\} \bigcap GL(wn,\mathbb{F}_q),$$

$$\mathcal{P}(w,n,\mathbb{F}_q) :=$$

$$\left\{ Y := \begin{pmatrix} Y_0 & & & Y_1 \\ & \ddots & & \vdots \\ & & Y_0 & Y_{n-1} \\ & & & Y_n \end{pmatrix} \middle| \begin{matrix} Y_0, Y_n \in GL(w,\mathbb{F}_q), \\ Y_1,\dots,Y_{n-1} \in \mathbb{F}_q^{w\times w}, \\ \text{a blank element in the} \\ \text{matrix denotes } 0 \in \mathbb{F}_q \end{matrix} \right\}, \tag{3}$$

and permutation ϖ on $[wn] := \{1,\dots,wn\}$ as

$$\begin{array}{cccc} \varpi : & [wn] & \to & [wn] \\ & \Psi & & \Psi \\ & (i-1)n+k & \mapsto & (k-1)w+i. \end{array} \tag{4}$$

We denote the corresponding permutation matrix by Π, i.e., the left multiplication by Π is equivalent to the permutation ϖ on rows of matrices in $\mathbb{F}_q^{wn\times wn}$.

Lemma 4: $\mathcal{L}(w,n,\mathbb{F}_q)$ and $\mathcal{P}(w,n,\mathbb{F}_q)$ are subgroups of $GL(wn,\mathbb{F}_q)$. Moreover, $\mathcal{L}(w,n,\mathbb{F}_q)$ is the conjugate of $\mathcal{P}(w,n,\mathbb{F}_q)$ by Π, i.e., $\mathcal{L}(w,n,\mathbb{F}_q) = \Pi^{-1}\cdot\mathcal{P}(w,n,\mathbb{F}_q)\cdot\Pi$.

The proof of Lemma 4 is given in Appendix A (Lemma 2 and its proof) in the full version of [36].

Remark 2: For matrix $W := (w_{i,j})_{i,j=1,\dots,N} \in \mathbb{F}_q^{N\times N}$ and element $\boldsymbol{g} := (G_1,\dots,G_N)$ in N-dimensional $\mathbb{V}$, $\boldsymbol{g}W$ denotes $(\sum_{i=1}^N G_i w_{i,1},\dots,\sum_{i=1}^N G_i w_{i,N}) = (\sum_{i=1}^N w_{i,1}G_i,\dots,\sum_{i=1}^N w_{i,N}G_i)$ by a natural multiplication of a N-dim. row vector and a $N\times N$ matrix. Thus it holds an associative law as $(\boldsymbol{g}W)W^{-1} = \boldsymbol{g}(WW^{-1}) = \boldsymbol{g}$ and a pairing invariance property $e(\boldsymbol{g}W, \boldsymbol{h}(W^{-1})^{\mathrm{T}}) = e(\boldsymbol{g},\boldsymbol{h})$ for any $\boldsymbol{g},\boldsymbol{h} \in \mathbb{V}$.

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 [36] 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, $(\boldsymbol{k}_0^*,\boldsymbol{k}_1^*,\dots,\boldsymbol{k}_\ell^*) \in \mathbb{G}^5 \times (\mathbb{G}^n)^\ell$ 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,

$$X := \begin{pmatrix} \mu & & & \mu'_1 \\ & \ddots & & \vdots \\ & & \mu & \mu'_{n-1} \\ & & & \mu'_n \end{pmatrix} \in \mathcal{H}(n,\mathbb{F}_q) \text{ of Eq. (1) in Sect. 4,}$$

where $\mu,\mu'_1,\dots,\mu'_n \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$ 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 $\Gamma := \{x_1,\dots,x_{n'}\}$ be $\boldsymbol{c}_1 := (\omega\vec{y})_{\mathbb{B}} = \omega(y_1\boldsymbol{b}_1 + \cdots + y_n\boldsymbol{b}_n) = (y_1\omega\mu G,\dots,y_{n-1}\omega\mu G,\ \omega(\sum_{i=1}^n y_i\mu'_i)G)$, where $\omega \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$ and $\vec{y} := (y_1,\dots,y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j}z^j = z^{n-1-n'}\cdot\prod_{j=1}^n (z-x_j)$. Then, $\boldsymbol{c}_1$ 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 $(y_1C_1,\dots,\ y_{n-1}C_1,C_2)$ (note that $y_iC_1 = y_i\omega\mu G$ for $i = 1,\dots,n-1$). That is, a ciphertext (excluding $\vec{y}$) can be just two group elements, or the size is constant in n.

Let $\mathbb{B}^* := (\boldsymbol{b}_i^*)$ 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 $\{s_i\}_{i=1,\dots,\ell}$ associated with access structure $\mathbb{S}$. Using $\{s_i\}_{i=1,\dots,\ell}$, we also set a secret key for $\mathbb{S}$ as $\boldsymbol{k}_i^* := (s_i\vec{e}_1 + \theta_i\vec{v}_i)_{\mathbb{B}^*}$ if $\rho(i) = v_i$ and $\boldsymbol{k}_i^* := (s_i\vec{v}_i)_{\mathbb{B}^*}$ if $\rho(i) = \neg v_i$ where $\vec{v}_i := (v_i^{n-1}, \dots, v_i, 1)$ and $\theta_i \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$. From the dual orthonormality of $\mathbb{B}$ and $\mathbb{B}^*$, if $\mathbb{S}$ accepts Γ, there exist a system of coefficients $\{\alpha_i\}_{i\in I}$ 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 $(y_1C_1, \dots, y_{n-1}C_1, C_2) \in \mathbb{G}^n$ and $\widetilde{\boldsymbol{k}}^*$ is parsed as a n-tuple $(D_1^*, \dots, D_n^*) \in \mathbb{G}^n$, 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 [3], 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 (which is defined in Definition 10 in Sect. 6.3), 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 Sect. 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 [36]. 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 $\{U_j \overset{\mathsf{U}}{\leftarrow} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)\}$ 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.

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

Remark 3: Let

$$\left.\begin{array}{l}
\begin{pmatrix} \boldsymbol{b}_{1,(i-1)n+1} \\ \vdots \\ \boldsymbol{b}_{1,in} \end{pmatrix} := \\
\begin{pmatrix}
B_{i,1} & & & B'_{i,1,1} & & B_{i,6} & & & B'_{i,6,1} \\
& \ddots & & \vdots & \cdots & & \ddots & & \vdots \\
& & B_{i,1} & B'_{i,1,n-1} & & & & B_{i,6} & B'_{i,6,n-1} \\
& & & B'_{i,1,n} & & & & & B'_{i,6,n}
\end{pmatrix} \\
\text{for } i = 1, \dots, 6, \text{ and } \mathbb{B}_1 := (\boldsymbol{b}_{1,1}, \dots, \boldsymbol{b}_{1,6n}),
\end{array}\right\} \qquad (5)$$

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.

$$\begin{aligned}
&\mathsf{Setup}(1^\lambda,\ n) : \\
&\quad (\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \{B_{i,j}, B'_{i,j,l}\}_{l=1,\dots,n}^{i,j=1,\dots,6}, \mathbb{B}_1^*) \overset{\mathsf{R}}{\leftarrow} \mathcal{G}_{\mathsf{ob}}^{\mathsf{KP\text{-}ABE}}(1^\lambda, 6, n), \\
&\quad \widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}),
\end{aligned}$$

$\widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, .., \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,5n+1}, .., \boldsymbol{b}_{1,6n}) = \{B_{i,j}, B'_{i,j,l}\}_{l=1,\dots,n}^{i=1,6;j=1,\dots,6}$,

$\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*, \boldsymbol{b}_{0,4}^*)$, $\widehat{\mathbb{B}}_1^* := (\boldsymbol{b}_{1,1}^*, .., \boldsymbol{b}_{1,n}^*, \boldsymbol{b}_{1,3n+1}^*, .., \boldsymbol{b}_{1,5n}^*)$,

$\mathsf{pk} := (1^\lambda, \mathsf{param}_n, \{\widehat{\mathbb{B}}_t\}_{t=0,1}), \mathsf{sk} := \{\widehat{\mathbb{B}}_t^*\}_{t=0,1}$, return pk, sk.

$\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \mathbb{S} := (M, \rho))$: $\vec{f} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q^{\mathfrak{r}}$,

$\vec{s}^{\mathrm{T}} := (s_1, \dots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$, $s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$, $\eta_0 \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$,

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

for $i = 1, \dots, \ell$, $\vec{v}_i := (v_i^{n-1}, \dots, v_i, 1)$ for $\rho(i) = v_i$ or $\neg v_i$,

if $\rho(i) = v_i$, $\theta_i \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$, $\vec{\eta}_i \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q^{2n}$,

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

if $\rho(i) = \neg v_i$, $\vec{\eta}_i \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q^{2n}$,

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

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

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

$\omega, \varphi_0, \varphi_1, \zeta \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$,

$\vec{y} := (y_1, \dots, y_n)$ s.t. $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \cdot \prod_{j=1}^{n'} (z - x_j)$,

$\boldsymbol{c}_0 := (\omega, \ 0, \ \zeta, \ 0, \ \varphi_0)_{\mathbb{B}_0}$, $C_{1,j} := \omega B_{1,j} + \varphi_1 B_{6,j}$,

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

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

$\mathsf{Dec}(\mathsf{pk}, \ \mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{k}_0^*, \boldsymbol{k}_1^*, \dots, \boldsymbol{k}_\ell^*)$,

$\mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{C_{1,j}, C_{2,j}\}_{j=1,\dots,6}, c_T))$:

If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{x_1, \dots, x_{n'}\}$, then compute I and $\{\alpha_i\}_{i \in I}$ such that $\vec{1} = \sum_{i \in I} \alpha_i M_i$, where M_i is the i-th row of M, and

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

$\vec{y} := (y_1, \dots, y_n)$ s.t. $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \cdot \prod_{j=1}^{n'} (z - x_j)$,

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

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

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

return $m' := c_T / K$.

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

$\mathsf{Dec}'(\mathsf{pk}, \ \mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{k}_0^*, \boldsymbol{k}_1^*, \dots, \boldsymbol{k}_\ell^*)$,

$\mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{C_{1,j}, C_{2,j}\}_{j=1,\dots,6}, c_T))$:

If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{x_1, \dots, x_{n'}\}$, then compute I and $\{\alpha_i\}_{i \in I}$ such that $\vec{1} = \sum_{i \in I} \alpha_i M_i$, where M_i is the i-th row of M, and

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

$\vec{y} := (y_1, \dots, y_n)$ s.t. $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \cdot \prod_{j=1}^{n'} (z - x_j)$,

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

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

$K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \cdot$

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

return $m' := c_T / K$.

[Correctness] Since $\vec{y} := (y_1, \dots, y_n)$ is defined by the polynomial equality $\sum_{j=0}^{n-1} y_{n-j} z^j := z^{n-1-n'} \cdot \prod_{j=1}^{n'} (z - x_j)$, the leading coefficient of the polynomial, y_1, is equal to 1. Therefore, note that $e(\boldsymbol{c}_1, \boldsymbol{k}_i^*) = (s_i\vec{e}_1 + \theta_i\vec{v}_i) \cdot \vec{y} = \omega s_i$ if $i \in I$ and $\rho(i) = v_i$ (i.e., $\vec{v}_i \cdot \vec{y} = 0$). 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

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,

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

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 $j = 1, \dots, n$; $\iota = 1, 2$, $\epsilon := (3\nu\hat{\ell} + 10n + 11)/q$, 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.

6.1 Proof Outline of Theorem 1

At the top level strategy of the security proof, the dual system encryption by Waters [40] 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, we introduce a series of refined forms of secret keys, namely, *partially randomized semi-funcional of type 0 and type j-ι* ($j = 1, \dots, n; \iota = 1, 2$). The forms have some similarity to those employed in [23], [25],

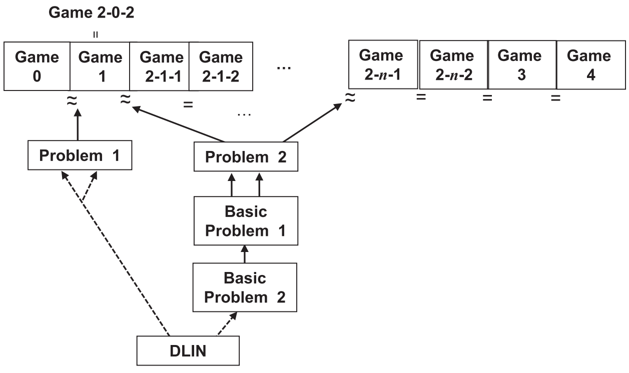


Fig. 1 Structure of reductions for the proof of Theorem 1.

which also achieved almost tight security from static assumptions. The form of ciphertext given in the final game, which has no plaintext information, is called *non-functional* (in particular, it is independent of the challenge bit).

To prove this theorem, we employ Game 0 (original semi-adaptive security game) through Game 4. In Game 1, the challenge ciphertext is changed to semi-functional form, and and *all* queried keys are changed to partially randomized semi-functional form of type 0. In Game 2-j-ι ($j = 1, \dots, n$; $\iota = 1, 2$), *all* queried keys are changed to partially randomized semi-functional form of type j-ι. In particular, secret keys are incrementally changed to partially randomized semi-functional form of type n-2, which has enough randomness for becoming (truly) semi-functional one. Namely, in Game 3, they are *all* changed to semi-functional. 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 [3]. The vertical reductions are also indicated in Fig. 1. The reduction steps indicated by dotted arrows can be shown in the same manner as those in the full version of [3].

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. (6). Similarly, a normal ciphertext (with attributes Γ) is expressed by Eq. (7). A semi-functional ciphertext is expressed by Eq. (10). A partially randomized semi-functional of type 0 key is expressed by Eqs. (8) and (9). A partially randomized semi-functional of type j-1 (resp. j-2) key is expressed by Eqs. (8) and (11) (resp. Eqs. (8) and (12)) for non-matching attributes $v_{h,i}$ as well as Eq. (9) for matching attributes $v_{h,i}$. A semi-functional key is expressed by Eq. (13) for non-matching attributes $v_{h,i}$ as well as Eq. (9) for matching attributes $v_{h,i}$. A non-functional ciphertext is expressed by Eq. (14) (with $\boldsymbol{c}_1$ in Eq. (10)).

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 $\beta \overset{\mathsf{U}}{\leftarrow} \{0, 1\}$ of Problem 1. We then show that the distribution of the secret keys and challenge ciphertext replied by the simulator is equivalent to those of Game 0 when $\beta = 0$ and those of Game 1 when $\beta = 1$. That is, the advantage of Problem 1 is equivalent to the advantage gap between Games 0 and 1 (Lemma 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 $j = 1, \dots, n$ is equivalent to the advantage of Problem 2 (Lemma 8), 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, $\boldsymbol{b}_{1,2n+1}, \dots, \boldsymbol{b}_{1,3n}$ and $\boldsymbol{b}^*_{1,2n+1}, \dots, \boldsymbol{b}^*_{1,3n}$, 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 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 in access matrices of any key queries below.

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

$$\left.\begin{array}{l}
\boldsymbol{k}^*_{h,0} := (-s_{h,0},\ \boxed{0},\ 1,\ \eta_{h,0},\ 0)_{\mathbb{B}^*_0}, \\
\text{for } i = 1, \dots, \ell, \\
\text{if } \rho_h(i) = v_{h,i}, \\
\boldsymbol{k}^*_{h,i} := (\overbrace{s_{h,i}\vec{e}_1 + \theta_{h,i}\vec{v}_{h,i},}^{n}\ \overbrace{\boxed{0^{2n}}}^{2n},\ \overbrace{\vec{\eta}_{h,i},}^{2n}\ \overbrace{0^n}^{n}\ )_{\mathbb{B}^*_1}, \\
\text{if } \rho_h(i) = \neg v_{h,i}, \\
\boldsymbol{k}^*_{h,i} := (\quad s_{h,i}\vec{v}_{h,i},\qquad \boxed{0^{2n}},\ \vec{\eta}_{h,i},\ 0^n\ )_{\mathbb{B}^*_1},
\end{array}\right\} \qquad (6)$$

where $\vec{f}_h \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q^r$, $\vec{s}_h^{\mathrm{T}} := (s_{h,1}, \dots, s_{h,\ell})^{\mathrm{T}} := M_h \cdot \vec{f}_h^{\mathrm{T}}$, $s_{h,0} := \vec{1} \cdot \vec{f}_h^{\mathrm{T}}, \theta_{h,i}, \eta_{h,0} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q, \vec{\eta}_{h,i} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q^{2n}, \vec{e}_1 := (1, 0, \dots, 0) \in \mathbb{F}_q^n$, and $\vec{v}_{h,i} := (v_{h,i}^{n-1}, \dots, v_{h,i}, 1) \in (\mathbb{F}_q^{\times})^n$. The challenge ciphertext for challenge plaintexts $(m^{(0)}, m^{(1)})$ and $\Gamma := \{x_j\}$ is:

$$\left.\begin{aligned}
\boldsymbol{c}_0 &:= (\omega,\ \boxed{0},\ \boxed{\zeta},\ 0,\ \varphi_0)_{\mathbb{B}_0},\\
\boldsymbol{c}_1 &:= (\ \overbrace{\omega\vec{y},}^{n}\ \overbrace{\boxed{0^{2n}},}^{2n}\ \overbrace{0^{2n},}^{2n}\ \overbrace{\varphi_1\vec{y}}^{n}\ )_{\mathbb{B}_1},\\
c_T &:= g_T^{\zeta} m^{(b)},
\end{aligned}\right\}\tag{7}$$

where $b \overset{\mathsf{U}}{\leftarrow} \{0,1\}$, $\omega, \zeta, \varphi_0, \varphi_1 \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$ 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:

$$\boldsymbol{k}^*_{h,0} := (-s_{h,0},\ \boxed{-r_{h,0}},\ 1,\ \eta_{h,0},\ 0)_{\mathbb{B}^*_0},\tag{8}$$

$$\left.\begin{aligned}
&\text{for } i = 1, \ldots, \ell,\\
&\text{if } \rho_h(i) = v_{h,i},\\
&\boldsymbol{k}^*_{h,i} := (\overbrace{s_{h,i}\vec{e}_1 + \theta_{h,i}\vec{v}_{h,i},}^{n}\ \overbrace{\boxed{r_{h,i}\vec{e}_1 + \widetilde{\theta}_{h,i}\vec{v}_{h,i}},\ 0^n,}^{2n}\ \overbrace{\vec{\eta}_{h,i},\ 0^n}^{3n})_{\mathbb{B}^*_1},\\
&\text{if } \rho_h(i) = \neg v_{h,i},\\
&\boldsymbol{k}^*_{h,i} := (\quad s_{h,i}\vec{v}_{h,i},\qquad \boxed{r_{h,i}\vec{v}_{h,i}},\ 0^n,\qquad \vec{\eta}_{h,i},\ 0^n)_{\mathbb{B}^*_1},
\end{aligned}\right\}\tag{9}$$

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

$$\left.\begin{aligned}
\boldsymbol{c}_0 &:= (\omega,\ \boxed{\tau},\ \zeta,\ 0,\ \varphi_0)_{\mathbb{B}_0},\\
\boldsymbol{c}_1 &:= (\ \overbrace{\omega\vec{y},}^{n}\ \overbrace{\boxed{\tau\vec{y},\ \tau\vec{y},}}^{2n}\ \overbrace{0^{2n},}^{2n}\ \overbrace{\varphi_1\vec{y}}^{n}\ )_{\mathbb{B}_1},\\
c_T &:= g_T^{\zeta} m,
\end{aligned}\right\}\tag{10}$$

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

Game 2-*j*-1 (*j* = 1, . . . , *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 $i = 1, \ldots, \ell$,

$$\left.\begin{aligned}
&\text{if } \rho_h(i) = v_{h,i}\ \wedge\ v_{h,i} \notin \Gamma,\\
&\boldsymbol{k}^*_{h,i} := (\overbrace{s_{h,i}\vec{e}_1 + \theta_{h,i}\vec{v}_{h,i},}^{n}\ \overbrace{\boxed{\xi_{h,i,j+1}}(r_{h,i}\vec{e}_1 + \widetilde{\theta}_{h,i}\vec{v}_{h,i}),}^{n}\\
&\overbrace{(r_{h,i}\vec{e}_1 + \widetilde{\theta}_{h,i}\vec{v}_{h,i})\boxed{(\textstyle\sum_{\kappa=1}^{j-1} \xi_{h,i,\kappa} Z_\kappa + \xi_{h,i,j} I_n)}}^{n},\ \overbrace{\vec{\eta}_{h,i},\ 0^n}^{3n})_{\mathbb{B}^*_1},\\
&\text{if } \rho_h(i) = \neg v_{h,i}\ \wedge\ v_{h,i} \in \Gamma,\\
&\boldsymbol{k}^*_{h,i} := (\overbrace{s_{h,i}\vec{v}_{h,i},}^{n}\ \overbrace{\boxed{\xi_{h,i,j+1}}\ r_{h,i}\vec{v}_{h,i},}^{n}\\
&\quad\overbrace{r_{h,i}\vec{v}_{h,i} \cdot \boxed{(\textstyle\sum_{\kappa=1}^{j-1} \xi_{h,i,\kappa} Z_\kappa + \xi_{h,i,j} I_n)}}^{n},\ \overbrace{\vec{\eta}_{h,i},\ 0^n}^{3n})_{\mathbb{B}^*_1},
\end{aligned}\right\}\tag{11}$$

where $(\xi_{h,i,\kappa})_{\kappa=1,\ldots,j+1} \overset{\mathsf{U}}{\leftarrow} \{(\xi_\kappa)_{\kappa=1,\ldots,j+1} \in \mathbb{F}_q^{j+1} \mid \sum_{i=1}^{j+1} \xi_i = 1\ \wedge\ \xi_{n+1} = 0 \text{ if } j = n\}$ 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, . . . , *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 $i = 1, \ldots, \ell$,

$$\left.\begin{aligned}
&\text{if } \rho_h(i) = v_{h,i}\ \wedge\ v_{h,i} \notin \Gamma,\\
&\boldsymbol{k}^*_{h,i} := (\overbrace{s_{h,i}\vec{e}_1 + \theta_{h,i}\vec{v}_{h,i},}^{n}\ \overbrace{\xi_{h,i,j+1}(r_{h,i}\vec{e}_1 + \widetilde{\theta}_{h,i}\vec{v}_{h,i}),}^{n}\\
&\quad\overbrace{(r_{h,i}\vec{e}_1 + \widetilde{\theta}_{h,i}\vec{v}_{h,i}) \cdot \boxed{(\textstyle\sum_{\kappa=1}^{j} \xi_{h,i,\kappa} Z_\kappa)}}^{n},\ \overbrace{\vec{\eta}_{h,i},\ 0^n}^{3n})_{\mathbb{B}^*_1},\\
&\text{if } \rho_h(i) = \neg v_{h,i}\ \wedge\ v_{h,i} \in \Gamma,\\
&\boldsymbol{k}^*_{h,i} := (\overbrace{s_{h,i}\vec{v}_{h,i},}^{n}\ \overbrace{\xi_{h,i,j+1}\ r_{h,i}\vec{v}_{h,i},}^{n}\\
&\quad\overbrace{r_{h,i}\vec{v}_{h,i} \cdot \boxed{(\textstyle\sum_{\kappa=1}^{j} \xi_{h,i,\kappa} Z_\kappa)}}^{n},\ \overbrace{\vec{\eta}_{h,i},\ 0^n}^{3n})_{\mathbb{B}^*_1},
\end{aligned}\right\}\tag{12}$$

where $Z_j \overset{\mathsf{U}}{\leftarrow} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}$ and all the other 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:

$$\left.\begin{aligned}
&\boldsymbol{k}^*_0 := (-s_{h,0},\ \boxed{w_{h,0}},\ 1,\ \eta_{h,0},\ 0)_{\mathbb{B}^*_0},\\
&\text{for } i = 1, \ldots, \ell,\\
&\text{if } \rho_h(i) = v_{h,i} \wedge v_{h,i} \notin \Gamma,\\
&\boldsymbol{k}^*_{h,i} := (\overbrace{s_{h,i}\vec{e}_1 + \theta_{h,i}\vec{v}_{h,i},}^{n}\quad \overbrace{0^n,\ \boxed{\vec{w}_{h,i}},}^{2n}\ \overbrace{\vec{\eta}_{h,i},\ 0^n}^{3n})_{\mathbb{B}^*_1},\\
&\text{if } \rho_h(i) = \neg v_{h,i} \wedge v_{h,i} \in \Gamma,\\
&\boldsymbol{k}^*_{h,i} := (\quad s_{h,i}\vec{v}_{h,i},\qquad 0^n,\ \boxed{\vec{\vec{w}}_{h,i}},\ \vec{\eta}_{h,i},\ 0^n)_{\mathbb{B}^*_1},
\end{aligned}\right\}\tag{13}$$

where $w_{h,0} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$, $\vec{w}_{h,i} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q^n$, $\vec{\vec{w}}_{h,i} \overset{\mathsf{U}}{\leftarrow} \mathsf{span}\langle\vec{y}\rangle^{\perp}$, 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

$$\boldsymbol{c}_0 := (\omega,\ \tau,\ \boxed{\zeta'},\ 0,\ \varphi_0)_{\mathbb{B}_0},\quad c_T := g_T^{\zeta} m^{(b)},\tag{14}$$

where $\zeta' \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$ (i.e., independent from $\zeta \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$), 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 $\mathsf{Adv}^{\mathsf{KP\text{-}ABE,SA}}_{\mathcal{A}}(\lambda) \le \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}2}}(\lambda) + \sum_{j=1}^{n} \left(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}j\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}j\text{-}2}}(\lambda)\right) + \epsilon$, where $\epsilon := (3\nu\hat{\ell} + 10n + 11)/q$. This completes the proof of Theorem 1. □

6.3 Lemmas

All the proofs of Lemmas in Sect. 6.3, i.e., Lemmas 5–12, are given in Appendix B.

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

$\mathcal{G}^{\mathsf{P1}}_\beta(1^\lambda, n):$

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

$\mathbb{B}_1 := (\boldsymbol{b}_{1,1}, \dots, \boldsymbol{b}^*_{1,6n})$ is calculated from $\{B_{i,j}, B'_{i,j,l}\}^{i,j=1,\dots,6}_{l=1,\dots,n}$,

$\widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,3}, .., \boldsymbol{b}^*_{0,5}), \widehat{\mathbb{B}}^*_1 := (\boldsymbol{b}^*_{1,1}, .., \boldsymbol{b}^*_{1,n}, \boldsymbol{b}^*_{1,3n+1}, .., \boldsymbol{b}^*_{1,6n})$,

$\delta, \delta_0, \omega, \varphi_\iota \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \tau, \rho \xleftarrow{\mathsf{U}} \mathbb{F}^\times_q$ 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 $i = 1, \dots, n$; $\vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}^n_q,\ \vec{\delta}_i \xleftarrow{\mathsf{U}} \mathbb{F}^{2n}_q$,

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

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

for $\beta \xleftarrow{\mathsf{U}} \{0, 1\}$. For a probabilistic adversary C, we define the advantage of C as the quantity

$$\mathsf{Adv}^{\mathsf{P1}}_C(\lambda) := \left|\Pr\left[C(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_0(1^\lambda, n)\right] - \Pr\left[C(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_1(1^\lambda, n)\right]\right|.$$

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

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

$\mathcal{G}^{\mathsf{P2}}_\beta(1^\lambda, n):$

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

$\widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, .., \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,3n+1}, .., \boldsymbol{b}_{1,6n})$ is calculated

from $\{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n},\ \ \tau, \rho \xleftarrow{\mathsf{U}} \mathbb{F}^\times_q$,

$\boldsymbol{f}^*_0 := \rho\boldsymbol{b}^*_{0,2},\ \boldsymbol{e}_0 := \tau\boldsymbol{b}_{0,2},\ \boldsymbol{f}^*_i := \rho\boldsymbol{b}^*_{1,n+i}$ for $i = 1, \dots, 2n$,

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

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

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

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

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

Lemma 7: For any adversary $\mathcal{A}$, there exists a probabilistic machine C_1, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P1}}_{C_1}(\lambda)$.

Lemma 8: For any adversary $\mathcal{A}$, there exists a probabilistic machine C_2, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(2\text{-}(j-1)\text{-}2)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}j\text{-}1)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P2}}_{C_{2\text{-}j}}(\lambda)$, where $C_{2\text{-}j}(\cdot) := C_2(j, \cdot)$.

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

Lemma 10: For any adversary $\mathcal{A}$, for any security parameter λ, $|\mathsf{Adv}^{(2\text{-}n\text{-}2)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)| \le 3\nu\hat{\ell}/q$, 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, $|\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda)| \le 1/q$.

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

6.4 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 $Z_{h,i} \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}$ 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 [41]. 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 Sect. 6.4.1 (resp. 6.4.2).

6.4.1 Iteration of Swaps and Conceptual Changes for Theorem 1

Theorem 1 is proven by the hybrid argument through $2n + 4$ games (given in Sect. 6.1).

First, in Game 0, coefficients of the hidden parts of $\boldsymbol{c}_1$ and $\boldsymbol{k}^*_{h,i}$ $(h = 1, \dots, \nu; i = 1, \dots, \ell)$ are all zero. Then, in the next Game 1, that of $\boldsymbol{c}_1$ is filled with $(\tau\vec{y}, \tau\vec{y}) \in \mathbb{F}^{2n}_q$ and the first n-dim. coefficient (block) of the hidden parts of $\boldsymbol{k}^*_{h,i}$ $(h = 1, \dots, \nu)$ are changed to $\vec{p}_{h,i} \in \mathbb{F}^n_q$ 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)

Coefficients of the hidden part of $\boldsymbol{c}_1$ in Game 0

$$\begin{array}{|c|c|}\hline \qquad\qquad & \qquad\qquad \\ \hline\end{array}$$

Coefficients of the hidden part of $\boldsymbol{c}_1$ in Game 1

$$\longrightarrow \quad \begin{array}{|c|c|}\hline \tau\vec{y} & \tau\vec{y} \\ \hline\end{array}$$

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

$$\begin{array}{r|c|c|} h=1 & \qquad & \qquad \\ \vdots & & \\ \vdots & & \\ \nu & & \end{array}$$

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

$$\longrightarrow \quad \begin{array}{r|c|c|} h=1 & \vec{p}_{1,i} & \qquad \\ \vdots & \vdots & \\ \vdots & \vdots & \\ \nu & \vec{p}_{\nu,i} & \end{array}$$

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

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

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

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

$$\xrightarrow[\vec{p}_{h,i} \cdot \xi_{h,i,j} I_n]{\text{swap}}$$

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

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

$$\xrightarrow{\substack{\text{change } \xi_{h,i,j} I_n \\ \text{to } \xi_{h,i,j} Z_j}}$$

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

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

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

$$\rightarrow \quad \begin{array}{r|c|c|} h=1 & \qquad & \vec{p}_{1,i} \cdot (\sum_{\kappa=1}^{n} \xi_{1,i,\kappa} Z_\kappa) \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \nu & & \vec{p}_{\nu,i} \cdot (\sum_{\kappa=1}^{n} \xi_{\nu,i,\kappa} Z_\kappa) \end{array}$$

$$= \quad \begin{array}{r|c|c|} h=1 & \qquad & \vec{p}_{1,i} \cdot Z_{1,i} \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \nu & & \vec{p}_{\nu,i} \cdot Z_{\nu,i} \end{array}$$

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 Sect. 6.4.2). 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 $Z_{h,i} \overset{\mathsf{U}}{\leftarrow} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}$, 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 Sect. 6.4.2).

Hence, in Game 3, the coefficient vector is changed to $\vec{\omega}_{h,i} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q^n$ if $\rho_h(i) = v_{h,i} \wedge v_{h,i} \notin \Gamma$, $\vec{\omega}_{h,i} \overset{\mathsf{U}}{\leftarrow} \mathsf{span}\langle \vec{y}\rangle^{\perp}$ 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.

6.4.2 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 $U \overset{\mathsf{U}}{\leftarrow} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ 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 $(Z_1, \ldots, Z_{j-1}, I_n)Z_j = (Z_1Z_j, \ldots, Z_{j-1}Z_j, Z_j)$ is uniformly distributed in $\left(\mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}\right)^j$ if $Z_i \overset{\mathsf{U}}{\leftarrow} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}$ 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 $A_{n-1} := \{\vec{u}' \in \mathbb{F}_q^n \,|\, \vec{y} \cdot \vec{u}' = y_n\}$ 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 $Z_\kappa \overset{\mathsf{U}}{\leftarrow} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}$ (Lemma 2).
4. $\vec{v}Z$ distributes uniformly in $W_{\vec{y},(\vec{y}\cdot\vec{v})} := \{\vec{w} \in \mathbb{F}_q^n \setminus \mathsf{span}\langle\vec{e}_n\rangle^\perp \,|\, \vec{y} \cdot \vec{w} = \vec{y} \cdot \vec{v}\}$ (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 [36] 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 $\mathcal{H}(n, \mathbb{F}_q)$ [36]): 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 $W'_{\vec{y},\pi} := \{(\vec{r}, \vec{w}) \in (\mathsf{span}\langle\vec{y}, \vec{e}_n\rangle \setminus \mathsf{span}\langle\vec{e}_n\rangle) \times (\mathbb{F}_q^n \setminus \mathsf{span}\langle\vec{e}_n\rangle^\perp) \,|\, \vec{r} \cdot \vec{w} = \pi\}$.
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 $U \overset{\mathsf{U}}{\leftarrow} \mathcal{H}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q)$ and $Z := (U^{-1})^{\mathrm{T}}$.

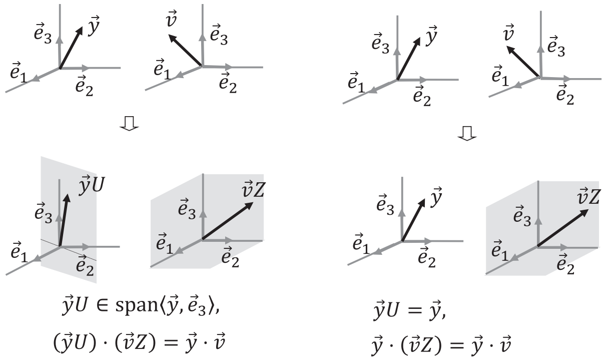

$\vec{e}_3$
$\vec{y}$
$\vec{e}_1$
$\vec{e}_2$
$\vec{v}$
⇩
$\vec{y}U$
$\vec{v}Z$
$\vec{y}U \in \mathrm{span}\langle\vec{y}, \vec{e}_3\rangle,$
$(\vec{y}U) \cdot (\vec{v}Z) = \vec{y} \cdot \vec{v}$
$\vec{y}U = \vec{y},$
$\vec{y} \cdot (\vec{v}Z) = \vec{y} \cdot \vec{v}$

Fig. 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.

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 $U \overset{\mathsf{U}}{\leftarrow} \mathcal{H}(n, \mathbb{F}_q) \cap GL(n, \mathbb{F}_q)$ 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 $U \overset{\mathsf{U}}{\leftarrow} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)$ 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 Sect. 6.4.1.

6.5 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 Sect. 6.1) is bounded by the advantage of Problem 3.

6.5.1 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 on 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 Sect. 7.3.2, 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

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

$$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \ldots, \boldsymbol{b}_{0,5}),\ \widehat{\mathbb{B}}_0^* := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,3}, \ldots, \boldsymbol{b}^*_{0,5}),$$

$$\widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, .., \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,3n+1}, .., \boldsymbol{b}_{1,6n}) \text{ is calculated as in Eq. (5) from } \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n},$$

$$\widehat{\mathbb{B}}_1^* := (\boldsymbol{b}^*_{1,1}, .., \boldsymbol{b}^*_{1,n}, \boldsymbol{b}^*_{1,3n+1}, .., \boldsymbol{b}^*_{1,6n}),$$

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

$$\delta, \delta_0, \omega, \varphi_0, \varphi_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \tau, \rho \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\times},$$
$$\boldsymbol{h}^*_{0,0} := (\delta, 0, 0, \delta_0, 0)_{\mathbb{B}_0^*},\ \ \boldsymbol{h}^*_{1,0} := (\delta, \rho, 0, \delta_0, 0)_{\mathbb{B}_0^*},$$
$$\boldsymbol{e}_{0,0} := (\omega, 0, 0, 0, \varphi_0)_{\mathbb{B}_0},\ \ \boldsymbol{e}_{1,0} := (\omega, \tau, 0, 0, \varphi_0)_{\mathbb{B}_0},$$
$$\text{for } j = 1, .., n;\ i = 1, .., n;\ \ \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n,$$
$$U_j \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q),\ \ Z_j := (U_j^{-1})^{\mathrm{T}},\ \vec{\delta}_{j,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n},$$
$$\begin{array}{llcccl}
\boldsymbol{h}^*_{0,j,i} := (& \overbrace{\delta\vec{e}_i,}^{n} & \overbrace{0^{2n},}^{2n} & \overbrace{\vec{\delta}_{j,i},}^{2n} & \overbrace{0^n}^{n} &)_{\mathbb{B}_1^*} \\
\boldsymbol{h}^*_{1,j,i} := (& \delta\vec{e}_i, & 0^n,\ \rho\vec{e}_i \cdot Z_j, & \vec{\delta}_{j,i}, & 0^n &)_{\mathbb{B}_1^*} \\
\boldsymbol{e}_{0,1} := (& \omega\vec{y}, & 0^{2n}, & 0^{2n}, & \varphi_1\vec{y} &)_{\mathbb{B}_1}, \\
\boldsymbol{e}_{1,1} := (& \omega\vec{y}, & \tau\vec{y},\quad \tau\vec{y}, & 0^{2n}, & \varphi_1\vec{y} &)_{\mathbb{B}_1},
\end{array}$$

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

For a probabilistic adversary $\mathcal{B}$, we define the advantage of $\mathcal{B}$ as the quantity $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P3}}(\lambda) :=$

$$\Big|\mathsf{Pr}\Big[\mathcal{B} \text{ outputs } 1 \,\Big|\varrho_1 \text{ and } \varrho_2 \text{ with } \beta = 0 \text{ are given to } \mathcal{B}\Big]$$
$$-\mathsf{Pr}\Big[\mathcal{B} \text{ outputs } 1 \,\Big|\varrho_1 \text{ and } \varrho_2 \text{ with } \beta = 1 \text{ are given to } \mathcal{B}\Big]\Big|.$$

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

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

The proof of Lemma 14 is given in Appendix C.1.

6.5.2 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 Sect. 6.1.

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

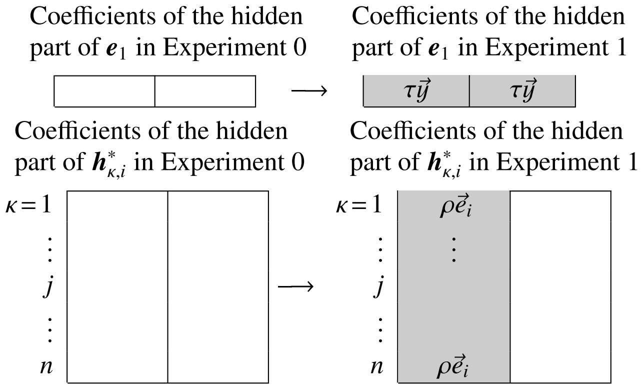
The proof of Lemma 15 is given in Appendix C.2.

6.5.3 Iteration of Swaps and Conceptual Changes for Lemma 14

For comparison of the proofs in Sects. 6.1 and 6.5, we describe the (simple) iteration of swaps and conceptual changes for the proof of Lemma 14 here. Refer to Sect. 6.4.1 for comparison.

Lemma 14 is proven by the hybrid argument through $2n + 2$ experiments (given in Appendix C.1): Experiment 0 ⇒ Experiment 1 ⇒ for $j = 1, \dots, n$; Experiment 2-j-1 ⇒ 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 $\boldsymbol{h}^*_{\kappa,i}$ ($\kappa = 1, \dots, n$) 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 $\boldsymbol{h}^*_{\kappa,i}$ ($\kappa = 1, \dots, n$) are changed to $\rho\vec{e}_i \in \mathbb{F}_q^n$ as: (Hereafter, a blank indicates zero coefficients)


Coefficients of the hidden part of $\boldsymbol{e}_1$ in Experiment 0

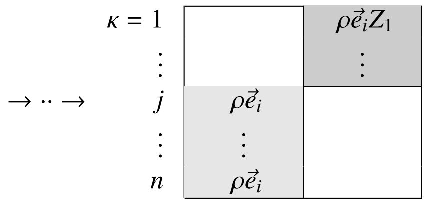
Coefficients of the hidden part of $\boldsymbol{e}_1$ in Experiment 1

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

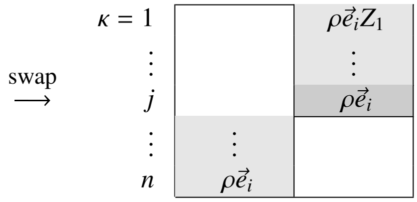
Coefficients of the hidden part of $\boldsymbol{h}^*_{\kappa,i}$ in Experiment 1

After that, in turn for $j = 1, \dots, n$, the coefficient vector $\rho\vec{e}_i \in \mathbb{F}_q^n$ is *swapped* to the second block of the hidden parts of $\boldsymbol{h}^*_{j,i}$ 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 $\rho\vec{e}_i Z_j$ ($j = 1, \dots, n$) 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.

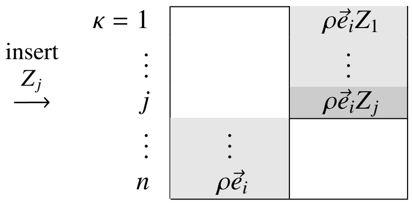
Coefficients of the hidden part of $\boldsymbol{h}^*_{\kappa,i}$ in Experiment 2-(j − 1)-2



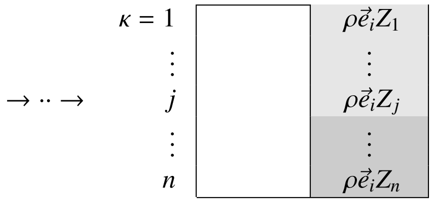
Coefficients of the hidden part of $\boldsymbol{h}^*_{\kappa,i}$ in Experiment 2-j-1



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



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



Insertion of Z_j is realized by a conceptual basis change determined by Z_j (see item 2 in Sect. 6.4.2).

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. The ABS scheme is based on the CP-ABE scheme with constant-size secret keys, which is given in Appendix D.2. The CP-ABE is the dual form of the KP-ABE in Sect. 5.3. While the underlying CP-ABE is only proven that it has *non-adaptive* payload-hiding security (Theorem 4 in Appendix D.2)[†], the weak security of the CP-ABE is enough to prove *adaptive*-predicate unforgeability of our ABS below.

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.

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

Remark 5: From Remark 3, $\{B^*_{i,j}, B'^*_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n}$ 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 $\mathsf{Adv}^{\mathsf{H,CR}}_{\mathcal{F}}(\lambda) := \Pr[(\varrho_1, \varrho_2) \in \mathsf{D}^2 \wedge \varrho_1 \neq \varrho_2 \wedge \mathsf{H}^{\lambda,\mathsf{D}}_{\mathsf{hk}}(\varrho_1) = \mathsf{H}^{\lambda,\mathsf{D}}_{\mathsf{hk}}(\varrho_2)]$, 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 $\mathcal{F}$, $\mathsf{Adv}^{\mathsf{H,CR}}_{\mathcal{F}}(\lambda)$ is negligible in λ.

7.2 Construction

$$\begin{aligned}
&\mathsf{Setup}(1^\lambda,\ n) : (\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \mathbb{B}_1, \{B^*_{i,j}, B'^*_{i,j,l}\}_{l=1,\ldots,n}^{i,j=1,\ldots,6},\\
&\qquad\qquad \mathbb{B}_2, \mathbb{B}^*_2) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{ABS}}_{\mathsf{ob}}(1^\lambda, 6, n),\quad \mathsf{hk} \xleftarrow{\mathsf{R}} \mathsf{KH}_\lambda,\\
&\quad \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}),\\
&\quad \widehat{\mathbb{B}}^*_1 := (\boldsymbol{b}^*_{1,1}, .., \boldsymbol{b}^*_{1,n}, \boldsymbol{b}^*_{1,3n+1}, .., \boldsymbol{b}^*_{1,4n}) = \{B^*_{i,j}, B'^*_{i,j,l}\}_{l=1,..,n}^{i=1,4;j=1,..,6},\\
&\quad \widehat{\mathbb{B}}_2 := (\boldsymbol{b}_{2,1}, \boldsymbol{b}_{2,2}, \boldsymbol{b}_{2,7}),\ \widehat{\mathbb{B}}^*_2 := (\boldsymbol{b}^*_{2,1}, \boldsymbol{b}^*_{2,2}, \boldsymbol{b}^*_{2,5}, \boldsymbol{b}^*_{2,6}),\\
&\quad \text{return } \mathsf{sk} := \boldsymbol{b}^*_{0,1},\\
&\quad\ \mathsf{pk} := (1^\lambda, \mathsf{hk}, \mathsf{param}_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\}) :\\
&\quad \vec{y} := (y_1, \ldots, y_n) \text{ s.t. } \textstyle\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \cdot \prod_{j=1}^{n'} (z - x_j),\\
&\quad \omega, \varphi_0, \varphi_1, \varphi_{2,1,1}, \varphi_{2,1,2}, \varphi_{2,2,1}, \varphi_{2,2,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
&\quad \boldsymbol{k}^*_0 := (\omega, 0, \varphi_0, 0)_{\mathbb{B}^*_0}, L^*_{1,j} := \omega B^*_{1,j} + \varphi_1 B^*_{4,j},\\
&\quad\ L^*_{2,j} := \textstyle\sum_{l=1}^n y_l(\omega B'^*_{1,j,l} + \varphi_1 B'^*_{4,j,l}) \text{ for } j = 1, \ldots, 6,\\
&\quad \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},\\
&\quad \text{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}).
\end{aligned}$$

[†] Non-adaptive security of CP-ABE means that the adversary's key queries may not depend on the challenge ciphertext [42]. See Defintion 19 in Appendix D.1.

Remark From $\{L^*_{1,j}, L^*_{2,j}\}_{j=1,\ldots,6}$ and $\vec{y}$, $\boldsymbol{k}^*_1$ is defined as

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

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

$\mathsf{Sig}(\mathsf{pk}, \mathsf{sk}_\Gamma, m, \mathbb{S} := (M,\rho))$: 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

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

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

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

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

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

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

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

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

$\boldsymbol{s}^*_{\ell+1} := \xi(\boldsymbol{k}^*_{2,1} + \mathsf{H}^{\lambda,\mathsf{D}}_{\mathsf{hk}}(m \,\|\, \mathbb{S}) \cdot \boldsymbol{k}^*_{2,2}) + \boldsymbol{r}^*_{\ell+1}$,

where $\boldsymbol{r}^*_{\ell+1} \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}^*_{2,5}, \boldsymbol{b}^*_{2,6} \rangle$, return $\vec{\boldsymbol{s}}^* := (\boldsymbol{s}^*_0, ..., \boldsymbol{s}^*_{\ell+1})$.

$\mathsf{Ver}(\mathsf{pk}, m, \mathbb{S} := (M,\rho), \vec{\boldsymbol{s}}^*)$:

$\vec{f} \xleftarrow{\mathsf{R}} \mathbb{F}_q^{r}$, $s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$, $\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$,

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

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

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

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

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

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

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

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

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

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 [38] (privacy of the ABS scheme in [38]).

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,

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

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 reveal signature queries, and $\epsilon := (6\nu_K\hat{\ell} + 20\nu_K n + 10\nu_K + 10\nu_S + 5)/q$.

7.3.1 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 in access matrices of any reveal signature queries below.

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

$$\boldsymbol{k}^*_0 := (\omega, \boxed{0}, \varphi_0, 0)_{\mathbb{B}^*_0}, \tag{15}$$

$$\left.\begin{array}{l} \boldsymbol{k}^*_1 := (\overbrace{\omega\vec{y},}^{n} \overbrace{\boxed{0^{2n}}}^{2n}, \overbrace{\varphi_1\vec{y},}^{n} \overbrace{0^{2n}}^{2n})_{\mathbb{B}^*_1}, \\ \boldsymbol{k}^*_{2,1} := (\omega(1,0), 0, 0, \varphi_{2,1,1}, \varphi_{2,1,2}, 0)_{\mathbb{B}^*_2}, \\ \boldsymbol{k}^*_{2,2} := (\omega(0,1), 0, 0, \varphi_{2,2,1}, \varphi_{2,2,2}, 0)_{\mathbb{B}^*_2}, \end{array}\right\} \tag{16}$$

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:

$$\left.\begin{array}{l} \boldsymbol{s}^*_0 := (\widetilde{\delta}, \boxed{0}, \sigma_0, 0)_{\mathbb{B}^*_0}, \\ \boldsymbol{s}^*_i := (\vec{t}_i, 0^{2n}, \vec{\sigma}_i, 0^{2n})_{\mathbb{B}^*_1} \text{ for } i = 1, \ldots, \ell, \\ \boldsymbol{s}^*_{\ell+1} := (\widetilde{\delta}(1, \mathsf{H}^{\lambda,\mathsf{D}}_{\mathsf{hk}}(m \,\|\, \mathbb{S})), \boxed{0^2}, \vec{\sigma}_{\ell+1}, 0)_{\mathbb{B}^*_2}, \end{array}\right\} \tag{17}$$

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

$$\left.\begin{array}{l}
\boldsymbol{c}_0 := (\ \boxed{-s_0 - s_{\ell+1}},\ \boxed{0},\ 0,\ \eta_0\ )_{\mathbb{B}_0},\\
\text{for } i = 1,\dots,\ell,\\
\quad \text{if } \rho(i) = v_i,\ \boldsymbol{c}_i := (\overbrace{s_i\vec{e}_1 + \theta_i\vec{v}_i,}^{n}\ \overbrace{\boxed{0^{2n}}}^{2n},\ \overbrace{0^n,}^{n}\ \overbrace{\vec{\eta}_i}^{2n}\ )_{\mathbb{B}_1},\\
\quad \text{if } \rho(i) = \neg v_i,\ \boldsymbol{c}_i := (s_i\vec{v}_i,\ \boxed{0^{2n}},\ 0^n,\ \vec{\eta}_i\ )_{\mathbb{B}_1},\\
\boldsymbol{c}_{\ell+1} :=\\
\quad (s_{\ell+1}\vec{e}_1 + \theta_{\ell+1}(-\mathsf{H}_{\mathsf{hk}}^{\lambda,\mathsf{D}}(m' \parallel \mathbb{S}'), 1), \boxed{0^2}, 0^2, \eta_{\ell+1})_{\mathbb{B}_2},
\end{array}\right\} \quad (18)$$

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

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

$$\boldsymbol{c}_0 := (-s_0 - s_{\ell+1},\ \boxed{-r_0 - r_{\ell+1}},\ 0,\ \eta_0)_{\mathbb{B}_0}, \quad (19)$$

for $i = 1,\dots,\ell$,

$$\left.\begin{array}{l}
\text{if } \rho(i) = v_i, \boldsymbol{c}_i := (\overbrace{s_i\vec{e}_1 + \theta_i\vec{v}_i,}^{n}\ \overbrace{\boxed{r_i\vec{e}_1 + \psi_i\vec{v}_i},\ 0^n,}^{2n}\ \overbrace{0^n, \vec{\eta}_i}^{3n})_{\mathbb{B}_1},\\
\text{if } \rho(i) = \neg v_i, \boldsymbol{c}_i := (s_i\vec{v}_i,\ \boxed{r_i\vec{v}_i},\ 0^n,\ 0^n, \vec{\eta}_i)_{\mathbb{B}_1},
\end{array}\right\} \quad (20)$$

$$\begin{array}{l}
\boldsymbol{c}_{\ell+1} := (s_{\ell+1}\vec{e}_1 + \theta_{\ell+1}(-\mathsf{H}_{\mathsf{hk}}^{\lambda,\mathsf{D}}(m' \parallel \mathbb{S}'), 1),\\
\qquad\qquad\qquad \boxed{\vec{\psi}_{\ell+1}}, 0^2, \eta_{\ell+1})_{\mathbb{B}_2},
\end{array} \quad (21)$$

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

Game 2-*h*-1 (*h* = 1, . . . , ν_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 reveal key query for Γ are:

$$\boldsymbol{k}_0^* := (\omega,\ \boxed{\tau'},\ \varphi_0,\ 0)_{\mathbb{B}_0^*}, \quad (22)$$

$$\boldsymbol{k}_1^* := (\ \overbrace{\omega\vec{y},}^{n}\ \overbrace{\boxed{\tau\vec{y},\ \tau\vec{y}}}^{2n},\ \overbrace{\varphi_1\vec{y},}^{n}\ \overbrace{0^{2n}}^{2n}\ )_{\mathbb{B}_1^*},$$

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

$$\begin{array}{l}
\text{if } \rho(i) = v_i \wedge v_i \notin \Gamma,\ \boldsymbol{c}_i := (\overbrace{s_i\vec{e}_1 + \theta_i\vec{v}_i,}^{n}\ \overbrace{0^n, \boxed{\vec{w}_i},}^{2n}\ \overbrace{0^n, \vec{\eta}_i}^{3n})_{\mathbb{B}_1},\\
\text{if } \rho(i) = \neg v_i \wedge v_i \in \Gamma,\ \boldsymbol{c}_i := (s_i\vec{v}_i,\ 0^n, \boxed{\vec{\overline{w}}_i},\ 0^n, \vec{\eta}_i)_{\mathbb{B}_1},
\end{array}$$

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

Game 2-*h*-2 (*h* = 1, . . . , ν_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. (20), and the components $\boldsymbol{k}_1^*$, $\boldsymbol{k}_{2,1}^*$ and $\boldsymbol{k}_{2,2}^*$ of the reply to the h-th reveal key query for Γ is given by Eq. (16) (and $\boldsymbol{k}_0^*$ is given by Eq. (22)). all the other variables are generated as in Game 2-h-1.

Game 3-*h* (*h* = 1, . . . , ν_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:

$$\left.\begin{array}{l}
\boldsymbol{s}_0^* := (\ \widetilde{\delta},\ \boxed{\pi_0},\ \sigma_0,\ 0\ )_{\mathbb{B}_0^*},\\
\boldsymbol{s}_{\ell+1}^* := (\ \widetilde{\delta}(1, \mathsf{H}_{\mathsf{hk}}^{\lambda,\mathsf{D}}(m \parallel \mathbb{S})),\ \boxed{\vec{\pi}_{\ell+1}},\ \vec{\sigma}_{\ell+1},\ 0\ )_{\mathbb{B}_2^*},
\end{array}\right\} \quad (23)$$

where $\pi_0 \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$, $\vec{\pi}_{\ell+1} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q^2$, 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:

$$\boldsymbol{c}_0 := (\ \boxed{\widetilde{s}_0},\ -r_0 - r_{\ell+1},\ 0,\ \eta_0\ )_{\mathbb{B}_0}, \quad (24)$$

where $\widetilde{s}_0 \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$ (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 $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{ABS,UF}}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) \le \left|\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)\right| + \sum_{h=1}^{\nu_K}(\left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1)\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda)\right| + \left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2)}(\lambda)\right|) + \sum_{h=1}^{\nu_S} \left|\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}(h-1))}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h)}(\lambda)\right| + \left|\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}\nu_S)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)\right| + \mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda) \le \mathsf{Adv}_{\mathcal{F}_0}^{\mathsf{DLIN}}(\lambda) + \sum_{l=1}^{2} \sum_{h=1}^{\nu_K}(\mathsf{Adv}_{\mathcal{F}_{l\text{-}h\text{-}0}}^{\mathsf{DLIN}}(\lambda) + \sum_{j=1}^{n} \sum_{\iota=1}^{2} \mathsf{Adv}_{\mathcal{F}_{l\text{-}h\text{-}j\text{-}\iota}}^{\mathsf{DLIN}}(\lambda)) + \sum_{h=1}^{\nu_S}(\mathsf{Adv}_{\mathcal{F}_{3\text{-}h}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_{4\text{-}h}}^{\mathsf{H,CR}}(\lambda)) + (6\nu_K\hat{\ell} + 20\nu_K n + 10\nu_K + 10\nu_S + 5)/q$. This completes the proof of Theorem 3. □

7.3.2 Lemmas

We will show Lemmas 16–24 for the proof of Theorem 3. The proofs of the lemmas except for Lemma 17 are given in Appendix E.

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

$$\begin{array}{l}
\mathcal{G}_\beta^{\mathsf{P4}}(1^\lambda, n) : (\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1,\\
\qquad\qquad \{B_{i,j}^*, B'^{\,*}_{i,j,l}\}_{l=1,\dots,n}^{i,j=1,\dots,6}, \mathbb{B}_2, \mathbb{B}_2^*) \overset{\mathsf{R}}{\leftarrow} \mathcal{G}_{\mathsf{ob}}^{\mathsf{ABS}}(1^\lambda, 6, n),\\
\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*, \boldsymbol{b}_{0,4}^*), \widehat{\mathbb{B}}_1^* := (\boldsymbol{b}_{1,1}^*, .., \boldsymbol{b}_{1,n}^*, \boldsymbol{b}_{1,3n+1}^*, .., \boldsymbol{b}_{1,6n}^*)
\end{array}$$

is calculated as in Eq. (5) from $\{B^*_{i,j}, B'^*_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n}$,

$$\widehat{\mathbb{B}}^*_2 := (\boldsymbol{b}^*_{2,1}, \boldsymbol{b}^*_{2,2}, \boldsymbol{b}^*_{2,5}, .., \boldsymbol{b}^*_{2,7}), \quad \delta, \delta_0 \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q,\ \rho \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q^{\times},$$

$$\boldsymbol{e}_{0,0} := (\delta, 0, 0, \delta_0)_{\mathbb{B}_0},\ \boldsymbol{e}_{1,0} := (\delta, \rho, 0, \delta_0)_{\mathbb{B}_0},$$

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

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

$$\vec{\psi} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q^2,$$

$$\boldsymbol{e}_{0,n+1} := (\delta, 0, 0^2, 0^2, \delta_{n+1})_{\mathbb{B}_2}, \boldsymbol{e}_{1,n+1} := (\delta, 0, \vec{\psi}, 0^2, \delta_{n+1})_{\mathbb{B}_2},$$

$$\text{return } (\mathsf{param}_n, \{\mathbb{B}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,1,2}, \{\boldsymbol{e}_{\beta,i}\}_{i=0,\ldots,n+1}),$$

for $\beta \overset{\mathsf{U}}{\leftarrow} \{0, 1\}$. For a probabilistic machine $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 4, $\mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}}(\lambda)$, 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, $\mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}}(\lambda) + 5/q$.

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

1. The challenger generates

$$(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \mathbb{B}_1, \{B^*_{i,j}, B'^*_{i,j,l}\}^{i,j=1,\ldots,6}_{l=1,\ldots,n}, \mathbb{B}_2, \mathbb{B}^*_2) \overset{\mathsf{R}}{\leftarrow} \mathcal{G}^{\mathsf{ABS}}_{\mathsf{ob}}(1^\lambda, 6, n),$$

$$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,4}), \widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, .., \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,3n+1}, .., \boldsymbol{b}_{1,6n}),$$

$\widehat{\mathbb{B}}^*_1 := (\boldsymbol{b}^*_{1,1}, .., \boldsymbol{b}^*_{1,n}, \boldsymbol{b}^*_{1,3n+1}, .., \boldsymbol{b}^*_{1,6n})$ is calculated as in Eq. (5) 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

$$\delta, \delta_0, \omega, \varphi_0, \varphi_1 \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q,\ \tau, \rho \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q^{\times},\ \boldsymbol{h}^*_{0,0} := (\omega, 0, \varphi_0, 0)_{\mathbb{B}^*_0},$$

$$\boldsymbol{h}^*_{1,0} := (\omega, \tau, \varphi_0, 0)_{\mathbb{B}^*_0}, \quad \boldsymbol{e}_0 := (\delta, \rho, 0, \delta_0)_{\mathbb{B}_0},$$

$$\text{for } j = 1, \ldots, n;\ i = 1, \ldots, n;$$

$$\vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n,\ \vec{\delta}_{j,i} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q^{2n},$$

$$U_j \overset{\mathsf{U}}{\leftarrow} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q),\ Z_j := (U_j^{-1})^{\mathrm{T}},$$

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

$$\text{for } i = 1, 2,\ \boldsymbol{h}^*_{2,i} := \omega\boldsymbol{b}^*_{2,i},$$

for $\beta \overset{\mathsf{U}}{\leftarrow} \{0, 1\}$, 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 $\mathsf{Adv}^{\mathsf{P5}}_{\mathcal{B}}(\lambda) :=$

$$\Big|\mathsf{Pr}\left[\mathcal{B} \text{ outputs } 1 \,\middle|\, \varrho_1 \text{ and } \varrho_2 \text{ with } \beta = 0 \text{ are given to } \mathcal{B}\right] - \mathsf{Pr}\left[\mathcal{B} \text{ outputs } 1 \,\middle|\, \varrho_1 \text{ and } \varrho_2 \text{ with } \beta = 1 \text{ are given to } \mathcal{B}\right]\Big|.$$

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, $\mathsf{Adv}^{\mathsf{P5}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_0}(\lambda) + \sum_{j=1}^{n} \sum_{\iota=1}^{2} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{j\text{-}\iota}}(\lambda) + (10n+5)/q$, 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 $(\mathsf{param}_n, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t\}_{t=0,2}, \mathbb{B}_1, \mathbb{B}^*_1, \boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{1,i}\}_{i=1,..,n}, \{\boldsymbol{h}^*_{\beta,2,i}, \boldsymbol{e}_{2,i}\}_{i=1,2}) \overset{\mathsf{R}}{\leftarrow} \mathcal{G}^{\mathsf{P6}}_{\beta}(1^\lambda, n)$, where

$$\mathcal{G}^{\mathsf{P6}}_{\beta}(1^\lambda, n) : (\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \mathbb{B}_1, \{B^*_{i,j}, B'^*_{i,j,l}\}^{i,j=1,\ldots,6}_{l=1,\ldots,n}, \mathbb{B}_2, \mathbb{B}^*_2) \overset{\mathsf{R}}{\leftarrow} \mathcal{G}^{\mathsf{ABS}}_{\mathsf{ob}}(1^\lambda, 6, n),$$

$$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,4}), \ \ \widehat{\mathbb{B}}_2 := (\boldsymbol{b}_{2,1}, \boldsymbol{b}_{2,2}, \boldsymbol{b}_{2,5}, \ldots, \boldsymbol{b}_{2,7}),$$

$\mathbb{B}^*_1 := (\boldsymbol{b}^*_{1,1}, .., \boldsymbol{b}^*_{1,6n})$ is calculated as in Eq. (5) from

$$\{B^*_{i,j}, B'^*_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n}, \ \ \sigma, \tau \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q^{\times},\ \omega, \delta, \delta_0 \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q,$$

$$\boldsymbol{h}^*_{0,0} := (\delta, 0, \delta_0, 0)_{\mathbb{B}^*_0},\ \boldsymbol{h}^*_{1,0} := (\delta, \sigma, \delta_0, 0)_{\mathbb{B}^*_0},$$

$$\boldsymbol{e}_0 := (\omega, \tau, 0, 0)_{\mathbb{B}_0}, \ \ \boldsymbol{h}^*_{1,i} := \delta\boldsymbol{b}^*_{1,i} \ \text{ for } i = 1, \ldots, n,$$

$$U \overset{\mathsf{U}}{\leftarrow} GL(2, \mathbb{F}_q),\ Z := (U^{-1})^{\mathrm{T}},$$

$$\text{for } i = 1, 2; \quad \vec{e}_i := (0^{i-1},\ 1,\ 0^{2-i}),\ \vec{\delta}_i \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q^2,$$

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

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

for $\beta \overset{\mathsf{U}}{\leftarrow} \{0, 1\}$. 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 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 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 reveal signature queries.

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, $|\mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}2)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P5}}_{\mathcal{B}_{2\text{-}h}}(\lambda) + 3\hat{\ell}/q$, 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 reveal signature queries.

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, $|\mathsf{Adv}^{(3\text{-}(h-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3\text{-}h)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P6}}_{\mathcal{B}_{3\text{-}h}}(\lambda) + \mathsf{Adv}^{\mathsf{H,CR}}_{\mathcal{F}_{4\text{-}h}}(\lambda) + 3/q$, 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 23: For any adversary $\mathcal{A}$, for any security parameter λ, $|\mathsf{Adv}^{(3\text{-}\nu_S)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda)| \le 1/q$.

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

References

[1] K. Takashima, "Expressive attribute-based encryption with constant-size ciphertexts from the decisional linear assumption," in Abdalla and Prisco [43], pp.298–317, 2014.

[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Cramer [47], pp.457–473, 2005.

[3] T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption," CRYPTO 2010, T. Rabin, ed., LNCS, vol.6223, pp.191–208, Springer, 2010. The full version is available as an online first article in Journal of Cryptology.

[4] S. Garg, C. Gentry, S. Halevi, A. Sahai, and B. Waters, "Attribute-based encryption for circuits from multilinear maps," in Canetti and Garay [44], pp.479–499, 2013.

[5] S. Gorbunov, V. Vaikuntanathan, and H. Wee, "Attribute-based encryption for circuits," STOC, D. Boneh, T. Roughgarden, and J. Feigenbaum, eds., pp.545–554, ACM, 2013.

[6] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," ISPEC 2009, F. Bao, H. Li, and G. Wang, eds., LNCS, vol.5451, pp.13–23, Springer, 2009.

[7] J. Herranz, F. Laguillaumie, and C. Ràfols, "Constant size ciphertexts in threshold attribute-based encryption," PKC 2010, P.Q. Nguyen and D. Pointcheval, eds., LNCS, vol.6056, pp.19–34, Springer, 2010.

[8] C. Chen, J. Chen, H.W. Lim, Z. Zhang, D. Feng, S. Ling, and H. Wang, "Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures," CT-RSA, ed. E. Dawson, LNCS, vol.7779, pp.50–67, Springer, 2013.

[9] N. Attrapadung, B. Libert, and E. de Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in Catalano et al. [46], pp.90–108, 2011.

[10] S. Yamada, N. Attrapadung, G. Hanaoka, and N. Kunihiro, "A framework and compact constructions for non-monotonic attribute-based encryption," PKC 2014, H. Krawczyk, ed., LNCS, vol.8383, pp.275–292, Springer, 2014.

[11] N. Attrapadung, "Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more," EUROCRYPT, P.Q. Nguyen and E. Oswald, eds., LNCS, vol.8441, pp.557–577, Springer, 2014.

[12] N. Attrapadung, "Dual system encryption framework in prime-order groups via computational pair encodings," ASIACRYPT 2016, Part II, pp.591–623, 2016.

[13] S. Agrawal and M. Chase, "Simplifying design and analysis of complex predicate encryption schemes," EUROCRYPT 2017, Part I, pp.627–656, 2017.

[14] N. Attrapadung, "Unbounded dynamic predicate compositions in attribute-based encryption," EUROCRYPT 2019, Part I, pp.34–67, 2019.

[15] S. Mitsunari, R. Sakai, and M. Kasahara, "A new traitor tracing," IEICE Trans. Fundamentals, vol.E85-A, no.2, pp.481–484, Feb. 2002.

[16] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," CRYPTO 2004, M.K. Franklin, ed., LNCS, vol.3152, pp.41–55, Springer, 2004.

[17] D. Boneh, X. Boyen, and E.J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in Cramer [47], pp.440–456, 2005.

[18] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," CRYPTO, V. Shoup, ed., Lecture Notes in Computer Science, vol.3621, pp.258–275, Springer, 2005.

[19] C. Gentry, "Practical identity-based encryption without random oracles," in Vaudenay [45], pp.445–464, 2006.

[20] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," ASIACRYPT, K. Kurosawa, ed., LNCS, vol.4833, pp.200–215, Springer, 2007.

[21] J.H. Cheon, "Security analysis of the strong diffie-hellman problem," in Vaudenay [45], pp.1–11, 2006.

[22] Y. Sakemi, G. Hanaoka, T. Izu, M. Takenaka, and M. Yasuda, "Solving a discrete logarithm problem with auxiliary input on a 160-bit elliptic curve," PKC, M. Fischlin, J. Buchmann, and M. Manulis, eds., LNCS, vol.7293, pp.595–608, Springer, 2012.

[23] J. Chen and H. Wee, "Semi-adaptive attribute-based encryption and improved delegation for boolean formula," in Abdalla and Prisco [43], pp.277–297, 2014.

[24] S. Agrawal and M. Chase, "A study of pair encodings: Predicate encryption in prime order groups," TCC 2016-A, Part II, pp.259–288, 2016. Full version is available at http://eprint.iacr.org/2015/413.

[25] J. Chen and H. Wee, "Fully, (almost) tightly secure IBE and dual system groups," CRYPTO 2013, Part II, pp.435–460, 2013.

[26] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures: Achieving attribute-privacy and collusion-resistance," IACR Cryptology ePrint Archive, vol.2008, p.328, 2008.

[27] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures," CT-RSA, A. Kiayias, ed., Lecture Notes in Computer Science, vol.6558, pp.376–392, Springer, 2011.

[28] T. Okamoto and K. Takashima, "Efficient attribute-based signatures for non-monotone predicates in the standard model," in Catalano et al. [46], pp.35–52, 2011. This is an extended abstract of a preliminary version of [38].

[29] Y. Sakai, N. Attrapadung, and G. Hanaoka, "Attribute-based signatures for circuits from bilinear map," PKC 2016, Part I, pp.283–300, 2016.

[30] R. Tsabary, "An equivalence between attribute-based signatures and homomorphic signatures, and new constructions for both," TCC 2017, Part II, pp.489–518, 2017.

[31] A. El Kaafarani and S. Katsumata, "Attribute-based signatures for unbounded circuits in the ROM and efficient instantiations from lattices," PKC 2018, Part II, pp.89–119, 2018.

[32] Y. Sakai, S. Katsumata, N. Attrapadung, and G. Hanaoka, "Attribute-based signatures for unbounded languages from standard assumptions," ASIACRYPT 2018, Part II, pp.493–522, 2018.

[33] P. Datta, T. Okamoto, and K. Takashima, "Efficient attribute-based signatures for unbounded arithmetic branching programs," PKC 2019, Part I, pp.127–158, 2019.

[34] T. Okamoto and K. Takashima, "Hierarchical predicate encryption for inner-products," ASIACRYPT 2009, M. Matsui, ed., LNCS, vol.5912, pp.214–231, Springer, 2009.

[35] T. Okamoto and K. Takashima, "Dual pairing vector spaces and their applications," IEICE Trans. Fundamentals, vol.E98-A, no.1, pp.3–15, Jan. 2015.

[36] T. Okamoto and K. Takashima, “Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption,” CANS 2011, D. Lin, G. Tsudik, and X. Wang, eds., LNCS, vol.7092, pp.138–159, Springer, 2011. Full version is available in Designs, Codes and Cryptography, vol.77, no.2-3, pp.725–771, 2015.

[37] A. Beimel, Secure Schemes for Secret Sharing and Key Distribution, PhD Thesis, Israel Institute of Technology, Technion, Haifa, 1996.

[38] T. Okamoto and K. Takashima, “Efficient attribute-based signatures for non-monotone predicates in the standard model,” IEEE Trans. Cloud Comput., vol.2, no.4, pp.409–421, 2014.Full version is available at http://eprint.iacr.org/2011/700.

[39] E. Shi and B. Waters, “Delegating capabilities in predicate encryption systems,” ICALP (2) 2008, L. Aceto, I. Damgård, L.A. Goldberg, M.M. Halldórsson, A. Ingólfsdóttir, and I. Walukiewicz, eds., LNCS, vol.5126, pp.560–578, Springer, 2008.

[40] B. Waters, “Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions,” CRYPTO 2009, S. Halevi, ed., LNCS, vol.5677, pp.619–636, Springer, 2009.

[41] T. Okamoto and K. Takashima, “Fully secure unbounded inner-product and attribute-based encryption,” ASIACRYPT, X. Wang and K. Sako, eds., Lecture Notes in Computer Science, vol.7658, pp.349–366, Springer, 2012. Full version is available at http://eprint.iacr.org/2012/671.

[42] S. Agrawal, S. Gorbunov, V. Vaikuntanathan, and H. Wee, “Functional encryption: New perspectives and lower bounds,” in Canetti and Garay [44], pp.500–518, 2013.

[43] M. Abdalla and R.D. Prisco, eds., Security and Cryptography for Networks — 9th International Conference, SCN 2014, Proceedings, Lecture Notes in Computer Science, vol.8642, Springer, Amalfi, Italy, Sept. 2014.

[44] R. Canetti and J.A. Garay, eds., Advances in Cryptology — CRYPTO 2013 — 33rd Annual Cryptology Conference, Proceedings, Part II, Lecture Notes in Computer Science, vol.8043, Springer, Santa Barbara, CA, USA, Aug. 2013.

[45] S. Vaudenay, ed., Advances in Cryptology — EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings, LNCS, vol.4004, Springer, St. Petersburg, Russia, May–June 2006.

[46] D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, eds., Public Key Cryptography — PKC 2011 — 14th International Conference on Practice and Theory in Public Key Cryptography, Proceedings, LNCS, vol.6571, Springer, Taormina, Italy, March 2011.

[47] R. Cramer, ed., Advances in Cryptology — EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings, LNCS, vol.3494, Springer, Aarhus, Denmark, May 2005.

Appendix A: Proofs of Lemmas in Sect. 4

A.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 $A_{n-1} := \{\vec{u}' \in \mathbb{F}_q^n \mid \vec{y} \cdot \vec{u}' = y_n\}$ 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}.

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 $V_{n-1} := \{\vec{u}' \in \mathbb{F}_q^n \mid \vec{y} \cdot \vec{u}' = 0\}$ over $\mathbb{F}_q$, the distribution of $Z := \sum_{\kappa=1}^n \xi_\kappa Z_\kappa$ with $(\xi_\kappa) \overset{\mathsf{U}}{\leftarrow} \{(\xi_\kappa)_{\kappa=1,\ldots,n} : \sum_{\kappa=1}^n \xi_\kappa = 1\}$ is equivalent to uniform one, i.e., $Z \overset{\mathsf{U}}{\leftarrow} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q)^{\mathrm{T}}$ 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 $(\xi_\kappa) \overset{\mathsf{U}}{\leftarrow} \{(\xi_\kappa)_{\kappa=1,\ldots,n} : \sum_{\kappa=1}^n \xi_\kappa = 1\}$,

$$\begin{aligned} Z &:= \sum_{\kappa=1}^n \xi_\kappa Z_\kappa = \sum_{\kappa=1}^n \xi_\kappa Z_1 + \sum_{\kappa=1}^n \xi_\kappa (Z_\kappa - Z_1) \\ &= Z_1 + \sum_{\kappa=2}^n \xi_\kappa \widetilde{Z}_\kappa, \qquad (\mathrm{A}\cdot 1) \end{aligned}$$

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. (A· 1) 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.2 Proof of Lemma 3

Lemma 3 For all $\vec{y} \in \mathbb{F}_q^n \setminus \mathsf{span}\langle \vec{e}_n \rangle$ and $\pi \in \mathbb{F}_q$, let $W_{\vec{y},\pi} := \{\vec{w} \in \mathbb{F}_q^n \setminus \mathsf{span}\langle \vec{e}_n \rangle^\perp \mid \vec{y} \cdot \vec{w} = \pi\}$, 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 $(\vec{y}, \vec{v}) \in \left(\mathbb{F}_q^n \setminus \mathsf{span}\langle \vec{e}_n \rangle\right) \times \left(\mathbb{F}_q^n \setminus \mathsf{span}\langle \vec{e}_n \rangle^\perp\right)$, if U and Z are generated as $U \overset{\mathsf{U}}{\leftarrow} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q), Z := (U^{-1})^{\mathrm{T}}$, then $\vec{v}Z$ is uniformly distributed in $W_{\vec{y},(\vec{y}\cdot\vec{v})}$.

Proof. Let $\begin{pmatrix} 1 & & & u'_1 \\ & \ddots & & \vdots \\ & & 1 & u'_{n-1} \\ & & & u'_n \end{pmatrix} := U,$

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ -(u'_n)^{-1}u'_1 & \ldots & -(u'_n)^{-1}u'_{n-1} & (u'_n)^{-1} \end{pmatrix} := (U^{-1})^{\mathrm{T}} := Z,$$

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

$$\begin{aligned} &\vec{w} := \vec{v}Z = (v_1 - u'_1(u'_n)^{-1}v_n, \ldots, v_{n-1} - u'_{n-1}(u'_n)^{-1}v_n, (u'_n)^{-1}v_n) \\ &= (u'_n)^{-1}v_n\left(\left(u'_n(v_1v_n^{-1}) - u'_1\right), \ldots, \left(u'_n(v_{n-1}v_n^{-1}) - u'_{n-1}\right), 1\right) \\ &= (u'_n)^{-1}v_n \cdot (\widetilde{u}_1, \ldots, \widetilde{u}_{n-1}, 1), \end{aligned}$$

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

$$\vec{y} \cdot \vec{v} = (u'_n)^{-1}\, v_n \left(\textstyle\sum_{j=1}^{n-1} y_j\widetilde{u}_j + y_n\right) = \vec{y} \cdot \vec{w}. \qquad (\mathrm{A}\cdot 2)$$

Case that $\boldsymbol{\vec{y} \cdot \vec{v} \neq 0}$: Since $\vec{y} \cdot \vec{v} \neq 0$, $\vec{u}'$ can be generated as: $(\widetilde{u}_1, \ldots, \widetilde{u}_{n-1}) \overset{\mathsf{U}}{\leftarrow} \{(\widetilde{u}_j)_{j=1,\ldots,n-1} \in \mathbb{F}_q^{n-1} \mid \sum_{j=1}^{n-1} y_j\widetilde{u}_j + y_n \neq 0\}$, $u'_n := v_n(\sum_{j=1}^{n-1} y_j\widetilde{u}_j + y_n)/(\vec{y} \cdot \vec{v})$, and $u'_j := u'_n(v_jv_n^{-1}) - \widetilde{u}_j$ 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 $(\widetilde{u}_1, .., \widetilde{u}_{n-1}) \overset{\mathsf{U}}{\leftarrow} \{(\widetilde{u}_j)_{j=1,..,n-1} \in \mathbb{F}_q^{n-1} \mid \sum_{j=1}^{n-1} y_j\widetilde{u}_j + y_n \neq 0\}$ 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. (A·2) 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 $j = 1, .., n-1$.

Since $(\widetilde{u}_1, .., \widetilde{u}_{n-1}) \xleftarrow{\mathsf{U}} \{(\widetilde{u}_j)_{j=1,..,n-1} \in \mathbb{F}_q^{n-1} \mid \sum_{j=1}^{n-1} y_j \widetilde{u}_j + y_n = 0\}$ 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 $W_{\vec{y},0}$. □

Appendix B: Proofs of Lemmas in Sect. 6.3

B.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 [3]. □

B.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, $\mathsf{Adv}_{\mathcal{C}}^{\mathsf{P2}}(\lambda) \leq \mathsf{Adv}_{\mathcal{F}_1}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_2}^{\mathsf{DLIN}}(\lambda) + 10/q$.

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 $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \boldsymbol{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}_1^*, \{\boldsymbol{h}_{\beta,i}^*, \boldsymbol{e}_i\}_{i=1,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\beta}^{\mathsf{BP1}}(1^{\lambda}, n)$, where

$$\mathcal{G}_{\beta}^{\mathsf{BP1}}(1^{\lambda}, n) : (\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*,$$

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

$\widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, .., \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,3n+1}, .., \boldsymbol{b}_{1,6n})$ is calculated as in Eq. (5) from $\{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\ldots,6;l=1,\ldots,n}$,

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

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

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

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

for $\beta \xleftarrow{\mathsf{U}} \{0, 1\}$. For a probabilistic adversary $\mathcal{D}$, the advantage of $\mathcal{D}$ for Basic Problem 1, $\mathsf{Adv}_{\mathcal{D}}^{\mathsf{BP1}}(\lambda)$, 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, $\mathsf{Adv}_{\mathcal{C}}^{\mathsf{P2}}(\lambda) \leq \mathsf{Adv}_{\mathcal{D}_1}^{\mathsf{BP1}}(\lambda) + \mathsf{Adv}_{\mathcal{D}_2}^{\mathsf{BP1}}(\lambda)$.

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

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., $\mathsf{Adv}_{\mathcal{C}}^{\mathsf{P2}}(\lambda) = \left|\mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{C}}^{0}(\lambda) \rightarrow 1\right] - \mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{C}}^{3}(\lambda) \rightarrow 1\right]\right|$. Therefore, from Lemmas 27–29, we obtain Lemma 25.

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

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

Based on Experiment 0, we define Experiments 0–3 below. In Experiment 0, a part framed by a box indicates coefficients to be changed in a subsequent experiment. In the other experiments, a part framed by a box indicates coefficients which were changed in an experiment from the previous one.

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

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

where all variables are generated as in Basic Problem 3.

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

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

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

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

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

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

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

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

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 $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \widehat{\mathbb{B}}_1, \mathbb{B}^*_1,\ \{\boldsymbol{h}^*_{\beta,i}\}_{i=1,\dots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{BP2}}_{\beta}(1^\lambda, n)$, where

$$\begin{aligned}
&\mathcal{G}^{\mathsf{BP2}}_{\beta}(1^\lambda, n) : (\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0,\\
&\qquad \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \mathbb{B}^*_1) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{KP\text{-}ABE}}_{\mathsf{ob}}(1^\lambda, 6, n),\\
&\widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, .., \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,3n+1}, .., \boldsymbol{b}_{1,6n}) \text{ is calculated as in}\\
&\text{Eq. (5) from } \{B_{i,j}, B'_{i,j,l}\}_{i,j=1,\dots,6;l=1,\dots,n}, \quad \theta, \psi \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
&\text{for } i = 1, \dots, n; \quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \ \ \vec{\delta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^n,\\
&\boldsymbol{h}^*_{0,i} := (\ \overbrace{0^n,}^{n}\ \ \overbrace{0^{2n},}^{2n}\ \ \overbrace{\psi\vec{e}_i,\ \ \vec{\delta}_i,}^{2n}\ \ \overbrace{0^n}^{n}\ )_{\mathbb{B}^*_1}\\
&\boldsymbol{h}^*_{1,i} := (\ 0^n,\ \ \theta\vec{e}_i,\ \ 0^n,\ \ \psi\vec{e}_i,\ \ \vec{\delta}_i,\ \ 0^n\ )_{\mathbb{B}^*_1}\\
&\text{return } (\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \widehat{\mathbb{B}}_1, \mathbb{B}^*_1, \{\boldsymbol{h}^*_{\beta,i}\}_{i=1,\dots,n}),
\end{aligned}$$

for $\beta \xleftarrow{\mathsf{U}} \{0, 1\}$. For a probabilistic adversary $\mathcal{E}$, the advantage of $\mathcal{E}$ for Basic Problem 2, $\mathsf{Adv}^{\mathsf{BP2}}_{\mathcal{E}}(\lambda)$, 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, $\mathsf{Adv}^{\mathsf{BP1}}_{\mathcal{D}}(\lambda) \ \le \mathsf{Adv}^{\mathsf{BP2}}_{\mathcal{E}}(\lambda)$.

Proof. Given a BP2 instance $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \widehat{\mathbb{B}}_1, \mathbb{B}^*_1, \{\boldsymbol{h}^*_{\beta,i}\}_{i=1,\dots,n})$, $\mathcal{E}$ 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 $i = 1, \dots, n$ and $\widehat{\mathbb{B}}'_1 := (\boldsymbol{b}_{1,1}, \dots, \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,3n+1}, \dots, \boldsymbol{b}_{1,6n})$.

$\mathcal{E}$ defines new dual orthonormal bases $\mathbb{D}_1 := (\boldsymbol{b}_{1,1}, \dots, \boldsymbol{b}_{1,2n}, \boldsymbol{d}_{1,2n+1}, \dots, \boldsymbol{d}_{1,3n}, \boldsymbol{b}_{1,3n+1}, \dots,\ \ \boldsymbol{b}_{1,6n})$ and $\mathbb{D}^*_1 := (\boldsymbol{b}^*_{1,1}, \dots, \boldsymbol{b}^*_{1,n}, \boldsymbol{d}^*_{1,n+1}, \dots, \boldsymbol{d}^*_{1,2n}, \boldsymbol{b}^*_{1,2n+1}, \dots, \boldsymbol{b}^*_{1,6n})$, 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 $i = 1, \dots, n$. We note that $\mathbb{D}_1$ is compatible with subbasis $\widehat{\mathbb{B}}'_1$. $\mathcal{E}$ then gives $\varrho := (\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \boldsymbol{e}_0, \widehat{\mathbb{B}}'_1, \mathbb{D}^*_1, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i\}_{i=1,\dots,n})$ 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

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

Therefore, when $\beta = 0$ (resp. $\beta = 1$), the distribution of ϱ is exactly same as that of instances from $\mathcal{G}^{\mathsf{BP1}}_0$ (resp. $\mathcal{G}^{\mathsf{BP1}}_1$). 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, $\mathsf{Adv}^{\mathsf{BP2}}_{\mathcal{E}}(\lambda) \ \le \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}}(\lambda) + 5/q$.

Lemma 31 is proven in a similar manner to Lemma 4 in the full version of [36]. □

B.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, $|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{C}_1}(\lambda)$.

Lemma 7 is proven in a similar manner to Lemma 4 in [3]. 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, $|\mathsf{Adv}^{(2\text{-}(j-1)\text{-}2)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}j\text{-}1)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{C}_{2\text{-}j}}(\lambda)$, 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. C_2 is given an index j and a Problem 2 instance, $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \boldsymbol{f}_0^*, \boldsymbol{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}_1^*, \{\boldsymbol{f}_i^*\}_{i=1,\dots,2n}, \{\boldsymbol{h}_{\beta,i}^*, \boldsymbol{e}_i\}_{i=1,\dots,n})$.
2. C_2 plays a role of the challenger in the security game against adversary $\mathcal{A}$.
3. 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 $\widehat{\mathbb{B}}_1' := (\boldsymbol{b}_{1,1}, \dots, \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,5n+1}, \dots, \boldsymbol{b}_{1,6n})$, that are obtained from the Problem 2 instance.
4. Then, C_2 (or challenger) obtains challenge attributes Γ with $\Gamma := \{x_1, \dots, x_{n'}\}$, and C_2 calculates $\vec{y} := (y_1, \dots, y_n)$ such that $\sum_{i=0}^{n-1} y_{n-i} z^i = z^{n-1-n'} \cdot \prod_{i=1}^{n'} (z - x_i)$. 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 $\kappa = 1, \dots, j-1$.
5. For $h = 1, \dots, \nu$, when the h-th key query is issued for access structure $\mathbb{S}_h := (M_h, \rho_h)$, C_2 generates $\vec{f}_h, \vec{g}_h \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\mathrm{r}}$, $(s_{h,1}, \dots, s_{h,\ell})^{\mathrm{T}} := M_h \cdot \vec{f}_h^{\mathrm{T}}$, $(r_{h,1}, \dots, r_{h,\ell})^{\mathrm{T}} := M_h \cdot \vec{g}_h^{\mathrm{T}}$, $s_{h,0} := \vec{1} \cdot \vec{f}_h^{\mathrm{T}}$, $r_{h,0} := \vec{1} \cdot \vec{g}_h^{\mathrm{T}}$, and answers as follows: C_2 calculates $\boldsymbol{k}_0^*$ as given in Eq. (8) using $\mathbb{B}_0^*$ of the Problem 2 instance and $s_{h,0}, r_{h,0}$ above, and the i-th component,
$$\boldsymbol{k}_{h,i}^* := \boldsymbol{k}_{h,i}^{*\,\mathsf{norm}} + \sum_{\iota=1}^{n} p_{h,i,\iota} \left(\xi_{h,i,j+1} \boldsymbol{f}_\iota^* + \sum_{\kappa=1}^{j-1} \xi_{h,i,\kappa} \sum_{l=1}^{n} \chi_{\kappa,\iota,l} \boldsymbol{f}_{n+l}^* + \xi_{h,i,j} \boldsymbol{h}_{\beta,\iota}^* \right),$$
where $\boldsymbol{k}_{h,i}^{*\,\mathsf{norm}}$ is a normal form given in Eq. (6) that is computed using $\mathbb{B}_1^*$ of the Problem 2 instance and $s_{h,i}$ above, $\vec{p}_{h,i} := (p_{h,i,1}, \dots, p_{h,i,n})$ 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 $(\xi_{h,i,\kappa})_{\kappa=1,\dots,j+1} \xleftarrow{\mathsf{U}} \{(\xi_\kappa)_{\kappa=1,\dots,j+1} \in \mathbb{F}_q^{j+1} \mid \sum_{\kappa=1}^{j+1} \xi_\kappa = 1 \ \wedge \ \xi_{n+1} = 0 \text{ if } j = n\}$. C_2 sends key $\mathsf{sk}_{\mathbb{S}_h} := (\mathbb{S}_h, \{\boldsymbol{k}_{h,i}^*\}_{i=0,\dots,\ell})$ to $\mathcal{A}$.
6. When C_2 receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ from $\mathcal{A}$, C_2 selects (challenge) bit $b \xleftarrow{\mathsf{U}} \{0,1\}$. C_2 computes the challenge ciphertext $(\boldsymbol{c}_0, \boldsymbol{c}_1, c_T)$ such that
$$\boldsymbol{c}_0 := \omega \boldsymbol{b}_{0,1} + \boldsymbol{e}_0 + \zeta \boldsymbol{b}_{0,3} + \varphi_0 \boldsymbol{b}_{0,5},$$
$$\boldsymbol{c}_1 := \textstyle\sum_{\iota=1}^{n} y_\iota (\omega \boldsymbol{b}_{1,\iota} + \boldsymbol{e}_\iota + \varphi_1 \boldsymbol{b}_{1,5n+\iota}), \quad c_T := g_T^\zeta m^{(b)},$$
where $\omega, \zeta, \varphi_0, \varphi_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and $(\boldsymbol{e}_0, \{\boldsymbol{e}_\iota\}_{\iota=1,\dots,n})$, $\mathbb{B}_0, \widehat{\mathbb{B}}_1$ are a part of the Problem 2 instance.
7. When a key query is issued by $\mathcal{A}$ after the encryption query, C_2 executes the same procedure as that of step 5.
8. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, C_2 outputs $\beta' := 1$. Otherwise, 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 $(\mathsf{param}_n, \{\widehat{\mathbb{B}}_t\}_{t=0,1}, \{\mathsf{sk}_{\mathbb{S}}^{(j)*}\}_{j=1,\dots,\nu}, \mathsf{ct}_\Gamma)$ in Games 2-j-1 and 2-j-2 are equivalent. For that purpose, we define new subbases $\boldsymbol{d}_{1,2n+1}, \dots, \boldsymbol{d}_{1,3n}$ and $\boldsymbol{d}_{1,2n+1}^*, \dots, \boldsymbol{d}_{1,3n}^*$ 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 $(\boldsymbol{d}_{1,2n+1}, \dots, \boldsymbol{d}_{1,3n})^{\mathrm{T}} := Z \cdot (\boldsymbol{b}_{1,2n+1}, \dots, \boldsymbol{b}_{1,3n})^{\mathrm{T}}$ and $(\boldsymbol{d}_{1,2n+1}^*, \dots, \boldsymbol{d}_{1,3n}^*)^{\mathrm{T}} := U \cdot (\boldsymbol{b}_{1,2n+1}^*, \dots, \boldsymbol{b}_{1,3n}^*)^{\mathrm{T}}$ and
$$\mathbb{D}_1 := (\boldsymbol{b}_{1,1}, \dots, \boldsymbol{b}_{1,2n}, \boldsymbol{d}_{1,2n+1}, \dots, \boldsymbol{d}_{1,3n}, \boldsymbol{b}_{1,3n+1}, \dots, \boldsymbol{b}_{1,6n}),$$
$$\mathbb{D}_1^* := (\boldsymbol{b}_{1,1}^*, \dots, \boldsymbol{b}_{1,2n}^*, \boldsymbol{d}_{1,2n+1}^*, \dots, \boldsymbol{d}_{1,3n}^*, \boldsymbol{b}_{1,3n+1}^*, \dots, \boldsymbol{b}_{1,6n}^*).$$

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.

if $(\rho_h(i) = v_{h,i} \wedge v_{h,i} \notin \Gamma) \vee (\rho_h(i) = \neg v_{h,i} \wedge v_{h,i} \in \Gamma)$,
$$\begin{aligned}\boldsymbol{k}_{h,i}^* &= (\overbrace{\cdots}^{2n}, \overbrace{\vec{p}_{h,i} \cdot (\sum_{\kappa=1}^{j-1} \xi_{h,i,\kappa} Z_\kappa + \xi_{h,i,j} I_n),}^{n} \overbrace{\cdots}^{3n})_{\mathbb{B}_1^*} \\ &= (\ \cdots, \ \vec{p}_{h,i} \cdot (\textstyle\sum_{\kappa=1}^{j-1} \xi_{h,i,\kappa} Z_\kappa + \xi_{h,i,j} I_n) Z, \ \cdots \ )_{\mathbb{D}_1^*}, \\ &= (\ \cdots, \ \vec{p}_{h,i} \cdot (\textstyle\sum_{\kappa=1}^{j} \xi_{h,i,\kappa} \widetilde{Z}_\kappa), \ \cdots \ )_{\mathbb{D}_1^*},\end{aligned}$$
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 $\rho_h(i) = \neg v_{h,i}$, $(\xi_{h,i,\kappa})_{\kappa=1,\dots,j+1} \xleftarrow{\mathsf{U}} \{(\xi_\kappa)_{\kappa=1,\dots,j+1} \in \mathbb{F}_q^{j+1} \mid \sum_{\kappa=1}^{j+1} \xi_\kappa = 1 \ \wedge \ \xi_{n+1} = 0 \text{ if } j = n\}$, and $\widetilde{Z}_\kappa := Z_\kappa Z$ for $\kappa = 1, \dots, j-1$, $\widetilde{Z}_j := Z$ 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 $(\mathsf{param}_n, \{\widehat{\mathbb{D}}_t\}_{t=0,1}, \{\mathsf{sk}_{\mathbb{S}}^{(j)*}\}_{j=1,\dots,\nu}, \mathsf{ct}_\Gamma)$ 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, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}n\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)| \le 3\nu\hat{\ell}/q$, 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.

if $(\rho_h(i) = v_{h,i} \wedge v_{h,i} \notin \Gamma) \vee (\rho_h(i) = \neg v_{h,i} \wedge v_{h,i} \in \Gamma)$,
$$\boldsymbol{k}_{h,i}^* = (\overbrace{\cdots}^{2n}, \overbrace{\vec{p}_{h,i} \cdot (\sum_{\kappa=1}^{n} \xi_{h,i,\kappa} Z_\kappa),}^{n} \overbrace{\cdots}^{3n})_{\mathbb{B}_1^*},$$
$$\text{otherwise,} \quad \boldsymbol{k}_{h,i}^* = (\overbrace{\cdots}^{2n}, \overbrace{0^n,}^{n} \overbrace{\cdots}^{3n})_{\mathbb{B}_1^*},$$
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 $\rho_h(i) = \neg v_{h,i}$, $(\xi_{h,i,\kappa})_{\kappa=1,\dots,n} \xleftarrow{\mathsf{U}} \{(\xi_\kappa)_{\kappa=1,\dots,n} \in \mathbb{F}_q^n \mid \sum_{\kappa=1}^n \xi_\kappa = 1\}$, and $Z_\kappa \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n,\mathbb{F}_q)^{\mathrm{T}}$ for $\kappa = 1,\dots,n$.

We note that $\{\widetilde{Z}_\kappa := Z_\kappa - Z_1\}_{\kappa=2,\dots,n}$ (given by $\{\vec{u}'_\kappa := (u'_{\kappa,1},\dots,u'_{\kappa,n}) \in \mathbb{F}_q^n\}_{\kappa=2,\dots,n}$) are linearly independent except that the matrix $(\vec{u}'_\kappa)_{\kappa=2,\dots,n} \in \mathbb{F}_q^{(n-1)\times n}$ does not have maximal rank $n-1$, i.e., except for probability $1/q$. Therefore, from Lemma 2, since $(\xi_{h,i,\kappa})_{\kappa=1,\dots,n}$ 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

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

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

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

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. (13). The corresponding shares $r_{h,i}$ are information-theoretically hidden from the adversary $\mathcal{A}$. Also, $r_{h,i}$ obtained from the other indices i for the h-th key 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. (13). This completes the proof of Lemma 10. □

Lemma 11 For any adversary $\mathcal{A}$, for any security parameter λ, $|\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda)| \le 1/q$.

Proof. Lemma 11 is proven in a similar manner to Lemma 7 in [3]. For completeness, we give the proof below.

To prove Lemma 11, we will show distribution $(\mathsf{param}_n, \{\widehat{\mathbb{B}}_t\}_{t=0,1}, \{\mathsf{sk}_{\mathbb{S}_h}\}_{h=1,\dots,\nu}, \mathsf{ct}_\Gamma)$ in Game 3 and that in Game 4 are equivalent, where $\mathsf{sk}_{\mathbb{S}_h}$ is the answer to the h-th key query, and ct_Γ is the challenge ciphertext. By definition, we only need to consider elements on $\mathbb{V}_0$ or $\mathbb{V}_0^*$. We define new bases $\mathbb{D}_0$ of $\mathbb{V}_0$ and $\mathbb{D}_0^*$ of $\mathbb{V}_0^*$ as follows: We generate $\theta \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and set $\boldsymbol{d}_{0,2} := (0,1,-\theta,0,0)_{\mathbb{B}} = \boldsymbol{b}_{0,2} - \theta\boldsymbol{b}_{0,3}$, $\boldsymbol{d}^*_{0,3} := (0,\theta,1,0,0)_{\mathbb{B}} = \boldsymbol{b}^*_{0,3} + \theta\boldsymbol{b}^*_{0,2}$. We set $\mathbb{D}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{d}_{0,2}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,4}, \boldsymbol{b}_{0,5})$, $\mathbb{D}_0^* := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,2}, \boldsymbol{d}^*_{0,3}, \boldsymbol{b}^*_{0,4}, \boldsymbol{b}^*_{0,5})$. We then easily verify that $\mathbb{D}_0$ and $\mathbb{D}_0^*$ are dual orthonormal, and are distributed the same as the original bases, $\mathbb{B}_0$ and $\mathbb{B}_0^*$. The $\mathbb{V}_0$ components $(\{\boldsymbol{k}^*_{h,0}\}_{h=1,\dots,\nu}, \boldsymbol{c}_0)$ in keys and challenge ciphertext $(\{\mathsf{sk}_{\mathbb{S}_h}\}_{h=1,\dots,\nu}, \mathsf{ct}_\Gamma)$ in Game 3 are expressed over bases $\mathbb{B}_0$ and $\mathbb{B}_0^*$ as $\boldsymbol{k}^*_{0,h} = (-s_{0,h}, w_{0,h}, 1, \eta_{h,0}, 0)_{\mathbb{B}_0^*}$, $\boldsymbol{c}_0 = (\omega,\tau,\zeta,0,\varphi_0)_{\mathbb{B}_0}$. Then, $\boldsymbol{k}^*_{0,h} = (-s_{0,h}, w_{0,h}, 1, \eta_{0,h}, 0)_{\mathbb{B}_0^*} = (-s_{0,h}, w_{0,h}+\theta, 1, \eta_{0,h}, 0)_{\mathbb{D}_0^*} = (-s_{0,h}, \vartheta_{0,h}, 1, \eta_{0,h}, 0)_{\mathbb{D}_0^*}$, where $\vartheta_{0,h} := w_{0,h} + \theta$ which are uniformly, independently distributed since $w_{0,h} \xleftarrow{\mathsf{U}} \mathbb{F}_q$. $\boldsymbol{c}_0 = (\omega,\tau,\zeta,0,\varphi_0)_{\mathbb{B}_0} = (\omega,\tau,\zeta+\tau\theta,0,\varphi_0)_{\mathbb{D}_0} = (\omega,\tau,\zeta',0,\varphi_0)_{\mathbb{D}_0}$ where $\zeta' := \zeta + \tau\theta$ which is uniformly, independently distributed since $\theta \xleftarrow{\mathsf{U}} \mathbb{F}_q$.

In the light of the adversary's view, both $(\mathbb{B}_0, \mathbb{B}_0^*)$ and $(\mathbb{D}_0, \mathbb{D}_0^*)$ are consistent with public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_n, \{\widehat{\mathbb{B}}_t\}_{t=0,1})$. Therefore, $\{\mathsf{sk}_{\mathbb{S}_h}\}_{h=1,\dots,\nu}$ and ct_Γ can be expressed as keys and ciphertext in two ways, in Game 3 over bases $(\mathbb{B}_0, \mathbb{B}_0^*)$ and in Game 4 over bases $(\mathbb{D}_0, \mathbb{D}_0^*)$. Thus, Game 3 can be conceptually changed to Game 4 if $\tau \neq 0$, i.e., except with probability $1/q$. □

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, $\mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda) = 0$. □

Appendix C: Proofs of Lemmas in Sect. 6.5

C.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, $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) \le \sum_{j=0}^n \sum_{\iota=1}^2 \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{j\text{-}\iota}}(\lambda) + (10n+10)/q$, 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

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

for $j = 1,\dots,n$; $i = 1,\dots,n$;

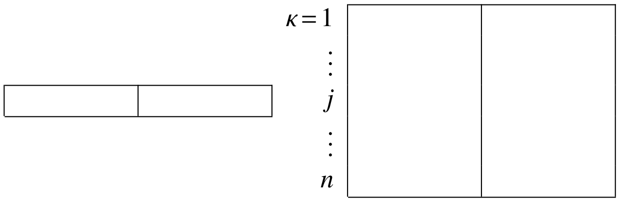
$$\vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n,\quad \vec{\delta}_{j,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n},$$

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

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:

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

for $j = 1, \ldots, n$; $i = 1, \ldots, n$;

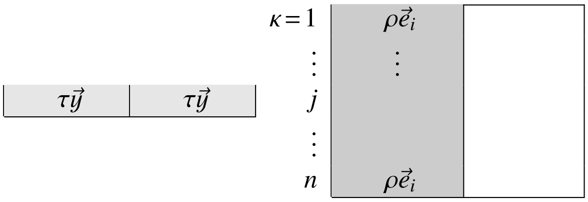
$$\vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \quad \vec{\delta}_{j,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n},$$

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

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

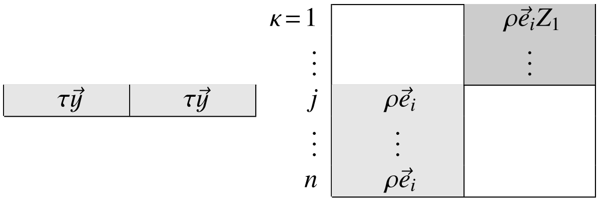
Coefficients of the hidden part of $\boldsymbol{e}_1$ in Experiment 1

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



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

Coefficients of the hidden part of $\boldsymbol{h}^*_{\kappa,i}$ in Exp. 2-(j−1)-2



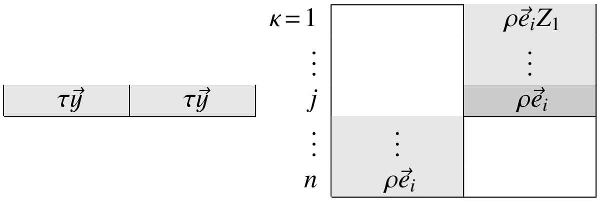
Experiment 2-*j*-1 ($\mathsf{Exp}^{2\text{-}j\text{-}1}_{\mathcal{B}}, \boldsymbol{j = 1, \ldots, n}$) **:** Experiment 2-0-2 is Experiment 2-0. Experiment 2-j-1 is the same as Experiment 2-(j − 1)-2 except the j-th component $\boldsymbol{h}^*_{j,i}$ are:

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

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

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

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



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

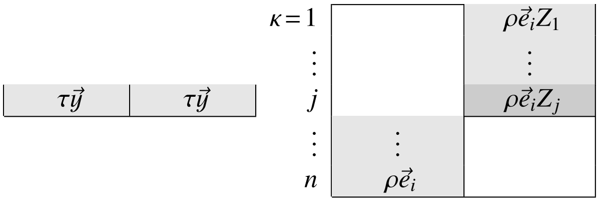
$$\text{for } i = 1, \ldots, n; \quad U_j \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n, \mathbb{F}_q), \ \ Z_j := (U_j^{-1})^{\mathrm{T}},$$

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

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

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

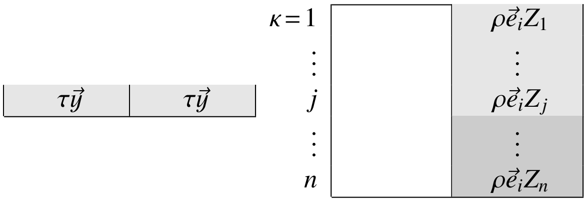
Coefficients of the hidden part of $\boldsymbol{h}^*_{\kappa,i}$ in Exp. 2-j-2



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 Exp. 2-n-2

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



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 $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) = |\mathsf{Pr}[\mathsf{Exp}^0_{\mathcal{B}}(\lambda) \to 1] - \mathsf{Pr}[\mathsf{Exp}^{2\text{-}n\text{-}2}_{\mathcal{B}}(\lambda) \to 1]| \leq \mathsf{Adv}^{\mathsf{P1}}_{C_0}(\lambda) + \sum_{j=1}^n \mathsf{Adv}^{\mathsf{P2}}_{C_j}(\lambda) \leq \sum_{j=0}^n \sum_{\iota=1}^2 \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{j,\iota}}(\lambda) + (10n + 10)/q$. This completes the proof of Lemma 14. □

Lemma 32: For any adversary $\mathcal{B}$, there exists a probabilistic machine C_0, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $|\mathsf{Pr}[\mathsf{Exp}^1_{\mathcal{B}}(\lambda) \to 1] - \mathsf{Pr}[\mathsf{Exp}^0_{\mathcal{B}}(\lambda) \to 1]| \leq \mathsf{Adv}^{\mathsf{P1}}_{C_0}(\lambda)$.

Proof. C_0 is given a P1 instance $(\mathsf{param}_n, \{\mathbb{B}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,1}, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_{\beta,i}\}_{i=0,\dots,n})$ and a target vector $\vec{y}$. C_0 then calculates $(\mathsf{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,1})$ in Experiment 0, and calculates $\boldsymbol{e}'_0 := \boldsymbol{e}_{\beta,0}, \boldsymbol{e}'_1 := \sum_{\iota=1}^n y_\iota \boldsymbol{e}_{\beta,\iota}, \boldsymbol{h}'^*_0 := \boldsymbol{h}^*_{\beta,0}, \{\boldsymbol{h}'^*_{j,i} := \boldsymbol{h}^*_{\beta,i} + \sum_{\iota=1}^n \delta_{j,i,\iota}\boldsymbol{b}_{1,3n+\iota}\}_{j=1,\dots,n;\, i=1,\dots,n}$ with $\delta_{j,i,\iota} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, sends $\varrho := (\mathsf{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,1}, \boldsymbol{h}'^*_0, \boldsymbol{e}'_0, \{\boldsymbol{h}'^*_{j,i}\}_{j=1,\dots,n;\, i=1,\dots,n}, \boldsymbol{e}'_1)$ to $\mathcal{B}$. 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 C, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $|\Pr[\mathsf{Exp}^{2\text{-}(j-1)\text{-}2}_{\mathcal{B}}(\lambda) \to 1] - \Pr[\mathsf{Exp}^{2\text{-}j\text{-}1}_{\mathcal{B}}(\lambda) \to 1]| \le \mathsf{Adv}^{\mathsf{P2}}_{C_j}(\lambda)$, where $C_j(\cdot) := C(j,\cdot)$ $(j \ge 1)$.

Proof. C is given a P2 instance $(\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}^*_0, \boldsymbol{f}^*_0, \boldsymbol{e}_0, \widehat{\mathbb{B}}_1, \mathbb{B}^*_1, \{\boldsymbol{f}^*_i\}_{i=1,\dots,2n}, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i\}_{i=1,\dots,n})$, a target vector $\vec{y}$ and an index j. 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

if $\kappa < j$; for $i = 1,\dots,n$,

$$\boldsymbol{h}'^*_{\kappa,i} := \delta\boldsymbol{b}^*_{1,i} + \textstyle\sum_{\iota=1}^n(\chi_{\kappa,i,\iota}\boldsymbol{f}^*_{n+\iota} + \delta_{\kappa,i,\iota}\boldsymbol{b}^*_{1,3n+\iota}) \ \text{ where}$$

$$Z_\kappa \xleftarrow{\mathsf{U}} \mathcal{H}_{\vec{y}}(n,\mathbb{F}_q)^{\mathrm{T}},\ (\chi_{\kappa,i,1},\dots,\chi_{\kappa,i,n}) := \vec{e}_i Z_\kappa,\ \delta_{\kappa,i,\iota} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

if $\kappa = j$; for $i = 1,\dots,n$,

$$\boldsymbol{h}'^*_{j,i} := \delta\boldsymbol{b}^*_{1,i} + \boldsymbol{h}^*_{\beta,i} + \textstyle\sum_{\iota=1}^n \delta_{j,i,\iota}\boldsymbol{b}^*_{1,3n+\iota} \text{ where } \delta_{j,i,\iota} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

if $\kappa > j$; for $i = 1,\dots,n$,

$$\boldsymbol{h}'^*_{\kappa,i} := \delta\boldsymbol{b}^*_{1,i} + \boldsymbol{f}^*_i + \textstyle\sum_{\iota=1}^n \delta_{\kappa,i,\iota}\boldsymbol{b}^*_{1,3n+\iota} \text{ where } \delta_{\kappa,i,\iota} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

and sends $\varrho := (\mathsf{param}_n, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,1}, \boldsymbol{h}'^*_0, \boldsymbol{e}'_0, \{\boldsymbol{h}'^*_{j,i}\}^{j=1,\dots,n}_{i=1,\dots,n}, \boldsymbol{e}'_1)$ to $\mathcal{B}$. 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, $\Pr[\mathsf{Exp}^{2\text{-}j\text{-}1}_{\mathcal{B}}(\lambda) \to 1] = \Pr[\mathsf{Exp}^{2\text{-}j\text{-}2}_{\mathcal{B}}(\lambda) \to 1]$.

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

For the target vector $\vec{y} := (y_1,\dots,y_n)$, 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 $(\boldsymbol{d}_{1,2n+1},\dots,\boldsymbol{d}_{1,3n})^{\mathrm{T}} := Z \cdot (\boldsymbol{b}_{1,2n+1},\dots,\boldsymbol{b}_{1,3n})^{\mathrm{T}}$ and $(\boldsymbol{d}^*_{1,2n+1},\dots,\boldsymbol{d}^*_{1,3n})^{\mathrm{T}} := U \cdot (\boldsymbol{b}^*_{1,2n+1},\dots,\boldsymbol{b}^*_{1,3n})^{\mathrm{T}}$ and

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

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.

if $\kappa < j$; for $i = 1,\dots,n$;

$$\begin{aligned}
\boldsymbol{h}^*_{\kappa,i} &= (\ \overbrace{\delta\vec{e}_i,}^{n}\quad \overbrace{0^n,\quad \rho\vec{e}_i \cdot Z_\kappa,}^{2n}\quad \overbrace{\vec{\delta}_{\kappa,i}, 0^n}^{3n})_{\mathbb{B}^*_1}\\
&= (\ \delta\vec{e}_i,\quad 0^n,\ \rho\vec{e}_i \cdot Z_\kappa Z,\quad \vec{\delta}_{\kappa,i}, 0^n)_{\mathbb{D}^*_1},
\end{aligned}$$

if $\kappa = j$; for $i = 1,\dots,n$;

$$\begin{aligned}
\boldsymbol{h}^*_{j,i} &= (\ \delta\vec{e}_i,\quad 0^n,\quad \rho\vec{e}_i,\quad \vec{\delta}_{j,i}, 0^n)_{\mathbb{B}^*_1}\\
&= (\ \delta\vec{e}_i,\quad 0^n,\quad \rho\vec{e}_i \cdot Z,\quad \vec{\delta}_{j,i}, 0^n)_{\mathbb{D}^*_1},
\end{aligned}$$

if $\kappa > j$; for $i = 1,\dots,n$;

$$\begin{aligned}
\boldsymbol{h}^*_{\kappa,i} &= (\ \delta\vec{e}_i,\quad \rho\vec{e}_i,\quad 0^n,\quad \vec{\delta}_{\kappa,i}, 0^n)_{\mathbb{B}^*_1}\\
&= (\ \delta\vec{e}_i,\quad \rho\vec{e}_i,\quad 0^n,\quad \vec{\delta}_{\kappa,i}, 0^n)_{\mathbb{D}^*_1},
\end{aligned}$$

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

C.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, $|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) + 3\nu\hat{\ell}/q$, 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, $(\mathsf{param}_n, \{\mathbb{B}_\iota, \mathbb{B}^*_\iota\}_{\iota=0,1})$.
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 $\widehat{\mathbb{B}}'_1 := (\boldsymbol{b}_{1,1},\dots,\boldsymbol{b}_{1,n},\boldsymbol{b}_{1,5n+1},\dots,\boldsymbol{b}_{1,6n})$, that are obtained from the Problem 3 instance.
4. When $\mathcal{B}$ (or challenger) obtains challenge attributes Γ with $\Gamma := \{x_1,\dots,x_{n'}\}$ in the first step of the game, $\mathcal{B}$ calculates $\vec{y} := (y_1,\dots,y_n)$ such that $\sum_{j=0}^{n-1} y_{n-j}z^j = z^{n-1-n'} \cdot \prod_{j=1}^{n'}(z - x_j)$, and 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, $(\boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{h}^*_{\beta,j,i}\}_{j=1,\dots,n;\, i=1,\dots,n}, \boldsymbol{e}_{\beta,1})$.
5. For $h = 1,\dots,\nu$, when the h-th key query is issued for access structure $\mathbb{S}_h := (M_h, \rho_h)$, $\mathcal{B}$ generates $\vec{f}_h, \vec{g}_h \xleftarrow{\mathsf{U}} \mathbb{F}^{\mathrm{r}}_q, (s_{h,1},\dots,s_{h,\ell})^{\mathrm{T}} := M_h \cdot \vec{f}^{\mathrm{T}}_h, (r_{h,1},\dots,r_{h,\ell})^{\mathrm{T}} := M_h \cdot \vec{g}^{\mathrm{T}}_h$,

$s_{h,0} := \vec{1} \cdot \vec{f}_h^{\mathrm{T}}, r_{h,0} := \vec{1} \cdot \vec{g}_h^{\mathrm{T}}$, and answers as follows: $\mathcal{B}$ calculates

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

for $i = 1, \ldots, \ell$, where $\boldsymbol{k}_{h,i}^{*\,\mathsf{norm}}$ is a normal form given in Eq. (6) 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 $(\xi_{h,i,j})_{j=1,\ldots,n} \overset{\mathsf{U}}{\leftarrow} \{(\xi_j)_{j=1,\ldots,n} \in \mathbb{F}_q^n \mid \sum_{j=1}^n \xi_j = 1\}$.

6. When $\mathcal{B}$ receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ from $\mathcal{A}$, $\mathcal{B}$ selects (challenge) bit $b \overset{\mathsf{U}}{\leftarrow} \{0, 1\}$. $\mathcal{B}$ 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 $\zeta \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$, 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. □

Appendix D: The Underlying CP-ABE for the Proposed ABS in Sect. 7

D.1 Definitions

Our definition of CP-ABE is the dual form of our KP-ABE given in Definition 5.

Definition 18: (Ciphertext-Policy Attribute-Based Encryption: CP-ABE) A ciphertext-policy attribute-based encryption scheme consists of probabilistic polynomial-time algorithms Setup, KeyGen, Enc and Dec. They are given as follows:

Setup takes as input security parameter 1^λ and a bound on the number of attributes per ciphertext n. It outputs public parameters pk and master secret key sk.

KeyGen takes as input public parameters pk, master secret key sk, and a set of attributes, $\Gamma := \{x_j\}_{1 \le j \le n'}$. It outputs a corresponding secret key sk_Γ.

Enc takes as input public parameters pk, message m in some associated message space msg, and access structure $\mathbb{S} := (M, \rho)$. It outputs a ciphertext $\mathsf{ct}_\mathbb{S}$.

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

The correctness of CP-ABE is standard and similarly defined as that for KP-ABE.

Definition 19 (Non-Adaptive Security [42]): The model for defining the (indistinguishability game-based) non-adaptively payload-hiding security (in [42]) of CP-ABE under chosen plaintext attack is given by the following game:

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

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

Challenge The adversary submits two messages $m^{(0)}, m^{(1)}$ and a challenge access structure, $\mathbb{S}$. provided that no Γ queried to the challenger in Phase 1 is accepted by $\mathbb{S}$. The challenger flips a coin $b \overset{\mathsf{U}}{\leftarrow} \{0, 1\}$, and computes $\mathsf{ct}_\mathbb{S}^{(b)} \overset{\mathsf{R}}{\leftarrow} \mathsf{Enc}(\mathsf{pk}, m^{(b)}, \mathbb{S})$. It gives $\mathsf{ct}_\mathbb{S}^{(b)}$ to the adversary.

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

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

We note that the adversary is not allowed to issue any key query after the challenge phase in the above non-adaptive game.

D.2 Construction and Security

We first give the orthonormal basis generator for the CP-ABE below.

$$\begin{aligned}
&\mathcal{G}_{\mathsf{ob}}^{\mathsf{CP\text{-}ABE}}(1^\lambda, 6, n) : (\mathsf{param}_n, \mathbb{D}_0, \mathbb{D}_0^*, \{D_{i,j}, D'_{i,j,l}\}_{l=1,..,n}^{i,j=1,..,6}, \mathbb{D}_1^*) \\
&\qquad \overset{\mathsf{R}}{\leftarrow} \mathcal{G}_{\mathsf{ob}}^{\mathsf{KP\text{-}ABE}}(1^\lambda, 6, n), \\
&\mathbb{B}_0 := \mathbb{D}_0^*, \ \mathbb{B}_0^* := \mathbb{D}_0, \ \mathbb{B}_1 := \mathbb{D}_1^*, \\
&B_{i,j}^* := D_{i,j}, B'^{\,*}_{i,j,l} := D'_{i,j,l} \text{ for } i, j = 1, \ldots, 6; l = 1, \ldots, n, \\
&\text{return } (\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1, \{B_{i,j}^*, B'^{\,*}_{i,j,l}\}_{l=1,\ldots,n}^{i,j=1,\ldots,6}).
\end{aligned}$$

We give our CP-ABE with constant-size secret keys below. We note that attributes x_j, v_i are in $\mathbb{F}_q^\times$, i.e., nonzero.

$$\begin{aligned}
&\mathsf{Setup}(1^\lambda, \ n) : (\mathsf{param}_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1, \{B_{i,j}^*, B'^{\,*}_{i,j,l}\}_{l=1,\ldots,n}^{i,j=1,\ldots,6}) \\
&\qquad \overset{\mathsf{R}}{\leftarrow} \mathcal{G}_{\mathsf{ob}}^{\mathsf{CP\text{-}ABE}}(1^\lambda, 6, n), \\
&\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}), \widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, .., \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,4n+1}, .., \boldsymbol{b}_{1,6n}), \\
&\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*, \boldsymbol{b}_{0,4}^*), \\
&\widehat{\mathbb{B}}_1^* := (\boldsymbol{b}_{1,1}^*, .., \boldsymbol{b}_{1,n}^*, \boldsymbol{b}_{1,3n+1}^*, .., \boldsymbol{b}_{1,4n}^*) = \{B_{i,j}^*, B'^{\,*}_{i,j,l}\}_{l=1,..,n}^{i=1,4; j=1,..,6}, \\
&\text{return } \mathsf{pk} := (1^\lambda, \mathsf{param}_n, \{\widehat{\mathbb{B}}_t\}_{t=0,1}), \ \mathsf{sk} := \{\widehat{\mathbb{B}}_t^*\}_{t=0,1}.
\end{aligned}$$

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

$\omega, \varphi_0, \varphi_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

$\vec{y} := (y_1, \ldots, y_n)$ s.t. $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \cdot \prod_{j=1}^{n'} (z - x_j)$,

$\boldsymbol{k}_0^* := (\omega, 0, 1, \varphi_0, 0)_{\mathbb{B}_0^*}, L_{1,j}^* := \omega B_{1,j}^* + \varphi_1 B_{4,j}^*$,

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

return $\mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}_0^*, \{L_{1,j}^*, L_{2,j}^*\}_{j=1,\ldots,6})$.

<u>Remark</u> From $\{L_{1,j}^*, L_{2,j}^*\}_{j=1,\ldots,6}$ and $\vec{y}$, $\boldsymbol{k}_1^*$ is defined as

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

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

$\mathsf{Enc}(\mathsf{pk},\ m,\ \mathbb{S} := (M, \rho))$: $\vec{f} \xleftarrow{\mathsf{R}} \mathbb{F}_q^{\mathfrak{r}}$,

$s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$, $\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$,

$\zeta, \eta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\boldsymbol{c}_0 := (-s_0, 0, \zeta, 0, \eta_0)_{\mathbb{B}_0}$,

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

if $\rho(i) = v_i$, $\theta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n}$,

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

if $\rho(i) = \neg v_i$, $\vec{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n}$,

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

$c_T := g_T^{\zeta} m$, return $\mathsf{ct}_{\mathbb{S}} := (\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell, c_T)$.

$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}_0^*, \{L_{1,j}^*, L_{2,j}^*\}_{j=1,\ldots,6}),$

$\mathsf{ct}_{\mathbb{S}} := (\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell, c_T))$:

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

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

$\vec{y} := (y_1, \ldots, y_n)$ s.t. $\sum_{j=0}^{n-1} y_{n-j} z^j = z^{n-1-n'} \cdot \prod_{j=1}^{n'} (z - x_j)$,

$$(C_1, \ldots, C_{6n}) := \sum_{i \in I\ \wedge\ \rho(i) = v_i} \alpha_i \boldsymbol{c}_i + \sum_{i \in I\ \wedge\ \rho(i) = \neg v_i} \frac{\alpha_i}{\vec{v}_i \cdot \vec{y}} \boldsymbol{c}_i,$$

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

$K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \cdot \prod_{j=1}^{6} \left(e(E_j, L_{1,j}^*) \cdot e(C_{jn}, L_{2,j}^*) \right)$,

return $m' := c_T / K$.

Theorem 4: The above CP-ABE scheme is non-adaptively payload-hiding against chosen plaintext attacks under the DLIN assumption.

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,

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{CP\text{-}ABE,NA}}(\lambda) \leq \mathsf{Adv}_{\mathcal{F}_0}^{\mathsf{DLIN}}(\lambda) + \sum_{l=1}^{2} \sum_{h=1}^{\nu_K} (\mathsf{Adv}_{\mathcal{F}_{l\text{-}h\text{-}0}}^{\mathsf{DLIN}}(\lambda) + \sum_{j=1}^{n} \sum_{\iota=1}^{2} \mathsf{Adv}_{\mathcal{F}_{l\text{-}h\text{-}j\text{-}\iota}}^{\mathsf{DLIN}}(\lambda)) + \epsilon, \tag{A·3}$$

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 $l = 1, 2$, ν_K is the maximum number of $\mathcal{A}$'s key queries, and ϵ is a negligible function in λ.

Proof Sketch. Theorem 4 is proven through a part of games for Theorem 3, i.e., Games 0, 1, 2-h-1 and 2-h-2 ($h = 1, \ldots, \nu_K$) in Sect. 7.3.1. The differences between ABS and CP-ABE are that the verification text for ABS corresponds to the challenge ciphertext for CP-ABE, only two spaces $\{\mathbb{V}_t\}_{t=0,1}$ are used in CP-ABE (not three spaces as in the case of ABS), and the dimension of $\mathbb{V}_0$ in CP-ABE is five (not four as in the case of ABS).

In Game 2-ν_K-2, we have secret keys $\boldsymbol{k}_{h,0}^* := (\omega_h, \tau'_h, 1, \varphi_{0,h}, 0)_{\mathbb{B}_0^*}$ for $h = 1, \ldots, \nu_K$ and the challenge ciphertext $\boldsymbol{c}_0 := (-s_0, -r_0, \zeta, 0, \eta_0)_{\mathbb{B}_0}$ where $\tau'_h \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{g} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\mathfrak{r}}, r_0 := \vec{1} \cdot \vec{g}^{\mathrm{T}}$. Therefore, we consider Game 3 for our CP-ABE as:

Game 3 : Same as Game 2-ν_K-2 except that $\boldsymbol{c}_0$ and c_T of the challenge ciphertext are

$$\boldsymbol{c}_0 := (-s_0, -r_0, \boxed{\zeta'}, 0, \eta_0)_{\mathbb{B}_0}, \quad c_T := g_T^{\zeta} m^{(b)},$$

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 2-ν_K-2.

We can prove the following facts as in Lemmas 11 and 12: For any adversary $\mathcal{A}$, for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}\nu_K\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)| \leq 1/q$ and $\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) = 0$. Therefore, we obtain the inequality (A·3). This completes the proof of Theorem 4. □

Appendix E: Proofs of Lemmas in Sect. 7.3.2

E.1 Proof of Lemma 16

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

Proof. Lemma 16 is proven through hierarchical (security) reductions for *sparse DPVS* which are developed in [36]. Lemma 16 is proven in a similar manner to Lemma 4 in the full version of [36], while the size of ciphertexts is small in [36] but the size of keys (and sgnatures) is small here. For completeness, we give the proof of Lemma 16 below. We first define Basic Problem 0 as in Definition 10 in [36].

Definition 20 (Basic Problem 0): Basic Problem 0 is to guess $\beta \in \{0, 1\}$, given $(\mathsf{param}_{\mathsf{BP0}}, \widehat{\mathbb{B}}, \mathbb{B}^*, \boldsymbol{y}_\beta^*, \boldsymbol{f}, \kappa G, \xi G, \delta\xi G) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{BP0}}(1^\lambda)$, where

$$\mathcal{G}_\beta^{\mathsf{BP0}}(1^\lambda) : \quad \mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda),$$

$$X := \begin{pmatrix} \vec{\chi}_1 \\ \vec{\chi}_2 \\ \vec{\chi}_3 \end{pmatrix} := (\chi_{i,j})_{i,j} \xleftarrow{\mathsf{U}} GL(3, \mathbb{F}_q),$$

$$
\begin{aligned}
&(\vartheta_{i,j})_{i,j} := \begin{pmatrix} \vec{\vartheta}_1 \\ \vec{\vartheta}_2 \\ \vec{\vartheta}_3 \end{pmatrix} := (X^{\mathrm{T}})^{-1}, \ \ \kappa, \xi \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\times}, \\
&\boldsymbol{b}_i := \kappa(\chi_{i,1}G, \chi_{i,2}G, \chi_{i,3}G) \ \text{ for } i = 1, 3, \ \ \widehat{\mathbb{B}} := (\boldsymbol{b}_1, \boldsymbol{b}_3), \\
&\boldsymbol{b}_i^* := \xi(\vartheta_{i,1}G, \vartheta_{i,2}G, \vartheta_{i,3}G) \text{ for } i=1,2,3, \ \mathbb{B}^* := (\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \boldsymbol{b}_3^*), \\
&g_T := e(G, G)^{\kappa\xi}, \ \ \mathsf{param}_{\mathsf{BP0}} := (\mathsf{param}_{\mathbb{G}}, \ g_T), \\
&\delta, \sigma, \omega \xleftarrow{\mathsf{U}} \mathbb{F}_q, \ \ \rho, \tau \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\times}, \\
&\boldsymbol{y}_0^* := (\delta, 0, \sigma)_{\mathbb{B}^*}, \ \ \ \boldsymbol{y}_1^* := (\delta, \rho, \sigma)_{\mathbb{B}^*}, \ \ \ \boldsymbol{f} := (\omega, \tau, 0)_{\mathbb{B}}, \\
&\text{return } \ (\mathsf{param}_{\mathsf{BP0}}, \widehat{\mathbb{B}}, \mathbb{B}^*, \boldsymbol{y}_\beta^*, \boldsymbol{f}, \kappa G, \xi G, \delta\xi G).
\end{aligned}
$$

for $\beta \xleftarrow{\mathsf{U}} \{0, 1\}$. For a probabilistic machine $\mathcal{D}$, we define the advantage of $\mathcal{D}$ for Basic Problem 0, $\mathsf{Adv}_{\mathcal{D}}^{\mathsf{BP0}}(\lambda)$, is similarly defined as in Definition 10.

Lemma 35 (Lemma 14 in [3]): For any adversary $\mathcal{D}$, there is a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{E}$, such that for any security parameter λ, $\mathsf{Adv}_{\mathcal{D}}^{\mathsf{BP0}}(\lambda) \ \leq \mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) + 5/q$.

Lemma 35 is proven in the full version of [3]. Therefore, the proof of Lemma 16 is reduced to that of the following Lemma 36, in which the matrix group $\mathcal{P}(6, n, \mathbb{F}_q)$ (Eq. (3)) has an important role.

Lemma 36: For any machine C, there is a probabilistic machine $\mathcal{D}$, whose running time is essentially the same as that of C, such that for any security parameter λ, $\mathsf{Adv}_C^{\mathsf{P4}}(\lambda) \ \leq \mathsf{Adv}_{\mathcal{D}}^{\mathsf{BP0}}(\lambda)$.

Proof. $\mathcal{D}$ is given a Basic Problem 0 instance $(\mathsf{param}_{\mathsf{BP0}}, \widehat{\mathbb{B}}, \mathbb{B}^*, \boldsymbol{y}_\beta^*, \boldsymbol{f}, \kappa G, \xi G)$. $\mathcal{D}$ generates random linear transformation defined by matrices $W_0 \xleftarrow{\mathsf{U}} GL(4, \mathbb{F}_q)$ on $\mathbb{G}^4$, $W_1 \xleftarrow{\mathsf{U}} \mathcal{P}(6, n, \mathbb{F}_q)^{\mathrm{T}}$ on $\mathbb{G}^{6n}$ and $W_2 \xleftarrow{\mathsf{U}} GL(7, \mathbb{F}_q)$ on $\mathbb{G}^7$ as in Remark 2, where $\mathcal{P}(6, n, \mathbb{F}_q)$ is given in Eq. (3). Then $\mathcal{D}$ sets

$$
\begin{aligned}
&\boldsymbol{d}_{0,\iota} := (\boldsymbol{b}_\iota^*, 0)W_0 \ \ \text{ for } \iota = 1, 2, \ \ \ \boldsymbol{d}_{0,3} := (0, 0, 0, \xi G)W_0, \\
&\boldsymbol{d}_{0,4} := (\boldsymbol{b}_3^*, 0)W_0, \ \ \ \boldsymbol{d}_{0,\iota}^* := (\boldsymbol{b}_\iota, 0)(W_0^{-1})^{\mathrm{T}} \ \ \text{ for } \iota = 1, 2, \\
&\boldsymbol{d}_{0,3}^* := (0, 0, 0, \kappa G)(W_0^{-1})^{\mathrm{T}}, \ \ \ \boldsymbol{d}_{0,4}^* := (\boldsymbol{b}_3, 0)(W_0^{-1})^{\mathrm{T}}, \\
&\boldsymbol{g}_{\beta,0} := (\boldsymbol{y}_\beta^*, 0)W_0 + \eta_0 \boldsymbol{d}_{0,4} \text{ where } \eta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q, \\
&\text{for } i = 1, \ldots, n, \\
&\quad \boldsymbol{p}_{1,6(i-1)+\iota} := (0^{6(i-1)}, \boldsymbol{b}_\iota^*, 0^3, 0^{6(n-i)})W_1 \text{ for } \iota = 1, 2, \\
&\quad \boldsymbol{p}_{1,6(i-1)+\iota} := (0^{6(i-1)}, 0^\iota, \xi G, 0^{5-\iota}, 0^{6(n-i)})W_1 \text{ for } \iota = 3, 4, 5, \\
&\quad \boldsymbol{p}_{1,6i} := (0^{6(i-1)}, \boldsymbol{b}_3^*, 0^3, 0^{6(n-i)})W_1, \\
&\quad \boldsymbol{p}_{1,6(i-1)+\iota}^* := (0^{6(i-1)}, \boldsymbol{b}_\iota, 0^3, 0^{6(n-i)})(W_1^{-1})^{\mathrm{T}} \text{ for } \iota = 1, 2, \\
&\quad \boldsymbol{p}_{1,6(i-1)+\iota}^* := (0^{6(i-1)}, 0^\iota, \kappa G, 0^{5-\iota}, 0^{6(n-i)})(W_1^{-1})^{\mathrm{T}} \text{ for } \iota = 3, 4, 5, \\
&\quad \boldsymbol{p}_{1,6i}^* := (0^{6(i-1)}, \boldsymbol{b}_3, 0^3, 0^{6(n-i)})(W_1^{-1})^{\mathrm{T}}, \\
&\quad \widetilde{\boldsymbol{g}}_{\beta,i} := (0^{6(i-1)}, \boldsymbol{y}_\beta^*, 0^3, 0^{6(n-i)})W_1, \\
&\boldsymbol{d}_{2,1} := (\boldsymbol{b}_1^*, 0^4)W_2, \ \ \boldsymbol{d}_{2,2} := (0^3, \xi G, 0^3)W_2, \\
&\boldsymbol{d}_{2,3} := (\boldsymbol{b}_2^*, 0^4)W_2, \ \ \boldsymbol{d}_{2,\iota} := (0^\iota, \xi G, 0^{6-\iota})W_2 \text{ for } \iota = 4, \ldots, 6, \\
&\boldsymbol{d}_{2,7} := (\boldsymbol{b}_3^*, 0^4)W_2, \ \ \boldsymbol{d}_{2,1}^* := (\boldsymbol{b}_1, 0^4)(W_2^{-1})^{\mathrm{T}}, \\
&\boldsymbol{d}_{2,2}^* := (0^3, \kappa G, 0^3)(W_2^{-1})^{\mathrm{T}}, \ \ \boldsymbol{d}_{2,3}^* := (\boldsymbol{b}_2, 0^4)(W_2^{-1})^{\mathrm{T}}, \\
&\boldsymbol{d}_{2,\iota}^* := (0^\iota, \kappa G, 0^{6-\iota})(W_2^{-1})^{\mathrm{T}} \text{ for } \iota = 4, \ldots, 6, \\
&\boldsymbol{d}_{2,7}^* := (\boldsymbol{b}_3, 0^4)(W_2^{-1})^{\mathrm{T}}, \\
&\boldsymbol{g}_{\beta,n+1} := (\boldsymbol{y}_\beta^*, 0^4)W_2 + \eta_{n+1}\boldsymbol{d}_{2,7} \text{ where } \eta_{n+1} \xleftarrow{\mathsf{U}} \mathbb{F}_q,
\end{aligned}
$$

where $(0^{6(i-1)}, \boldsymbol{v}, 0^3, 0^{6(n-i)}) := (0^{6(i-1)}, \widetilde{G}_1, \widetilde{G}_2, \widetilde{G}_3, 0^3, 0^{6(n-i)})$ for any $\boldsymbol{v} := (\widetilde{G}_1, \widetilde{G}_2, \widetilde{G}_3) \in \mathbb{G}^3$. Then, $\mathbb{D}_0 := (\boldsymbol{d}_{0,i})_{i=1,\ldots,4}$ and $\mathbb{D}_0^* := (\boldsymbol{d}_{0,i}^*)_{i=1,\ldots,4}$, $\mathbb{P}_1 := (\boldsymbol{p}_{1,i})_{i=1,\ldots,6n}$ and $\mathbb{P}_1^* := (\boldsymbol{p}_{1,i}^*)_{i=1,\ldots,6n}$ are dual orthonormal bases.

Moreover, we see that the distribution of $\mathbb{D}_1$ is equivalent to that of bases generated by using random special type matrix $Y \xleftarrow{\mathsf{U}} \mathcal{P}(6, n, \mathbb{F}_q)^{\mathrm{T}}$. For the permutation ϖ given in Eq. (4) and the associated matrix Π, the left multiplication by Π^{-1} gives the permutation ϖ^{-1} of the basis vectors $(\boldsymbol{p}_{1,i})_{i=1,\ldots,6n}$ and the right multiplication by Π gives the permutation π^{-1} of the coordinates of vectors in $\mathbb{G}^{6n}$. Therefore, by the conjugate action of the matrix Π, we obtain a basis $\mathbb{D}_1 := (\boldsymbol{d}_{1,\iota})_{\iota=1,\ldots,6n}$, whose distribution is equivalent to that of bases generated by using random special type matrix $X \xleftarrow{\mathsf{U}} \mathcal{L}(6, n, \mathbb{F}_q)^{\mathrm{T}} = \Pi^{-1} \cdot \mathcal{P}(6, n, \mathbb{F}_q)^{\mathrm{T}} \cdot \Pi$, and its dual $\mathbb{D}_1^* := (\boldsymbol{d}_{1,\iota}^*)_{\iota=1\ldots,6n}$.

The new basis $\widetilde{\mathbb{D}}_2$ is the same as $\mathbb{D}_2$ except that the second and third basis vectors are changed to random $\widetilde{\boldsymbol{d}}_{2,3}, \widetilde{\boldsymbol{d}}_{2,4} \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{d}_{2,3}, \boldsymbol{d}_{2,4} \rangle$.

$\mathcal{D}$ can compute $(\mathbb{D}_\iota)_{\iota=0,1}$, $\widetilde{\mathbb{D}}_2$, $\widehat{\mathbb{D}}_0^* := (\boldsymbol{d}_{0,1}^*, \boldsymbol{d}_{0,3}^*, \boldsymbol{d}_{0,4}^*)$, $\widehat{\mathbb{D}}_1^* := (\boldsymbol{d}_{1,1}^*, \ldots, \boldsymbol{d}_{1,n}^*, \boldsymbol{d}_{1,3n+1}^*, \ldots, \boldsymbol{d}_{1,6n}^*)$, $\widehat{\mathbb{D}}_2^* := (\boldsymbol{d}_{2,1}^*, \boldsymbol{d}_{2,2}^*, \boldsymbol{d}_{2,5}^*, \ldots, \boldsymbol{d}_{2,7}^*)$, $\boldsymbol{g}_{\beta,0}, \boldsymbol{g}_{\beta,i} := \widetilde{\boldsymbol{g}}_{\beta,i} + \boldsymbol{\eta}_i$ with $\boldsymbol{\eta}_i \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{d}_{1,4n+1}, \ldots, \boldsymbol{d}_{1,6n} \rangle$ for $i = 1, \ldots, n$, $\boldsymbol{g}_{\beta,n+1}$ from $\widehat{\mathbb{B}} := (\boldsymbol{b}_1, \boldsymbol{b}_3)$, $\mathbb{B}^*$, $\boldsymbol{y}_\beta^*$, κG and ξG. $\mathcal{D}$ sets $N_0 := 4, N_1 := 6n, N_2 := 7$ and $\mathsf{param}_n := (\mathsf{param}_{\mathsf{G}}, \ (N_t)_{t=0,1,2}, \ g_T)$, and then gives $(\mathsf{param}_n, \{\mathbb{D}_t, \widehat{\mathbb{D}}_t^*\}_{t=0,1}, \widetilde{\mathbb{D}}_2, \widehat{\mathbb{D}}_2^*, \{\boldsymbol{g}_{\beta,i}\}_{i=0,\ldots,n+1})$ to C, and outputs $\beta' \in \{0, 1\}$ if C outputs β'.

$\boldsymbol{g}_{\beta,0}$ is expressed over basis $\mathbb{D}_0$ as

$$
\begin{aligned}
\boldsymbol{g}_{0,0} &= (\boldsymbol{y}_0^*, 0)W_0 + \eta_0 \boldsymbol{d}_{0,4} = (\delta, 0, 0, \delta_0)_{\mathbb{D}_0}, \\
\boldsymbol{g}_{1,0} &= (\boldsymbol{y}_1^*, 0)W_0 + \eta_0 \boldsymbol{d}_{0,4} = (\delta, \rho, 0, \delta_0)_{\mathbb{D}_0},
\end{aligned}
$$

with $\delta_0 := \sigma + \eta_0$, and $\boldsymbol{g}_{\beta,i}$ $(i = 1, \ldots, n)$ are expressed over bases $\mathbb{P}_1$ and $\mathbb{D}_1$ as

$$
\begin{aligned}
\boldsymbol{g}_{0,i} &= (0^{6(i-1)}, \boldsymbol{y}_0^*, 0^3, 0^{6(n-i)})W_1 + \boldsymbol{\eta}_i \\
&= (0^{6(i-1)}, \delta, 0, 0^3, \sigma, 0^{6(n-i)})_{\mathbb{P}_1} + \boldsymbol{\eta}_i \\
&= (\overbrace{\delta\vec{e}_i}^{n}, \overbrace{0^{2n}}^{2n}, \overbrace{0^n}^{n}, \overbrace{\vec{\delta}_i}^{2n})_{\mathbb{D}_1}, \text{where } \vec{\delta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n}, \\
\boldsymbol{g}_{1,i} &= (0^{6(i-1)}, \boldsymbol{y}_1^*, 0^3, 0^{6(n-i)})W_1 + \boldsymbol{\eta}_i \\
&= (0^{4(i-1)}, \delta, \rho, 0^3, \sigma, 0^{4(n-i)})_{\mathbb{P}_1} + \boldsymbol{\eta}_i \\
&= (\overbrace{\delta\vec{e}_i}^{n}, \overbrace{\rho\vec{e}_i, 0^n}^{2n}, \overbrace{0^n}^{n}, \overbrace{\vec{\delta}_i}^{2n})_{\mathbb{D}_1}, \text{where } \vec{\delta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n}.
\end{aligned}
$$

$\boldsymbol{g}_{\beta,n+1}$ is expressed over basis $\mathbb{D}_2$ and $\widetilde{\mathbb{D}}_2$ as

$$
\boldsymbol{g}_{0,n+1} = (\boldsymbol{y}_0^*, 0^4)W_2 + \eta_{n+1}\boldsymbol{d}_{2,7} = (\delta, 0, 0, 0^3, \delta_{n+1})_{\mathbb{D}_2}
$$

$$= (\delta, 0, 0, 0^3, \delta_{n+1})_{\widetilde{\mathbb{D}}_2}$$

$$\boldsymbol{g}_{1,n+1} = (\boldsymbol{y}_1^*, 0^4)W_2 + \eta_{n+1}\boldsymbol{d}_{2,7} = (\delta, 0, \rho, 0^3, \delta_{n+1})_{\mathbb{D}_2},$$
$$= (\delta, 0, \vec{\psi}, 0^2, \delta_{n+1})_{\widetilde{\mathbb{D}}_2},$$

with $\delta_{n+1} := \sigma + \eta_{n+1}$. Here, two-dimensional vector $(\rho, 0)$ is changed to random $\vec{\psi}$ by the basis change from $\mathbb{D}_2$ to $\widetilde{\mathbb{D}}_2$.

Here, $\delta, \rho, \delta_0, \vec{\delta}_i$, and δ_{n+1} are uniformly and independently distributed. Therefore, the distribution of $(\mathsf{param}_n, \{\mathbb{D}_t, \widehat{\mathbb{D}}_t^*\}_{t=0,1}, \widetilde{\mathbb{D}}_2, \widehat{\mathbb{D}}_2^*, \{\boldsymbol{g}_{\beta,i}\}_{i=0,\ldots,n+1})$ is exactly the same as $\left\{\varrho \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{P4}}(1^\lambda, n)\right\}$. □

From Lemmas 35 and 36, we have $\mathsf{Adv}_{\mathcal{C}}^{\mathsf{P4}}(\lambda) \leq \mathsf{Adv}_{\mathcal{D}}^{\mathsf{BP0}}(\lambda) \leq \mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) + 5/q$. This completes the proof of Lemma 16. □

E.2 Proofs of Lemmas 18–24

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

Proof. A Problem 6 instance is given as $(\mathsf{param}_n, \{\widehat{\mathbb{B}}_t, \mathbb{B}_t^*\}_{t=0,2}, \mathbb{B}_1, \mathbb{B}_1^*, \boldsymbol{h}_{\beta,0}^*, \boldsymbol{e}_0, \{\boldsymbol{h}_{1,i}^*\}_{i=1,..,n}, \{\boldsymbol{h}_{\beta,2,i}^*, \boldsymbol{e}_{2,i}\}_{i=1,2})$. Note that the sparse DPVS technique is employed only to the first vector space $\mathbb{V}_1$. Hence, we decompose the instance into two parts, standard (non-sparse) DPVS elements and sparse DPVS ones.

The former one is $(\{\widehat{\mathbb{B}}_t, \mathbb{B}_t^*\}_{t=0,2}, \boldsymbol{h}_{\beta,0}^*, \boldsymbol{e}_0, \{\boldsymbol{h}_{\beta,2,i}^*, \boldsymbol{e}_{2,i}\}_{i=1,2})$, and this is an Problem 2 instance in [3] (Definition 5) with $d = 1, n_1 = 2$. The Problem 2 in [3] is reduced from Basic Problem 0 (in Definition 20).

The latter part is $(\mathbb{B}_1, \mathbb{B}_1^*, \{\boldsymbol{h}_{1,i}^*\}_{i=1,..,n})$ where $\boldsymbol{h}_{1,i}^* := \delta\boldsymbol{b}_{1,i}^*$. Since a Basic Problem 0 instance includes $\kappa G, \xi G, \delta\xi G$ (which are also included in DLIN instances), we can simulate all the sparse part, $\{\boldsymbol{h}_{1,i}^*\}_{i=1,..,n}$, as well as $\mathbb{B}_1, \mathbb{B}_1^*$ just from $\kappa G, \xi G, \delta\xi G$.

Consequently, we can simulate both parts from a Basic Problem 0 instance, and then we have $\mathsf{Adv}_{\mathcal{C}}^{\mathsf{P6}}(\lambda) \leq \mathsf{Adv}_{\mathcal{D}}^{\mathsf{BP0}}(\lambda) \leq \mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) + 5/q$. This completes the proof of Lemma 18. □

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

Proof. In order to prove Lemma 19, we construct a probabilistic machine $\mathcal{B}_0$ against Problem 1 by using any adversary $\mathcal{A}$ in a security game (Game 0 or 1) as a black box as follows:

1. $\mathcal{B}_0$ is given Problem 4 instance $(\mathsf{param}_n, \{\mathbb{B}_\iota, \widehat{\mathbb{B}}_t^*\}_{t=0,1,2}, \{\boldsymbol{e}_{\beta,i}\}_{i=0,\ldots,n+1})$.
2. $\mathcal{B}_0$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_0$ sets $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,4})$, $\widehat{\mathbb{B}}_1 := (\boldsymbol{b}_{1,1}, \ldots, \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,4n+1}, \ldots, \boldsymbol{b}_{1,6n})$, $\widehat{\mathbb{B}}_2 := (\boldsymbol{b}_{2,1}, \boldsymbol{b}_{2,2}, \boldsymbol{b}_{2,7})$, $\widehat{\mathbb{B}}_1'^* := (\boldsymbol{b}_{1,1}^*, \ldots, \boldsymbol{b}_{1,n}^*, \boldsymbol{b}_{1,3n+1}^*, \ldots, \boldsymbol{b}_{1,4n}^*)$, $\widehat{\mathbb{B}}_2'^* := (\boldsymbol{b}_{2,1}^*, \boldsymbol{b}_{2,2}^*, \boldsymbol{b}_{2,5}^*, \boldsymbol{b}_{2,6}^*)$. $\mathcal{B}_0$ obtains $\widehat{\mathbb{B}}_t$ and $\widehat{\mathbb{B}}_t'^*$ from $\mathbb{B}_t$ and $\widehat{\mathbb{B}}_t^*$ in the Problem 1 instance, and returns $\mathsf{pk} := (1^\lambda, \mathsf{hk}, \mathsf{param}_n, \{\widehat{\mathbb{B}}_t\}_{t=0,1,2}, \{\widehat{\mathbb{B}}_t'^*\}_{t=1,2}, \boldsymbol{b}_{0,3}^*)$ to $\mathcal{A}$, where $\mathsf{hk} \xleftarrow{\mathsf{R}} \mathsf{KH}_\lambda$.
4. When a reveal key query is issued for attribute set Γ, $\mathcal{B}_0$ answers a correct secret key (Eqs. (15) and (16)) computed by using $\{\widehat{\mathbb{B}}_t^*\}_{t=0,1,2}$, i.e., normal key. When a reveal signature query is issued for access structure $\mathbb{S}$, $\mathcal{B}_1$ answers a correct signature (Eq. (17)) computed by using $\{\widehat{\mathbb{B}}_t^*\}_{t=0,1,2}$, i.e., normal signature.
5. When $\mathcal{B}_0$ receives an output $(m', \mathbb{S}', \vec{s}'^*)$ from $\mathcal{A}$ (where $\mathbb{S}' := (M, \rho)$), $\mathcal{B}_0$ calculates verification text $(\boldsymbol{c}_0, \ldots, \boldsymbol{c}_{\ell+1})$ as follows:
$$\boldsymbol{c}_0 := (-s_0 - s_{\ell+1})\boldsymbol{b}_{0,1} + (-r_0 - r_{\ell+1})\boldsymbol{e}_{\beta,0},$$
$$\boldsymbol{c}_i := \textstyle\sum_{j=1}^n \left(c_{i,j}\boldsymbol{b}_{1,j} + d_{i,j}\boldsymbol{e}_{\beta,j}\right) + \boldsymbol{\eta}_i \quad \text{for } i = 1, \ldots, \ell,$$
$$\boldsymbol{c}_{\ell+1} := (s_{\ell+1} + r_{\ell+1})\boldsymbol{e}_{\beta,n+1}$$
$$+\theta_{\ell+1}\left(\mathsf{H}_{\mathsf{hk}}^{\lambda,\mathsf{D}}(m' \,\|\, \mathbb{S}')\boldsymbol{b}_{2,1} + \boldsymbol{b}_{2,2}\right) + \boldsymbol{\eta}_{\ell+1},$$
where $\vec{f}, \vec{g} \xleftarrow{\mathsf{R}} \mathbb{F}_q^{\mathrm{r}}$, $(s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$, $s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$, $(r_1, \ldots, r_\ell)^{\mathrm{T}} := M \cdot \vec{g}^{\mathrm{T}}$, $r_0 := \vec{1} \cdot \vec{g}^{\mathrm{T}}$, $s_{\ell+1}, r_{\ell+1}, \theta_i, \theta_{\ell+1}, \xi_i, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $i = 1, \ldots, \ell$, and $\vec{c}_i := (c_{i,j}) := s_i\vec{e}_1 + \theta_i\vec{v}_i$, $\vec{d}_i := (d_{i,j}) := r_i\vec{e}_1 + \xi_i\vec{v}_i$ if $\rho(i) = v_i$ or $\vec{c}_i := (c_{i,j}) := s_i\vec{v}_i$, $\vec{d}_i := (d_{i,j}) := r_i\vec{v}_i$ if $\rho(i) = \neg v_i$, $\boldsymbol{\eta}_i \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}_{1,4n+1}, \ldots, \boldsymbol{b}_{1,6n}\rangle$ for $i = 1, \ldots, \ell$, $\boldsymbol{\eta}_{\ell+1} \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}_{2,7}\rangle$ and $\boldsymbol{b}_{0,1}, \{\boldsymbol{b}_{1,j}\}_{j=1,\ldots,n}, \boldsymbol{b}_{2,1}, \boldsymbol{b}_{2,2}, \{\boldsymbol{e}_{\beta,j}\}_{j=0,\ldots,n+1}$ are from the Problem 4 instance. $\mathcal{B}_0$ gives the challenge ciphertext to $\mathcal{A}$.
6. When a reveal key query or reveal signature query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{B}_0$ executes the same procedure as that of step 4.
7. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_0$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_0$ outputs $\beta' := 0$.

When $\beta = 0$, it is straightforward that the distribution by $\mathcal{B}_0$'s simulation is equivalent to that in Game 0. When $\beta = 1$, the distribution by $\mathcal{B}_0$'s simulation is equivalent to that in Game 1. □

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 reveal signature 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 $\mathsf{hk} \overset{\mathsf{R}}{\leftarrow} \mathsf{KH}_\lambda, \widehat{\mathbb{B}}'_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,4}), \widehat{\mathbb{B}}'_1 := (\boldsymbol{b}_{1,1}, \ldots, \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,4n+1}, \ldots, \boldsymbol{b}_{1,6n})$ 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 reveal key 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. (22) and $\boldsymbol{k}_1^*$, $\boldsymbol{k}_{2,1}^*$ and $\boldsymbol{k}_{2,2}^*$ are calculated as in Eq. (16) using fresh $\omega, \tau', \varphi_0, \varphi_1, \varphi_{2,1,1}, \ldots, \varphi_{2,2,2} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$.
   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 14, $(\boldsymbol{h}_{\beta,0}^*, \boldsymbol{e}_0, \boldsymbol{h}_{\beta,1}^*, \{\boldsymbol{e}_{\beta,j,\iota}\}_{j=1,\ldots,n;\,\iota=1,\ldots,n}, \{\boldsymbol{h}_{2,i}^*\}_{i=1,2})$. $\mathcal{B}_1$ 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 $\boldsymbol{r}_i^* \overset{\mathsf{U}}{\leftarrow} \mathsf{span}\langle \boldsymbol{b}_{2,5}^*, \boldsymbol{b}_{2,6}^* \rangle$.
   c. if $\kappa > h$, $\boldsymbol{k}_0^*$ is calculated as in Eq. (15) and $\boldsymbol{k}_1^*$, $\boldsymbol{k}_{2,1}^*$ and $\boldsymbol{k}_{2,2}^*$ are calculated as in Eq. (16) using fresh $\omega, \varphi_0, \varphi_1, \varphi_{2,1,1}, \ldots, \varphi_{2,2,2} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$.

   $\mathcal{B}_1$ 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 reveal signature query for $\mathbb{S} := (M, \rho)$, $\mathcal{B}_1$ generates a normal form signature as in Eq. (17), and sends it to $\mathcal{A}$
6. When $\mathcal{B}_1$ receives an output $(m', \mathbb{S}', \vec{s}')$ from $\mathcal{A}$, $\mathcal{B}_1$ calculates verification text $(\boldsymbol{c}_0, \ldots, \boldsymbol{c}_{\ell+1})$ as follows: $\mathcal{B}_1$ generates $\vec{f}, \vec{g} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q^{\mathfrak{r}}, (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}, (r_1, \ldots, r_\ell)^{\mathrm{T}} := M \cdot \vec{g}^{\mathrm{T}}, s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}, r_0 := \vec{1} \cdot \vec{g}^{\mathrm{T}}, s_{\ell+1}, r_{\ell+1}, \psi_i \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$ and $\mathcal{B}_1$ calculates

   $$\boldsymbol{c}_0 := \boldsymbol{c}_0^{\mathsf{norm}} + r_0 \boldsymbol{e}_0 - r_{\ell+1} \boldsymbol{b}_{0,2},$$
   $$\boldsymbol{c}_i := \boldsymbol{c}_i^{\mathsf{norm}} + \textstyle\sum_{j,\iota=1}^{n} \xi_{i,j} p_{i,\iota} \boldsymbol{e}_{\beta,j,\iota} \text{ for } i = 1, \ldots, \ell,$$
   $$\boldsymbol{c}_{\ell+1} := \boldsymbol{c}_{\ell+1}^{\mathsf{norm}} + p'_{\ell+1,1} \boldsymbol{b}_{2,3} + p'_{\ell+1,2} \boldsymbol{b}_{2,4},$$

   where $\boldsymbol{c}_i^{\mathsf{norm}}$ is a normal form given in Eq. (18) 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 $(\xi_{i,j})_{j=1,\ldots,n} \overset{\mathsf{U}}{\leftarrow} \{(\xi_j)_{j=1,\ldots,n} \in \mathbb{F}_q^n \mid \sum_{j=1}^n \xi_j = 1\}$ 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 $(m', \mathbb{S}', \vec{s}')$ 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 reveal signature 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 $\tau'_0 \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$, 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. □

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, $|\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}(h-1))}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{3\text{-}h}}^{\mathsf{P6}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_{4\text{-}h}}^{\mathsf{H,CR}}(\lambda) + 3/q$, 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 [38]. For completeness, we give the proof of Lemma 22 below.

Proof. In order to prove Lemma 22, we construct a probabilistic machine $\mathcal{B}_3$ against Problem 6 by using any adversary $\mathcal{A}$ in a security game (Game 3-($h-1$) or 3-h) as a black box as follows:

1. $\mathcal{B}_3$ is given an integer h and a Problem 6 instance, $(\mathsf{param}_n, \{\widehat{\mathbb{B}}_t, \mathbb{B}_t^*\}_{t=0,2}, \mathbb{B}_1, \mathbb{B}_1^*, \boldsymbol{h}_{\beta,0}^*, \boldsymbol{e}_0, \{\boldsymbol{h}_{1,l}^*\}_{l=1,..,n}, \{\boldsymbol{h}_{\beta,2,l}^*, \boldsymbol{e}_{2,l}\}_{l=1,2})$.
2. $\mathcal{B}_3$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_3$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1^\lambda, \mathsf{hk}, \mathsf{param}_n, \{\widehat{\mathbb{B}}'_t\}_{t=0,1,2}, \{\widehat{\mathbb{B}}_t^*\}_{t=1,2}, \boldsymbol{b}_{0,3}^*)$ of Game 3-($h-1$) (and 3-h), where $\mathsf{hk} \overset{\mathsf{R}}{\leftarrow} \mathsf{KH}_\lambda$, $\widehat{\mathbb{B}}'_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,4}), \widehat{\mathbb{B}}'_1 := (\boldsymbol{b}_{1,1}, \ldots, \boldsymbol{b}_{1,n}, \boldsymbol{b}_{1,4n+1}, \ldots, \boldsymbol{b}_{1,6n})$, $\widehat{\mathbb{B}}'_2 := (\boldsymbol{b}_{2,1}, \boldsymbol{b}_{2,2}, \boldsymbol{b}_{2,7})$, and $\widehat{\mathbb{B}}_1^* := (\boldsymbol{b}_{1,1}^*, \ldots, \boldsymbol{b}_{1,n}^*, \boldsymbol{b}_{1,3n+1}^*, \ldots, \boldsymbol{b}_{1,4n}^*), \widehat{\mathbb{B}}_2^* := (\boldsymbol{b}_{2,1}^*, \boldsymbol{b}_{2,2}^*, \boldsymbol{b}_{2,5}^*, \boldsymbol{b}_{2,6}^*)$, that are obtained from the Problem 6 instance.
4. When a reveal key query is issued for attribute $\Gamma := \{x_1, \ldots, x_{n'}\}$, $\mathcal{B}_3$ answers semi-functional key $\{\boldsymbol{k}_t^*\}_{t \in T}$ where $T := \{0, 1, (2,1), (2,2)\}$, with Eqs. (16), (22),

that is computed by using $\{\mathbb{B}_t^*\}_{t=0,1,2}$ of the Problem 6 instance.

5. When the ι-th reveal signature query is issued for message m and attribute $\mathbb{S} := (M, \rho)$, $\mathcal{B}_3$ answers as follows:

   a. When $1 \le \iota \le h-1$, $\mathcal{B}_3$ answers semi-functional signature $\vec{\boldsymbol{s}}^* := (\boldsymbol{s}_i)_{i=0,\dots,\ell+1}$ such that $\boldsymbol{s}_0$ and $\boldsymbol{s}_\ell + 1$ are computed by Eq. (23), and others are computed by Eq. (17) using $\{\mathbb{B}_t^*\}_{t=0,1,2}$ of the Problem 6 instance.

   b. When $\iota = h$, $\mathcal{B}_3$ calculates $\vec{\boldsymbol{s}}^* := (\boldsymbol{s}_0^*, .., \boldsymbol{s}_{\ell+1}^*)$ by using $\{\widehat{\mathbb{B}}_t^*\}_{t=0,1,2}, \boldsymbol{h}_{\beta,0}^*, \{\boldsymbol{h}_{1,l}^*\}_{l=1,..,n}, \{\boldsymbol{h}_{\beta,2,l}^*\}_{l=1,2}$ of the Problem 6 instance as follows:

   $$\boldsymbol{s}_0^* := \boldsymbol{h}_{\beta,0}^*, \ \boldsymbol{s}_i^* := \textstyle\sum_{l=1}^n z_{i,l}\boldsymbol{h}_{1,l}^* + \boldsymbol{r}_i^* \text{ for } i = 1, .., \ell,$$
   $$\boldsymbol{s}_{\ell+1}^* := \boldsymbol{h}_{\beta,2,1}^* + \mathsf{H}_{\mathsf{hk}}^{\lambda,\mathsf{D}}(m \,\|\, \mathbb{S}) \cdot \boldsymbol{h}_{\beta,2,2}^*,$$

   where $(\zeta_i) \overset{\mathsf{U}}{\leftarrow} \{(\zeta_i) \mid \sum_{i=1}^{\ell} \zeta_i M_i = \vec{1}\}$, and if $\rho(i) = (t, \vec{v}_i)$, then $\vec{z}_i := (z_{i,l}) \overset{\mathsf{U}}{\leftarrow} \{\vec{z}_i \mid \vec{z}_i \cdot \vec{v}_i = 0, \ z_{i,1} = \zeta_i\}$, if $\rho(i) = \neg(t, \vec{v}_i)$, then $\vec{z}_i := (z_{i,l}) \overset{\mathsf{U}}{\leftarrow} \{\vec{z}_i \mid \vec{z}_i \cdot \vec{v}_i = \zeta_i\}$, and $\boldsymbol{r}_i^* \overset{\mathsf{U}}{\leftarrow} \mathsf{span}\langle \boldsymbol{b}_{1,3n+1}^*, \dots, \boldsymbol{b}_{1,4n}^* \rangle$ for $i = 1, \dots, \ell$.

   c. When $\iota \ge h+1$, $\mathcal{B}_3$ answers normal signature $\vec{\boldsymbol{s}}^*$ with Eq. (17), that is computed by using $\{\mathbb{B}_t^*\}_{t=0,1,2}$ of the Problem 6 instance.

6. When $\mathcal{B}_3$ receives an output $(m', \mathbb{S}', \vec{\boldsymbol{s}}'^*)$ from $\mathcal{A}$, $\mathcal{B}_3$ calculates semi-functional verification text $\vec{\boldsymbol{c}} := (\boldsymbol{c}_0, \dots, \boldsymbol{c}_{\ell+1})$ with Eqs. (19), (20), (21) as follows: $\boldsymbol{c}_i$ for $i = 1, \dots, \ell$ are calculated as Eq. (20) by using basis $\mathbb{B}_1$, and using the coefficient $s_0 := \sum_{k=1}^r f_k$,

   $$\alpha_l, \widetilde{\alpha}_l \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q \ \text{ for } l = 1,2, \quad \widetilde{\boldsymbol{f}}_0 := \widetilde{\alpha}_1 \boldsymbol{e}_0 + \widetilde{\alpha}_2 \boldsymbol{b}_{0,1},$$
   $$\boldsymbol{f}_{2,j} := \alpha_1 \boldsymbol{e}_{2,j} + \alpha_2 \boldsymbol{b}_{2,j},$$
   $$\widetilde{\boldsymbol{f}}_{2,j} := \widetilde{\alpha}_1 \boldsymbol{e}_{2,j} + \widetilde{\alpha}_2 \boldsymbol{b}_{2,j} \ \text{ for } j = 1,2;$$
   $$\boldsymbol{c}_0 := -s_0 \boldsymbol{b}_{0,1} - \widetilde{\boldsymbol{f}}_0 + \boldsymbol{q}_0,$$
   $$\boldsymbol{c}_{\ell+1} := \widetilde{\boldsymbol{f}}_{2,1} - \mathsf{H}_{\mathsf{hk}}^{\lambda,\mathsf{D}}(m' \,\|\, \mathbb{S}') \cdot \boldsymbol{f}_{2,1} + \boldsymbol{f}_{2,2} + \boldsymbol{q}_{\ell+1},$$

   where $\boldsymbol{q}_0 \overset{\mathsf{U}}{\leftarrow} \mathsf{span}\langle \boldsymbol{b}_{0,4} \rangle$, $\boldsymbol{q}_{\ell+1} \overset{\mathsf{U}}{\leftarrow} \mathsf{span}\langle \boldsymbol{b}_{2,7} \rangle$, and $\boldsymbol{b}_{0,1}, \boldsymbol{e}_0, \boldsymbol{b}_{2,j}, \boldsymbol{e}_{2,j}$ for $j = 1,2$ are from the Problem 6 instance. $\mathcal{B}_3$ verifies the signature $(m', \mathbb{S}', \vec{\boldsymbol{s}}'^*)$ using Ver with the above $(\boldsymbol{c}_0, \dots, \boldsymbol{c}_{\ell+1})$, and outputs $\beta' := 1$ if the verification succeeds, $\beta' := 0$ otherwise.

Claim 1: The pair of signature $\vec{\boldsymbol{s}}^*$ generated in case (b) of step 5 and verification text $\vec{\boldsymbol{c}}$ generated in step 6 has the same distribution as that in Game 3-$(h-1)$ (resp. Game 3-h) when $\beta = 0$ (resp. $\beta = 1$) except with probability $1/q$ (resp. $\mathsf{Adv}_{\mathcal{F}_{4\text{-}h}}^{\mathsf{H,CR}}(\lambda) + 2/q$ for a probabilistic machine $\mathcal{F}_4$ with essentially same running time as that of $\mathcal{A}$, where $\mathcal{F}_{4\text{-}h}(\cdot) := \mathcal{F}_4(h, \cdot)$).

Proof. We consider the joint distribution of $\vec{\boldsymbol{c}}$ and $\vec{\boldsymbol{s}}^*$. Clearly, a part of verification text, $\boldsymbol{c}_1, \dots, \boldsymbol{c}_\ell$, and a part of signature, $\boldsymbol{s}_1^*, \dots, \boldsymbol{s}_\ell^*$, are the same as those in Game 3-$(h-1)$ and Game 3-h. Hence, we only consider $\boldsymbol{c}_0, \boldsymbol{c}_{\ell+1}, \boldsymbol{s}_0^*$, and $\boldsymbol{s}_{\ell+1}^*$.

When $\beta = 0$, it is straightforward the joint distribution of $\boldsymbol{c}_0, \boldsymbol{c}_{\ell+1}, \boldsymbol{s}_0^*$, and $\boldsymbol{s}_{\ell+1}^*$ are the same as those in Game 3-$(h-1)$ except that δ defined in Problem 6 is zero, i.e., except with probability $1/q$.

When $\beta = 1$, we need to check that $-r_{\ell+1}$ in $\boldsymbol{c}_0$ (given in Eq. (19)), $\vec{\psi}_{\ell+1}$ in $\boldsymbol{c}_{\ell+1}$ (given in Eq. (21)), π_0 in $\boldsymbol{s}_0^*$ and $\vec{\pi}_{\ell+1}$ in $\boldsymbol{s}_{\ell+1}^*$ (given in Eq. (23)) are distributed as in those in Game 5-h, i.e., these are uniformly and independently distributed (with negligible probability). These are given as

$$-r_{\ell+1} = -u_0^{-1}\widetilde{s}_{\ell+1},$$
$$\vec{\psi}_{\ell+1} = \left(\widetilde{s}_{\ell+1} - \widetilde{\theta}_{\ell+1} \cdot \mathsf{H}_{\mathsf{hk}}^{\lambda,\mathsf{D}}(m' \,\|\, \mathbb{S}'), \widetilde{\theta}_{\ell+1}\right) \cdot Z_{d+1},$$
$$\pi_0 = u_0, \ \ \vec{\pi}_{\ell+1} = \left(1, \mathsf{H}_{\mathsf{hk}}^{\lambda,\mathsf{D}}(m \,\|\, \mathbb{S})\right) \cdot U_{d+1},$$

where $u_0 \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q^\times$, $\widetilde{\theta}_{\ell+1}, \widetilde{s}_{\ell+1} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$, which are independent from all the other variables and $U_{d+1} \overset{\mathsf{U}}{\leftarrow} GL(2, \mathbb{F}_q), Z_{d+1} := (U_{d+1}^{-1})^{\mathrm{T}}$. Since $(m, \mathbb{S}) \neq (m', \mathbb{S}')$, $\vec{\psi}_{\ell+1} \cdot \vec{\pi}_{\ell+1} = \alpha\widetilde{\theta}_{\ell+1} + \widetilde{s}_{\ell+1}$ with nonzero $\alpha \left(:= \mathsf{H}_{\mathsf{hk}}^{\lambda,\mathsf{D}}(m \,\|\, \mathbb{S}) - \mathsf{H}_{\mathsf{hk}}^{\lambda,\mathsf{D}}(m' \,\|\, \mathbb{S}')\right)$ except with probability $\mathsf{Adv}_{\mathcal{F}_{4\text{-}h}}^{\mathsf{H,CR}}(\lambda)$ for a probabilistic machine $\mathcal{F}_{4\text{-}h}$ with essentially same running time as that of $\mathcal{A}$.

Then, coefficients $-r_{\ell+1}$ and π_0 are uniformly and independently distributed, which are independent from $\vec{\psi}_{\ell+1} \cdot \vec{\pi}_{\ell+1} = \alpha\widetilde{\theta}_{\ell+1} + \widetilde{s}_{\ell+1}$ since $u_0 \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q^\times$, $\widetilde{s}_{\ell+1}, \widetilde{\theta}_{\ell+1} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$ and $\alpha \neq 0$. Moreover, from the pairwise independence lemma (Lemma 3 in the full version of [3]), the pair of vectors $(\vec{\psi}_{\ell+1}, \vec{\pi}_{\ell+1})$ is uniformly distributed in the space $\{(\vec{\psi}_{\ell+1}, \vec{\pi}_{\ell+1}) | \vec{\psi}_{\ell+1} \cdot \vec{\pi}_{\ell+1} = \alpha\widetilde{\theta}_{\ell+1} + \widetilde{s}_{\ell+1}\}$. Therefore, the joint distribution of $\boldsymbol{c}_0, \boldsymbol{c}_{\ell+1}, \boldsymbol{s}_0^*$, and $\boldsymbol{s}_{\ell+1}^*$ are the same as those in Game 3-h except that δ defined in Problem 6 is zero or $\vec{\psi}_{\ell+1} \cdot \vec{\pi}_{\ell+1} = 0$ i.e., except with probability $\mathsf{Adv}_{\mathcal{E}_{6\text{-}h}}^{\mathsf{H,CR}}(\lambda) + 2/q$. This completes the proof of Claim 1. □

Therefore, $|\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}(h-1))}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h)}(\lambda)| \le \mathsf{Adv}_{\mathcal{B}_{3\text{-}h}}^{\mathsf{P6}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_{4\text{-}h}}^{\mathsf{H,CR}}(\lambda) + 1/q + 2/q = \mathsf{Adv}_{\mathcal{B}_{3\text{-}h}}^{\mathsf{P6}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_{4\text{-}h}}^{\mathsf{H,CR}}(\lambda) + 3/q$ from Shoup's difference lemma. This completes the proof of Lemma 22. □

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

Lemma 23 is proven in a manner similar to Lemma 17 in the full version of [38]. For completeness, we give the proof of Lemma 23 below.

Proof. To prove Lemma 23, we will show distribution $(\mathsf{param}_n, \{\widehat{\mathbb{B}}_t\}_{t=0,1,2}, \{\widehat{\mathbb{B}}_t^*\}_{t=1,2}, \boldsymbol{b}_{0,3}^*, \{\mathsf{sk}_\Gamma^{(j)}\}_{j=1,..,\nu_K}, \{\vec{\boldsymbol{s}}^{(j)*}\}_{j=1,..,\nu_S}, \boldsymbol{c})$ in Game 3-ν_S and that in Game 4 are equivalent, where $\mathsf{sk}_\Gamma^{(j)}$ is the answer to the j-th reveal key query, $\vec{\boldsymbol{s}}^{(j)*}$ is that to the j-th reveal signature query, and $\vec{\boldsymbol{c}}$ is the verification text $(\boldsymbol{c}_0, \dots, \boldsymbol{c}_{\ell+1})$. By the definition of these games, we only need to consider elements in $\mathbb{V}_0$. We define new dual orthonormal bases $\mathbb{D}_0$ and $\mathbb{D}_0^*$ of $\mathbb{V}_0$ as follows: We generate $\theta \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$, and set $\boldsymbol{d}_{0,2} := (\theta, 1, 0, 0)_{\mathbb{B}} = \theta\boldsymbol{b}_{0,1} + \boldsymbol{b}_{0,2}, \boldsymbol{d}_{0,1}^* := (1, -\theta, 0, 0)_{\mathbb{B}} = \boldsymbol{b}_{0,1}^* - \theta\boldsymbol{b}_{0,2}^*$. Let $\mathbb{D}_0 :=$

$(\boldsymbol{b}_{0,1}, \boldsymbol{d}_{0,2}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,4})$ and $\mathbb{D}_0^* := (\boldsymbol{d}_{0,1}^*, \boldsymbol{b}_{0,2}^*, \boldsymbol{b}_{0,3}^*, \boldsymbol{b}_{0,4}^*)$. Then, $\mathbb{D}_0$ and $\mathbb{D}_0^*$ are dual orthonormal, and are distributed the same as the original bases, $\mathbb{B}_0$ and $\mathbb{B}_0^*$.

The $\mathbb{V}_0$ components $\{\boldsymbol{k}_0^{(j)*}\}_{j=1,\dots,\nu_K}$ in keys, $\{\boldsymbol{s}_0^{(j)*}\}_{j=1,\dots,\nu_S}$ in signatures, and verification text $\boldsymbol{c}_0$ in Game 3-ν_S are expressed over bases $\mathbb{B}_0$ and $\mathbb{B}_0^*$ as $\boldsymbol{k}_0^{(j)*} = (\omega^{(j)}, \tau_0'^{(j)}, \varphi_0^{(j)}, 0)_{\mathbb{B}_0^*}$, $\boldsymbol{s}_0^{(j)*} = (\widetilde{\delta}^{(j)}, \pi_0^{(j)}, \sigma_0^{(j)}, 0)_{\mathbb{B}_0^*}$ and $\boldsymbol{c}_0 = (-s_0 - s_{\ell+1}, -r_0 - r_{\ell+1}, 0, \eta_0)_{\mathbb{B}_0}$. Then,

$$\begin{aligned}\boldsymbol{k}_0^{(j)*} &= (\omega^{(j)}, \tau_0'^{(j)}, \varphi_0^{(j)}, 0)_{\mathbb{B}_0^*} = (\omega^{(j)}, \tau_0'^{(j)} + \theta\omega^{(j)}, \varphi_0^{(j)}, 0)_{\mathbb{D}_0^*} \\ &= (\omega^{(j)}, \vartheta^{(j)}, \varphi_0^{(j)}, 0)_{\mathbb{D}_0^*},\end{aligned}$$

where $\vartheta^{(j)} := \tau_0'^{(j)} + \theta\omega^{(j)}$ which are uniformly, independently distributed since $\tau_0'^{(j)} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$,

$$\begin{aligned}\boldsymbol{s}_0^{(j)*} &= (\widetilde{\delta}^{(j)}, \pi_0^{(j)}, \sigma_0^{(j)}, 0)_{\mathbb{B}_0^*} = (\widetilde{\delta}^{(j)}, \pi_0^{(j)} + \theta\widetilde{\delta}^{(j)}, \sigma_0^{(j)}, 0)_{\mathbb{D}_0^*} \\ &= (\widetilde{\delta}^{(j)}, \widetilde{\vartheta}^{(j)}, \sigma_0^{(j)}, 0)_{\mathbb{D}_0^*}\end{aligned}$$

where $\widetilde{\vartheta}^{(j)} := \pi_0^{(j)} + \theta\widetilde{\delta}^{(j)}$ which are uniformly, independently distributed since $\pi_0^{(j)} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$, and

$$\begin{aligned}\boldsymbol{c}_0 &= (-s_0 - s_{\ell+1},\ -r_0 - r_{\ell+1},\ 0,\ \eta_0)_{\mathbb{B}_0} \\ &= (-s_0 - s_{\ell+1} - \theta(-r_0 - r_{\ell+1}),\ -r_0 - r_{\ell+1},\ 0,\ \eta_0)_{\mathbb{D}_0} \\ &= (\widetilde{s}_0,\ -r_0 - r_{\ell+1},\ 0,\ \eta_0)_{\mathbb{D}_0}\end{aligned}$$

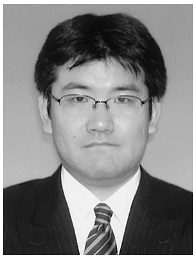
where $\widetilde{s}_0 := -s_0 - s_{\ell+1} - \theta(-r_0 - r_{\ell+1})$ which is uniformly, independently distributed since $\theta \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$ if $-r_0 - r_{\ell+1} \neq 0$.

In the light of the adversary's view, both $(\mathbb{B}_0, \mathbb{B}_0^*)$ and $(\mathbb{D}_0, \mathbb{D}_0^*)$ are consistent with public key $\mathsf{pk} := (1^\lambda, \mathsf{hk}, \mathsf{param}_n, \{\widehat{\mathbb{B}}_t\}_{t=0,1,2}, \{\widehat{\mathbb{B}}_t^*\}_{t=1,2}, \boldsymbol{b}_{0,3}^*)$. Therefore, $\{\mathsf{sk}_\Gamma^{(j)}\}_{j=1,\dots,\nu_K}$, $\{\vec{\boldsymbol{s}}^{(j)*}\}_{j=1,\dots,\nu_S}$, and $\vec{\boldsymbol{c}}$ can be expressed as keys, signatures, and verification text in two ways, in Game 3-ν_S over bases $\{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=0,1,2}$ and in Game 4 over bases $\mathbb{D}_0, \mathbb{D}_0^*, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=1,2}$. Thus, Game 3-$\nu_S$ can be conceptually changed to Game 4 if $-r_0 - r_{\ell+1} \neq 0$, i.e., except with probability $1/q$. □

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

Lemma 24 is proven in a manner similar to Lemma 18 in the full version of [38]. For completeness, we give the proof of Lemma 24 below.

Proof. Let $(\boldsymbol{s}_0'^*, \dots, \boldsymbol{s}_{\ell+1}'^*)$ be signature $\mathcal{A}$ outputs. If $e(\boldsymbol{b}_{0,1}, \boldsymbol{s}_0'^*) = 1$, the verification fails by the definition of Ver. Otherwise, the verification fails except with negligible probability regardless of the output of the adversary since coefficient $\widetilde{s}_0$ of $\boldsymbol{b}_{0,1}$ in $\boldsymbol{c}_0$ (Eq. (24)) is uniform and independent from all the other variables, and the coefficient of $\boldsymbol{b}_{0,1}^*$ in $\boldsymbol{s}_0'^*$ is nonzero. Hence, $\mathsf{Adv}_{\mathcal{A}}^{(6)}(\lambda) = 1/q$. □



Katsuyuki Takashima received the B.S., M.S. and PhD degrees from Kyoto University, Kyoto, Japan, in 1993, 1995 and 2009, respectively. He is presently engaged in research on cryptography and information security at Information Technology R&D center, Mitsubishi Electric Corporation. He received the JSIAM Transactions Best Paper Award in 2003 and 2016, and IEICE Best Paper Award in 2015 and 2016. He is a member of JSIAM, MSJ, IPSJ, MSJ and IACR.